International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

An Intelligent Generative AI Framework for Adaptive Threat Monitoring and Secure Cloud Computing

[1]Dr Vemuri Sudarsan Rao,[2]Dr Kavitha Guda , [3]Dr.Macha Sarada
[1]Associate Professor , Department of Computer Science and Engineering, Sri Chaitanya Institute of Technology and Research, Khammam, Telangana, India
[1]Email:sudharshan.cse2008@gmail.com
[2]Associate Professor, Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology , cheeryal(V),Medchal Dist,Hyderabad, Telangana -501301, India
[2]Email:kavitharddy.darshan@gmail.com
[3]Associate Professor, Department of Computer Science and Engineering(Artificial Intelligence and Machine Learning), Anurag Engineering College ,Kodad ,Suryapet ,Telangana- 508206, India
[3]Email:saradaramaraok@gmail.com

ABSTRACT

The rapid evolution of cloud computing has enabled organizations to deploy scalable applications and distributed services with greater efficiency; however, it has also increased the complexity of protecting cloud infrastructures against sophisticated and continuously evolving cyber threats. Conventional cloud security monitoring solutions primarily rely on static rules, predefined signatures, and manually crafted detection policies, making them less effective against zero-day attacks, advanced persistent threats, and dynamic attack behaviors. To address these limitations, this research proposes an intelligent Generative AI-driven framework for adaptive cloud security monitoring that delivers proactive threat analysis and continuous security assessment across modern cloud environments.The proposed framework integrates security telemetry from multiple cloud sources, including system logs, network traffic, authentication records, application events, and resource utilization metrics, to establish a comprehensive view of cloud security operations. Advanced generative artificial intelligence techniques are employed to model complex behavioral patterns, correlate security events, generate contextual threat intelligence, and identify previously unseen attack scenarios that cannot be effectively recognized using conventional signature-based approaches. By combining intelligent anomaly detection with adaptive learning, the framework continuously refines its detection capability based on newly observed attack patterns, thereby improving its resilience against evolving cybersecurity threats.Furthermore, the proposed system incorporates automated risk assessment and intelligent alert prioritization to reduce false-positive notifications and assist security analysts in making timely and informed decisions. Experimental evaluation is performed using standard performance metrics, including accuracy, precision, recall, F1-score, detection rate, and false-positive rate, to assess the effectiveness of the proposed framework. The results demonstrate that the integration of Generative AI with adaptive security analytics significantly enhances threat detection performance, strengthens situational awareness, and improves the overall security posture of cloud computing environments. The proposed framework offers a scalable, intelligent, and future-ready solution for safeguarding cloud infrastructures while supporting automated cyber defense against emerging and sophisticated security threats.

Keywords: Generative Artificial Intelligence, Cloud Security, Adaptive Security Monitoring, Threat Detection, Intelligent Security Analytics, Anomaly Detection, Cybersecurity, Cloud Computing, Threat Intelligence, Risk Assessment.

I. INTRODUCTION

Cloud computing has changed the way organizations store information, deploy applications, and manage computing resources. Its flexible structure allows businesses to access services whenever required without maintaining extensive physical infrastructure. At the same time, this flexibility has created a security environment that is difficult to observe and control. Cloud platforms continuously

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

generate large volumes of network traffic, access records, application events, and system logs. Examining such information through conventional monitoring techniques has become increasingly challenging, particularly when threats are designed to remain hidden within normal activities.

Most traditional cloud security tools depend on predefined rules, known attack signatures, and fixed alert conditions. These approaches can identify familiar threats, but their effectiveness may decrease when an attacker changes the behavior or introduces a previously unseen technique. Another concern is the large number of alerts generated by security systems. Many of these alerts may not represent serious incidents, forcing security teams to spend considerable time separating genuine threats from harmless events. As cloud workloads and user activities change frequently, a static monitoring strategy may fail to reflect the actual security state of the environment.

Artificial intelligence has introduced new possibilities for analyzing complex security data. Machine learning techniques can discover patterns and identify activities that differ from expected behavior. However, many conventional models still provide limited contextual information about why an event has been classified as suspicious. Generative AI offers a broader capability by examining relationships among multiple events, interpreting security observations, and producing meaningful descriptions of potential threats. This makes it useful for cloud environments where a single attack may involve several connected actions occurring across different services.

The proposed Generative AI-Powered Adaptive Cloud Security Monitoring System is designed to provide continuous and intelligent observation of cloud activities. It processes information collected from system logs, network events, authentication records, and resource usage patterns. Suspicious activities are evaluated according to their behavior and surrounding context rather than relying only on fixed signatures. The generative component assists in interpreting detected abnormalities and presenting understandable threat insights for further analysis. An adaptive learning mechanism is also included so that the monitoring process can respond to changing conditions. Newly observed events and threat patterns can be used to refine future security decisions, allowing the system to remain relevant as the cloud environment evolves. Through the integration of intelligent monitoring, anomaly recognition, contextual threat analysis, and adaptive learning, the proposed approach aims to improve threat visibility, reduce unnecessary alerts, and support timely security responses in modern cloud infrastructures.

II. LITERATURE SURVEY

1. Title: Practical Machine Learning for Cloud Intrusion Detection: Challenges and the Way Forward

Authors: Ram Shankar Siva Kumar, Andrew Wicker, and Matt Swann

Abstract: This study discusses the practical difficulties involved in applying machine learning techniques to intrusion detection within continuously changing cloud environments. The authors explain that conventional anomaly detection models often struggle when normal cloud behaviour changes over time. The work examines challenges related to feature selection, model maintenance, evolving attack patterns, and false alarms. It further emphasizes that a successful cloud security solution requires more than high model accuracy; it must also remain reliable when deployed under real operational conditions. The study provides an important foundation for developing adaptive security monitoring systems that can adjust to changing cloud activities.

2. Title: A Survey of Large Language Models for Cyber Threat Detection

Authors: Y. Chen et al.

Abstract: This research reviews the growing use of large language models in cyber threat detection. The study examines how LLMs can support security activities such as log interpretation, threat intelligence processing, malicious content identification, and anomaly discovery. It highlights the ability of language models to understand contextual relationships within complex security information, which is often difficult for traditional

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

rule-based tools. The authors also discuss concerns involving computational requirements, privacy, model reliability, and explainability. The survey indicates that LLM-based security systems can strengthen existing detection frameworks when combined with domain-specific knowledge and carefully designed security controls.

3. Title: Large Language Models for Cyber Security: A Systematic Literature Review

Authors: Hanxiang Xu, Shenao Wang, Ningke Li, Kailong Wang, Yanjie Zhao, Kai Chen, Ting Yu, Yang Liu, and Haoyu Wang

Abstract: This systematic review investigates the application of large language models across different areas of cybersecurity. The authors analyze research involving vulnerability detection, malware analysis, network intrusion identification, and phishing detection. The study finds that LLMs provide useful capabilities for processing unstructured security information and supporting intelligent threat analysis. At the same time, limitations related to dataset diversity, privacy, interpretability, and domain adaptation are identified. The authors suggest fine-tuning, transfer learning, and domain-oriented training as promising methods for improving the effectiveness of LLM-based cybersecurity solutions.

4. Title: Advancing Anomaly Detection in Cloud Environments with Generative AI

Authors: U. Demirbaga et al.

Abstract: This work presents CloudGEN, a generative AI-oriented approach developed for anomaly detection in cloud environments. The study explores how generative techniques can learn complex characteristics of cloud operations and distinguish abnormal activities from legitimate behaviour. Unlike static security mechanisms, the proposed approach is designed to recognize patterns that may change as workloads and cloud conditions evolve. The research demonstrates the growing value of generative models for detecting previously unseen abnormalities and strengthening cloud monitoring. The work is closely connected to adaptive security systems because it focuses on continuous analysis within dynamic computing environments.

5. Title: Enhancing Cloud Security Using Generative AI

Authors: V. K. Srivastava et al.

Abstract: The study proposes a generative AI-enhanced intrusion detection approach that combines Transformer-based anomaly analysis with conditional generative adversarial networks. Synthetic attack samples are generated to improve the representation of less frequent threat classes, while the Transformer component examines complex relationships within security data. The proposed method addresses common intrusion detection difficulties such as imbalanced datasets, changing attacks, and the need for timely threat recognition. The findings suggest that generative techniques can improve the adaptability of cloud security models by exposing them to a broader range of attack behaviour during training.

6. Title: Leveraging Large Language Models for Scalable and Explainable Cybersecurity Log Analysis

Authors: G. Palma et al.

Abstract: This research investigates the use of large language models for classifying and interpreting cybersecurity logs. Several LLMs are examined and compared with conventional machine learning techniques for identifying suspicious security events. The study focuses not only on detection performance but also on the need to provide understandable explanations for security decisions. Such contextual interpretation can assist analysts in examining large volumes of alerts and determining which events require immediate attention. The findings support the use of language models as an intelligent analysis layer in modern security monitoring systems.

III. EXISTING SYSTEM

The existing cloud security monitoring system mainly depends on traditional mechanisms such as firewalls, intrusion detection systems, predefined security rules, and signature-based threat identification. These techniques continuously examine network traffic, access records, and system logs to find activities that match already known attack patterns. Although such methods are useful for detecting familiar threats, they often struggle when an attacker introduces a new technique or slightly modifies an existing attack. Some current systems use machine learning-based anomaly detection, but these

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

models may still produce a large number of false alerts when legitimate cloud behaviour changes unexpectedly. Another major limitation is that security events are often examined separately, making it difficult to identify a complete attack formed by several low-risk activities occurring across different cloud services. The existing approach also requires frequent rule updates and considerable manual involvement from security analysts to investigate alerts and understand their actual impact. As a result, conventional systems may experience delayed threat recognition, limited adaptability, alert overload, and reduced effectiveness against unknown or continuously evolving cloud attacks.

IV. PROPOSED SYSTEM

The proposed Generative AI-Powered Adaptive Cloud Security Monitoring System introduces an intelligent framework for continuously observing and protecting dynamic cloud environments. Instead of depending entirely on fixed rules and known attack signatures, the system collects and examines cloud logs, network activities, authentication records, user behaviour, and resource usage patterns to identify unusual events. Machine learning-based anomaly detection is used to recognize deviations from normal cloud operations, while the generative AI component studies the context and relationship between multiple security events. This allows the system to produce meaningful threat descriptions and reveal suspicious activities that may remain unnoticed when individual alerts are analysed separately. An adaptive learning mechanism updates the monitoring behaviour according to newly observed threats and changes in normal cloud usage. Detected events are assigned risk levels so that serious incidents can be given higher priority, reducing the burden created by unnecessary alerts. The system also presents security findings through an interactive monitoring dashboard, enabling administrators to view threat details, risk status, and generated security insights. By combining continuous monitoring, adaptive anomaly detection, contextual analysis, and generative AI, the proposed system aims to provide faster threat recognition and more effective protection against both known and emerging cloud attacks.

V. SYSTEM ARCHITECTURE

The system architecture of the Generative AI-Powered Adaptive Cloud Security Monitoring System follows a layered process in which cloud information is collected, analysed, interpreted, and converted into meaningful security actions. The process begins with the data source layer, which gathers information from cloud infrastructure such as virtual machines, containers, and storage services. Network traffic, user login activities, access records, system logs, application events, and outputs from existing security tools are also included. These different sources provide a broad view of what is happening across the cloud environment.

The collected information is forwarded to the data ingestion layer through log collectors, agents, and application programming interfaces. Since cloud environments generate events continuously, a streaming pipeline is used to receive data without waiting for manual collection. The incoming records are temporarily maintained in raw data storage so that original event details remain available for later investigation or reprocessing.

After ingestion, the data enters the processing and analysis engine. During preprocessing, incomplete or unnecessary values are cleaned, data formats are normalized, and important security characteristics are extracted. The processed information is then converted into a structured form that can be examined by the detection models. This stage improves data consistency and prevents noisy records from affecting the quality of threat analysis.

The anomaly detection module applies machine learning techniques such as Isolation Forest, Autoencoder, and LSTM to identify behaviour that differs from normal cloud operations. An unusual login attempt, abnormal traffic flow, unexpected resource usage, or suspicious sequence of events can therefore be recognized even when it does not exactly match a known attack signature. The detection results are exchanged with the Generative AI module, which studies relationships among events and adds contextual meaning to the identified abnormalities.

The Generative AI module acts as an intelligent interpretation layer within the architecture. It correlates related events, identifies possible threat patterns, explains the suspected attack, and produces

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

contextual security insights. Instead of presenting analysts with isolated technical alerts, the system attempts to describe how several activities may be connected. This helps reveal complex attacks that develop gradually across multiple cloud services.

Once an event has been analysed, the risk scoring and prioritization component estimates its seriousness. Alerts are ranked according to their likely impact and surrounding context, allowing high-risk incidents to receive immediate attention. Historical security information is stored in the security data lake, while known threat intelligence and previous attack knowledge are maintained in the knowledge base. These two repositories support deeper analysis and provide useful references for future security decisions.

The alert and response management layer converts detected threats into actionable incidents. Alerts are generated, enriched with contextual and risk information, and prioritized before a suitable response is recommended or automatically performed. The monitoring dashboard then presents real-time threat views, risk trends, reports, AI-generated attack insights, and overall system health. This gives the administrator or Security Operations Center analyst a clear view of current security conditions.

Finally, the administrator investigates important alerts, validates incidents, takes necessary action, and updates security policies. The outcome of these decisions is returned through a continuous feedback loop. This feedback allows the monitoring process to learn from previous incidents and adjust to new cloud behaviour over time. As a result, the architecture operates as an adaptive security cycle rather than a fixed detection mechanism, improving its ability to respond to emerging and changing cloud threats.

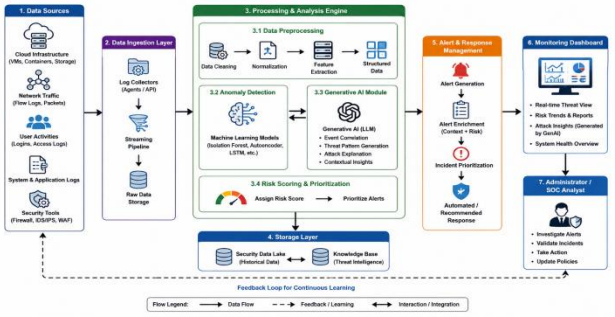

Fig 5.1: System Architecture

VI. IMPLEMENTATION

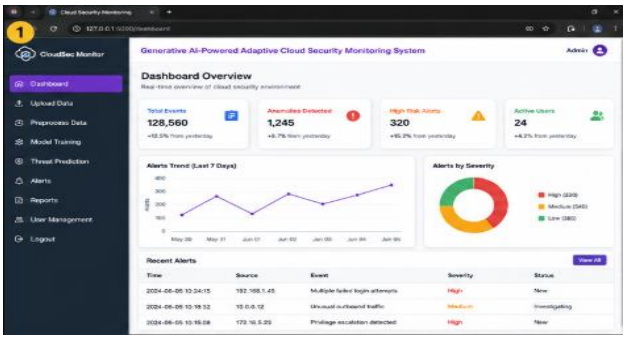

Fig 6.1: Dashboard

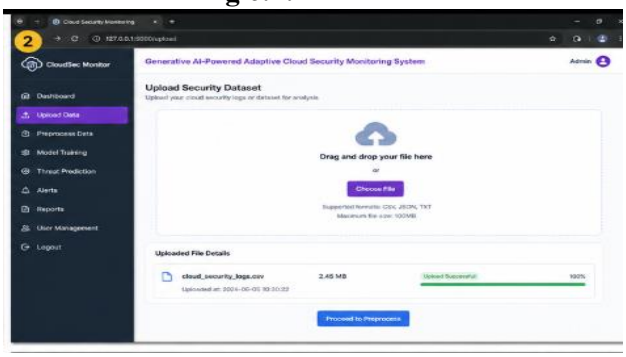

Fig 6.2: Uploading Dataset

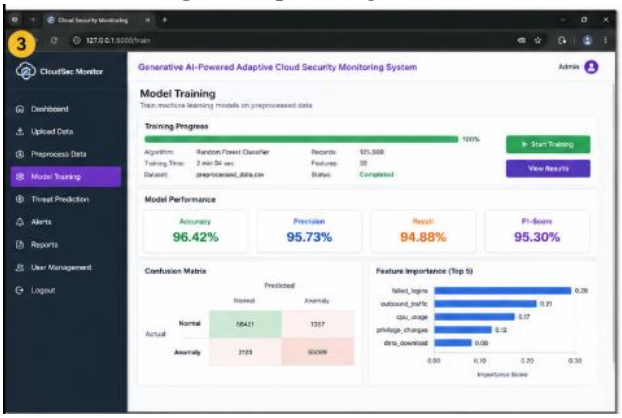

Fig 6.3: Model Training

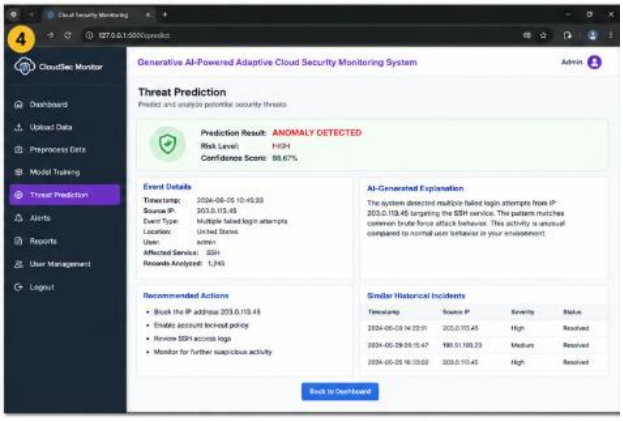

Fig 6.4: Threat Prediction

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

VII. CONCLUSION

The Generative AI-Powered Adaptive Cloud Security Monitoring System presents an intelligent approach to protecting modern cloud environments from changing and previously unknown cyber threats. The system brings together continuous data collection, preprocessing, anomaly detection, risk assessment, and generative AI-based threat interpretation within a unified security framework. Unlike conventional monitoring solutions that mainly depend on fixed rules and known signatures, the proposed approach examines behavioural changes and relationships among security events to identify suspicious activities more effectively. The use of Generative AI also helps transform complex alerts into understandable explanations and recommended responses, allowing security analysts to investigate incidents with better context. Through adaptive learning and continuous feedback, the monitoring process can improve as new attack patterns and cloud behaviours emerge. Overall, the proposed system offers a scalable and responsive security solution that can reduce alert overload, improve threat visibility, and support faster decision-making in dynamic cloud infrastructures.

VIII. FUTURE SCOPE

The future development of the Generative AI-Powered Adaptive Cloud Security Monitoring System can focus on making threat detection more autonomous, accurate, and suitable for large-scale cloud infrastructures. The system can be extended to support multi-cloud and hybrid environments, allowing security events from different platforms to be examined through a single monitoring framework. Future versions may integrate advanced large language models with real-time threat intelligence so that newly reported vulnerabilities and attack techniques can be considered during incident analysis. Federated learning can also be introduced to improve detection models across multiple organizations without directly sharing sensitive security data. Another useful extension would be autonomous response orchestration, where the system could isolate compromised resources, block suspicious access, rotate exposed credentials, or apply temporary security policies according to the detected risk. Explainable AI techniques may further improve the clarity of security decisions by showing the main factors behind each alert. With continued development, the framework could evolve into a self-improving cloud defence platform capable of predicting attack progression, adapting to new threats, and supporting security teams with faster and more reliable incident handling.

IX. REFERENCES

[1] M. A. Ferrag et al., “Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities,” Internet of Things and Cyber-Physical Systems, vol. 5, pp. 1–34, 2025. doi: 10.1016/j.iotcps.2025.01.001.

[2] N. O. Jaffal et al., “Large Language Models in Cybersecurity: A Survey of Applications, Vulnerabilities, and Defense Techniques,” AI, vol. 6, no. 9, 2025. doi: 10.3390/ai6090216.

[3] J. Zhang et al., “When LLMs Meet Cybersecurity: A Systematic Literature Review,” Cybersecurity, vol. 8, 2025. doi: 10.1186/s42400-025-00361-w.

[4] M. Uddin et al., “Generative AI Revolution in Cybersecurity: A Comprehensive Review of Threats, Opportunities and Future Directions,” Artificial Intelligence Review, vol. 58, 2025. doi: 10.1007/s10462-025-11219-5.

[5] W. Kasri et al., “From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity,” Computation, vol. 13, no. 2, 2025. doi: 10.3390/computation13020030.

[6] Y. Yao et al., “A Survey on Large Language Model Security and Privacy: The Good, the Bad, and the Ugly,” High-Confidence Computing, vol. 4, 2024. doi: 10.1016/j.hcc.2024.100211.

[7] F. Alwahedi et al., “Machine Learning Techniques for IoT Security: Current Research and Future Vision with Generative AI and Large Language Models,” Internet of Things and Cyber-Physical Systems, vol. 4, pp. 74–92, 2024. doi: 10.1016/j.iotcps.2023.12.003.

[8] A. R. Al-Ghuwairi et al., “Intrusion Detection in Cloud Computing Based on Time Series Anomalies Utilizing Machine Learning,” Journal of Cloud Computing, vol. 12, 2023. doi: 10.1186/s13677-023-00491-x.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[9] I. Jada and T. O. Mayayise, "The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome of a Systematic Literature Review," Data and Information Management, vol. 8, 2024. doi: 10.1016/j.dim.2023.100063.

[10] K. Orpak et al., "Generative AI and Cybersecurity," Maandblad voor Accountancy en Bedrijfseconomie, vol. 99, 2025. doi: 10.5117/mab.99.149299.

[11] J. Xu et al., "Large Language Models for Cyber Security: A Systematic Literature Review," ACM Computing Surveys, 2025. doi: 10.1145/3769676.

[12] N. Mohamed et al., "Artificial Intelligence and Machine Learning in Cybersecurity: A Deep Dive into State-of-the-Art Techniques and Future Paradigms," Knowledge and Information Systems, 2025. doi: 10.1007/s10115-025-02429-y.

[13] A. Hozouri et al., "A Comprehensive Survey on Intrusion Detection Systems with Advances in Machine Learning, Deep Learning and Emerging Cybersecurity Challenges," Discover Artificial Intelligence, vol. 5, 2025. doi: 10.1007/s44163-025-00578-1.

[14] A. Vassilev et al., "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," NIST AI 100-2e2025, National Institute of Standards and Technology, 2025. doi: 10.6028/NIST.AI.100-2e2025.

[15] B. C. Das, M. H. Amini, and Y. Wu, "Security and Privacy Challenges of Large Language Models: A Survey," ACM Computing Surveys, vol. 57, no. 6, 2025. doi: 10.1145/3712001. :contentReference[oaicite:0]{index=0}

[16] K. Ahi and S. Valizadeh, "Large Language Models and Generative AI in Cybersecurity and Privacy: A Survey of Dual-Use Risks, AI-Generated Malware, Explainability, and Defensive Strategies," Proc. IEEE Silicon Valley Cybersecurity Conf. (SVCC), 2025. doi: 10.1109/SVCC65277.2025.11133642. :contentReference[oaicite:1]{index=1}

[17] S. Tian et al., "Exploring the Role of Large Language Models in Cybersecurity: A Systematic Survey,"
2025. :contentReference[oaicite:2]{index=2}

[18] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41–50, 2018. doi: 10.1109/TETCI.2017.2772792.

[19] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019. doi: 10.1109/ACCESS.2019.2895334.

[20] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-Based Intrusion Detection Approach Using Machine Learning Techniques," Big Data Mining and Analytics, vol. 6, no. 3, pp. 311–320, 2023. doi: 10.26599/BDMA.2022.9020023.

[21] A. B. Nassif, M. A. Talib, Q. Nasir, and F. M. Dakalbab, "Machine Learning for Anomaly Detection: A Systematic Review," IEEE Access, vol. 9, pp. 78658–78700, 2021. doi: 10.1109/ACCESS.2021.3083060.

[22] S. Russell and P. Norvig, *Artificial Intelligence: A Modern Approach*, 4th ed. Hoboken, NJ, USA: Pearson, 2021.

[23] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[24] Y. Cao et al., "A Survey of AI-Generated Content (AIGC)," ACM Computing Surveys, vol. 57, no. 5, 2025. doi: 10.1145/3704262. :contentReference[oaicite:3]{index=3}

[25] S. Gökstorp, S. Katsikeas, and P. Johnson, "Machine Learning for Cybersecurity: A Comprehensive Literature Review," ACM Computing Surveys, vol. 58, no. 9, 2026. doi: 10.1145/3796543. :contentReference[oaicite:4]{index=4}