

An Intelligent Machine Learning Framework for Adaptive Cyber Threat Detection Across Multi-Cloud Computing Environments

¹Dr Vemuri Sudarsan Rao, ²Dr Kavitha Guda, ³Dr.Macha Sarada

¹Associate Professor, Department of Computer Science and Engineering, Sri Chaitanya Institute of Technology and Research, Khammam, Telangana, India

¹Email: sudharshan.cse2008@gmail.com

²Associate Professor, Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology, cheeryal(V), Medchal Dist, Hyderabad, Telangana -501301, India

²Email: kavitharddy.darshan@gmail.com

³Associate Professor, Department of Computer Science and Engineering (Artificial Intelligence and Machine Learning), Anurag Engineering College, Kodad, Suryapet, Telangana- 508206, India

³Email: saradaramaraok@gmail.com

ABSTRACT

The rapid expansion of cloud computing has encouraged enterprises to adopt multi-cloud architectures to improve service availability, workload distribution, scalability, and business continuity. Despite these advantages, managing security across multiple cloud providers remains a significant challenge because each platform generates diverse security logs, network events, and access records. The fragmented nature of these environments makes it difficult for conventional security solutions to correlate security incidents and detect sophisticated cyberattacks in a timely manner. Consequently, there is a growing need for intelligent security frameworks capable of providing unified threat analysis across heterogeneous cloud infrastructures. This study proposes an adaptive artificial intelligence-based threat detection framework that enhances cybersecurity in multi-cloud environments through automated data analysis and intelligent decision-making. The proposed framework aggregates security-related information from multiple cloud resources, preprocesses the collected data, extracts discriminative features, and applies supervised machine learning techniques to classify benign and malicious activities. By

learning behavioral characteristics from historical security events, the system effectively identifies anomalous network traffic, unauthorized authentication attempts, suspicious user behavior, privilege misuse, and other potential security threats. Unlike conventional rule-based approaches, the proposed framework continuously improves its detection capability by recognizing evolving attack patterns and reducing dependence on manually defined security rules. The effectiveness of the proposed framework is evaluated using standard machine learning performance metrics, including accuracy, precision, recall, F1-score, and false-positive rate. Experimental analysis demonstrates that intelligent learning models can significantly improve threat detection capability while minimizing false alarms and maintaining consistent performance in dynamic cloud environments. The proposed framework offers a scalable, efficient, and proactive security solution that strengthens cyber resilience, enables early threat identification, and supports secure service delivery across distributed multi-cloud computing platforms.

Keywords: Artificial Intelligence (AI), Anomaly Detection, Cloud Computing, Cybersecurity, Machine Learning (ML), Multi-Cloud Environment, Network

Security, Threat Detection, Threat Intelligence.

I. INTRODUCTION

Cloud computing has become a fundamental part of modern digital infrastructure by providing scalable computing resources, flexible storage, and on-demand services. Organizations increasingly rely on multiple cloud platforms rather than a single provider to improve service availability, reduce dependency on one infrastructure, and meet diverse operational requirements. This multi-cloud approach allows applications and workloads to be distributed across different cloud environments. Although it offers significant advantages, the distributed nature of multi-cloud infrastructure introduces additional security complexities that are difficult to address using conventional protection mechanisms.

Security management in a multi-cloud environment is challenging because each cloud platform may use different architectures, monitoring tools, access-control policies, logging formats, and security configurations. The lack of unified visibility makes it difficult for security teams to identify suspicious activities occurring across multiple platforms. Attackers may exploit misconfigured resources, compromised credentials, insecure interfaces, or communication channels between cloud services. Since security events are generated continuously and in large volumes, manual analysis and fixed rule-based detection systems may not provide timely identification of advanced or previously unknown threats.

Traditional intrusion and threat detection mechanisms mainly depend on predefined signatures, static rules, and known attack patterns. Such approaches can perform effectively against previously identified threats but often struggle with zero-day attacks, evolving attack techniques, and subtle behavioral anomalies. In a multi-cloud

setting, these limitations become more significant because malicious activities may be distributed across different cloud services and may not appear suspicious when analyzed independently. Therefore, an intelligent detection approach capable of examining diverse security information and discovering hidden relationships among events is required.

Artificial Intelligence (AI) and Machine Learning (ML) provide promising capabilities for strengthening security monitoring in complex cloud infrastructures. These technologies can process large volumes of network traffic, authentication records, system logs, user activities, and resource usage patterns to learn the characteristics of normal and abnormal behavior. By identifying deviations from expected patterns, AI-based models can detect suspicious activities that may not match existing attack signatures. The learning capability of such systems also supports adaptation to changing cloud workloads and newly emerging cyber threats. The proposed AI-Driven Threat Detection Framework for Multi-Cloud Environments aims to establish a centralized and intelligent security monitoring mechanism across heterogeneous cloud platforms. The framework gathers security-related data from multiple cloud environments, preprocesses the collected information, extracts relevant behavioral and network features, and applies intelligent classification or anomaly detection techniques. The detected activities are categorized according to their potential security risk, enabling suspicious events to be identified at an early stage.

The framework is intended to improve threat visibility, reduce false alerts, and support faster security decision-making. By correlating events generated from different cloud infrastructures, it can provide a broader understanding of coordinated attack behavior and potential security incidents. The

integration of automated threat analysis with multi-cloud monitoring can reduce the burden on security administrators while improving the consistency and responsiveness of the detection process.

Overall, the proposed work focuses on developing an adaptive security framework capable of addressing the dynamic and distributed nature of multi-cloud computing. Through intelligent data analysis and automated threat recognition, the system seeks to enhance the protection of cloud resources, sensitive information, and digital services. The framework contributes toward building a more resilient multi-cloud ecosystem in which potential threats can be identified and assessed before they cause significant operational or data-related damage.

II. LITERATURE SURVEY

1. Title: Machine Learning for Anomaly Detection and Categorization in Multi-Cloud Environments

Authors: Tara Salman, D. Bhamare, A. Erbad, R. Jain, and M. Samaka

Abstract: This study investigates the use of machine learning for identifying and categorizing abnormal activities in multi-cloud infrastructures. Unlike conventional approaches that focus only on determining whether an event is normal or malicious, the work also classifies detected anomalies into meaningful categories. The proposed approach analyzes network-related behavior using machine learning techniques and demonstrates the suitability of intelligent models for heterogeneous cloud environments. The research highlights the importance of automated anomaly categorization for improving incident analysis and accelerating security responses across multiple cloud platforms.

2. Title: Emergent (In)Security of Multi-Cloud Environments

Authors: Morgan Reece, Theodore Lander Jr., Sudip Mittal, Nidhi Rastogi, Josiah

Dijkstra, and Andy Sampson

Abstract: This research examines the expanding security risks associated with the adoption of multi-cloud computing. As organizational workloads are distributed among several cloud service providers, the number of attack paths, vulnerabilities, and configuration challenges also increases. The authors apply established risk-analysis techniques to identify and prioritize significant multi-cloud threats and corresponding defensive measures. The study finds that authentication mechanisms and architectural design represent particularly important risk areas. The work provides useful guidance for prioritizing security investments and designing stronger protection strategies for distributed cloud environments.

3. Title: AI-Enabled System for Efficient and Effective Cyber Incident Detection and Response in Cloud Environments

Authors: Mohammed Ashfaq M. Farzaan, Mohamed Chahine Ghanem, Ayman El-Hajjar, and Deepthi N. Ratnayake

Abstract: This paper proposes an artificial intelligence-based system for detecting and responding to cyber incidents in cloud environments. The framework combines network traffic classification, web intrusion detection, and post-incident malware analysis within an integrated security architecture. Machine learning and deep learning models are used to automate the identification of malicious behavior and improve incident-handling efficiency. The study reports strong results for network traffic classification and malware analysis and demonstrates deployment across cloud platforms. The findings indicate that AI-based security systems can provide scalable and automated cyber defense for complex cloud infrastructures.

4. Title: AI-Driven Anomaly Detection in Cloud Computing Environments

Authors: Research study on AI-based cloud

anomaly detection

Abstract: This study reviews the growing application of artificial intelligence for anomaly detection in cloud computing systems. It examines supervised learning, unsupervised learning, deep learning, and hybrid approaches used to recognize deviations from expected cloud behavior. The research emphasizes that AI-based models can process large volumes of dynamic data and identify security incidents that conventional static mechanisms may overlook. It also discusses the role of anomaly detection in security improvement, resource optimization, and operational monitoring while identifying concerns related to scalability, model accuracy, and false alarms.

5. Title: AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience

Authors: Shamnad Mohamed Shaffi, Sunish Vengathattil, Jezeena Nikarhil Sidhick, and Resmi Vijayan

Abstract: This paper explores the contribution of artificial intelligence to modern cloud security through intelligent threat detection, predictive analysis, and automated response. The authors explain how machine learning can examine extensive network activities and identify abnormal behavior before it develops into a serious security breach. The study also considers behavior-based detection, AI-supported encryption, and adaptive defense mechanisms. In addition to technical advantages, the research discusses challenges involving privacy, algorithmic bias, regulatory compliance, and reliability. It concludes that AI can substantially strengthen cloud resilience when implemented through scalable and responsible security architectures.

6. Title: Emerging Security Challenges and AI-Driven Solutions in Multi-Cloud

and Hybrid Environments

Author: Sheshananda Reddy Kandula

Abstract: This work analyzes major security problems found in multi-cloud and hybrid computing environments and investigates the potential of AI-based solutions. The study addresses challenges arising from fragmented security policies, heterogeneous infrastructure, distributed data, and increasing attack complexity. Artificial intelligence is presented as a mechanism for improving threat detection, security automation, policy management, and intelligent decision-making. The research highlights the need for unified monitoring and adaptive protection strategies capable of operating across diverse cloud platforms. It provides important insights into the development of more coordinated and scalable multi-cloud defense mechanisms.

III. EXISTING SYSTEM

The existing security systems used in multi-cloud environments mainly depend on traditional mechanisms such as signature-based intrusion detection, predefined security rules, firewalls, access control policies, and individual monitoring tools provided by different cloud service providers. These mechanisms generally operate independently within each cloud platform and analyze security events based on known attack patterns or fixed threshold values. Security logs, network traffic, user activities, and resource events generated across different cloud infrastructures are often monitored separately, resulting in fragmented visibility of the overall security environment. Although conventional systems are effective in detecting previously identified threats, they face difficulties in recognizing zero-day attacks, advanced persistent threats, insider activities, and coordinated attacks that span multiple cloud platforms. The large volume and heterogeneous nature of multi-cloud security data further increase the complexity of

manual monitoring and incident analysis. Moreover, differences in logging formats, security policies, and monitoring mechanisms among cloud providers make centralized threat identification difficult. As a result, existing systems may generate high false-positive rates, experience delays in detecting sophisticated attacks, and require significant involvement from security administrators. These limitations create a need for a unified, adaptive, and intelligent threat detection mechanism capable of analyzing security information across the entire multi-cloud infrastructure.

IV. PROPOSED SYSTEM

The proposed system introduces an AI-driven threat detection framework designed to provide unified and intelligent security monitoring across multi-cloud environments. The framework collects and integrates security-related information, including network traffic, authentication records, user activities, system logs, and resource behavior, from multiple cloud platforms into a centralized analysis environment. The collected data is preprocessed to remove inconsistencies, handle missing values, normalize features, and transform heterogeneous cloud records into a suitable format for intelligent analysis. Machine learning and AI-based models are then applied to learn normal behavioral patterns and identify suspicious deviations that may indicate unauthorized access, network intrusions, insider threats, malicious activities, or previously unseen attacks. Unlike conventional rule-based mechanisms, the proposed framework can analyze complex relationships among events generated across different cloud infrastructures and support the detection of coordinated threats. The system classifies detected activities according to their security risk and provides timely alerts to assist administrators in taking appropriate actions. By combining centralized monitoring,

automated analysis, and adaptive threat recognition, the proposed system aims to improve detection accuracy, reduce false alarms, shorten response time, and provide better visibility across the complete multi-cloud infrastructure.

V. SYSTEM ARCHITECTURE

The system architecture of the AI-Driven Threat Detection Framework for Multi-Cloud Environments is designed to provide centralized, intelligent, and continuous security monitoring across heterogeneous cloud infrastructures. The architecture integrates multiple cloud platforms, a data ingestion layer, an AI/ML engine, external threat intelligence sources, alert and visualization mechanisms, and security administrators. The overall information flow begins with the collection of security data from different cloud environments and continues through preprocessing, intelligent analysis, threat scoring, alert generation, and administrative response.

The Multi-Cloud Environments layer represents the primary data sources of the proposed framework. It includes infrastructures such as AWS Cloud, Microsoft Azure, Google Cloud, and other cloud services. Each platform continuously produces large volumes of security-related information. AWS contributes VPC flow logs, CloudTrail logs, and security group information, while Microsoft Azure provides activity logs, NSG flow logs, and monitoring data. Google Cloud supplies VPC flow logs, administrative activity logs, and cloud monitoring records. Collecting information from multiple platforms enables the framework to obtain a unified view of activities occurring throughout the distributed cloud infrastructure.

The collected security information is transferred to the Data Ingestion Layer, which acts as an intermediary between the multi-cloud platforms and the intelligent detection engine. Log collectors and software

agents gather records from the connected cloud resources and forward them through a streaming ingestion mechanism. This approach supports the continuous processing of newly generated security events. Secure transmission mechanisms are used to protect the collected information while it moves from individual cloud platforms to the centralized AI/ML processing environment. The AI/ML Engine forms the core of the proposed architecture. Its first stage is data preprocessing, where raw cloud records are prepared for intelligent analysis. Data cleaning removes incomplete, duplicated, or irrelevant entries, while normalization converts numerical values into a consistent scale. Feature extraction identifies security-relevant characteristics from network and user activities, and data transformation converts heterogeneous records into a common analytical representation. These preprocessing operations improve data quality and ensure that information obtained from different cloud platforms can be analyzed effectively.

After preprocessing, the prepared information is passed to the AI/ML Models stage. The framework applies anomaly detection to discover activities that deviate from established normal behavior. Classification models categorize security events into normal and malicious classes or specific threat categories. Behavioral analysis examines changes in user, network, and resource activity, while deep learning models identify complex and hidden attack patterns within large-scale security data. The combined use of these intelligent techniques improves the capability of the framework to recognize both known and previously unseen cyber threats.

The detected suspicious activities are then processed through the Threat Detection and Scoring stage. Risk scoring assigns a measurable threat level to each detected event according to its characteristics and

potential impact. Threat correlation connects related events generated across different cloud platforms to identify coordinated attacks. Attack pattern identification determines whether the observed activities resemble known or emerging malicious behavior, while severity assessment classifies incidents according to their level of risk. This stage helps prioritize serious threats and reduces unnecessary attention to low-risk events.

The architecture also incorporates a Threat Intelligence Integration component to strengthen the accuracy and contextual awareness of the detection process. Indicators of compromise and external security feeds are used to compare detected activities with known malicious patterns. Reputation analysis evaluates suspicious users, network addresses, domains, and other entities, while contextual enrichment adds relevant information to the detected incident. The framework receives additional knowledge from global threat feeds, vulnerability databases, open-source intelligence sources, and dark web monitoring services. This external intelligence helps the system recognize emerging threats that may not yet exist within the locally collected cloud data.

Once a threat is confirmed, the results are transferred to the Output Layer. The alert and response component generates real-time warnings, supports automated response actions, creates incident tickets, and delivers notifications through appropriate communication channels. Security findings are also presented through a dashboard and visualization interface containing threat overviews, attack trends, risk heatmaps, and information about high-priority threats. These visual representations allow security personnel to understand the overall security condition of the multi-cloud environment quickly.

Finally, the Administrator or Security Operations Center (SOC) Team receives the analyzed threat information and performs the necessary security actions. Administrators can investigate suspicious incidents, analyze their origin and impact, respond to confirmed attacks, and take corrective measures to protect cloud resources. Through the integration of multi-cloud data collection, AI-powered detection, threat intelligence, automated alerts, and centralized visualization, the proposed architecture provides improved visibility across cloud platforms, real-time threat monitoring, reduced false positives, faster security response, and a scalable and adaptive protection mechanism for modern multi-cloud environments.

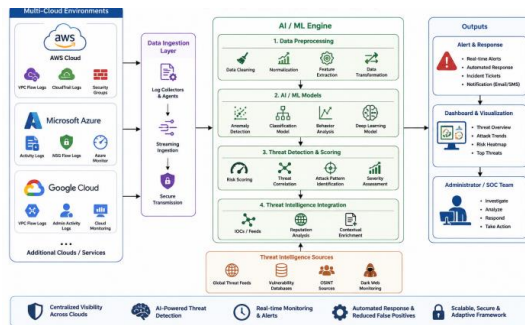


Fig 5.1: System Architecture

VI. IMPLEMENTATION

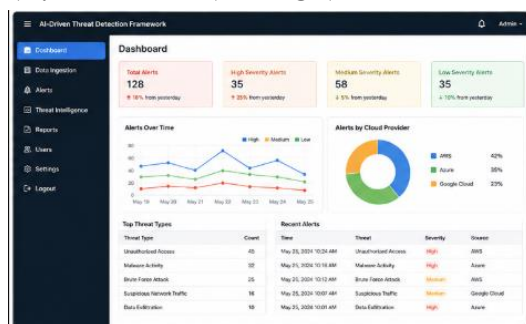


Fig 6.1: Dashboard

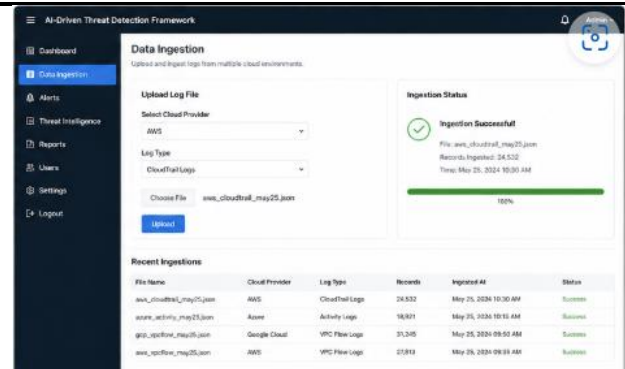


Fig 6.2: Data Uploading

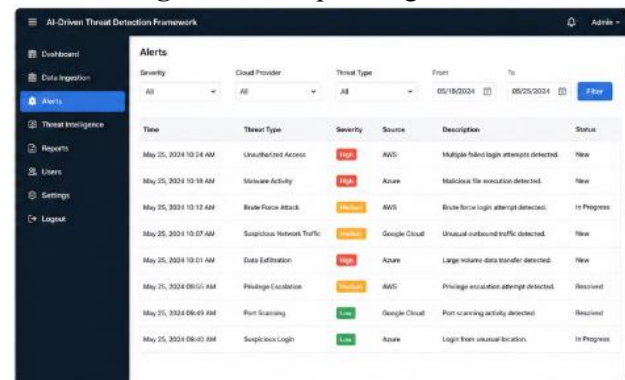


Fig 6.3: Detected Alerts

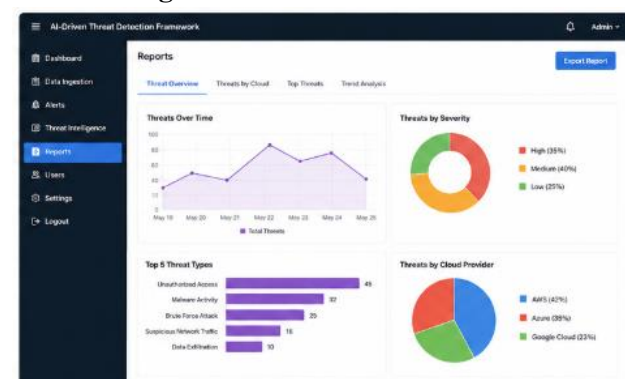


Fig 6.4: Threat Analytics

VII. CONCLUSION

The AI-Driven Threat Detection Framework for Multi-Cloud Environments provides an intelligent and unified approach to addressing the growing security challenges of distributed cloud infrastructures. The proposed system integrates security information from multiple cloud platforms and applies data preprocessing, anomaly detection, classification, behavioral analysis, threat correlation, and risk assessment to identify suspicious activities more effectively. By combining AI-based analysis

with external threat intelligence, the framework is capable of detecting unauthorized access, malware activity, brute-force attempts, suspicious network behavior, data exfiltration, and other emerging threats. The centralized dashboard, real-time alerts, and analytical reports improve security visibility and help administrators understand and respond to incidents quickly. Compared with conventional rule-based and isolated monitoring approaches, the proposed framework offers greater adaptability, reduced manual effort, improved detection capability, and better support for coordinated threat identification across cloud platforms. Thus, the system establishes a scalable and responsive security mechanism that can strengthen cyber resilience and support the safe management of modern multi-cloud environments.

VIII. FUTURE SCOPE

The future scope of the AI-Driven Threat Detection Framework for Multi-Cloud Environments can be extended by incorporating advanced deep learning, federated learning, reinforcement learning, and explainable AI techniques to improve detection accuracy, adaptability, and transparency. Federated learning can enable different cloud platforms to collaboratively improve threat detection models without directly sharing sensitive organizational data, while explainable AI can provide understandable reasons behind each security alert and risk score. The framework can also be enhanced with automated incident response and self-healing capabilities to isolate compromised resources, block malicious connections, revoke suspicious access, and restore affected services with minimal human intervention. Integration with zero-trust security architectures, blockchain-based audit mechanisms, container and serverless workload monitoring, and advanced threat intelligence sources can further strengthen protection. In

addition, future implementations can focus on detecting adversarial attacks against AI models, predicting threats before actual exploitation, supporting edge-cloud infrastructures, and developing lightweight real-time models capable of processing large-scale security streams. These advancements can transform the proposed framework into a more autonomous, explainable, privacy-aware, and proactive security solution for increasingly complex multi-cloud ecosystems.

REFERENCES

- [1] T. Salman, D. Bhamare, A. Erbad, R. Jain, and M. Samaka, "Machine learning for anomaly detection and categorization in multi-cloud environments," in Proc. 4th IEEE Int. Conf. Cyber Security and Cloud Computing (CSCloud), 2017, pp. 97–103. doi: 10.1109/CSCloud.2017.15.
- [2] A. M. Abdallah and M. A. Al-Sinani, "Cloud network anomaly detection using machine and deep learning techniques—Recent research advancements," IEEE Access, vol. 12, pp. 52306–52334, 2024. doi: 10.1109/ACCESS.2024.3387164.
- [3] M. Cantone, C. Marrocco, and A. Bria, "Machine Learning in Network Intrusion Detection: A Cross-Dataset Generalization Study," IEEE Access, vol. 12, pp. 144489–144508, 2024. doi: 10.1109/ACCESS.2024.3472907.
- [4] F. Wang and S. Xie, "Cybersecurity in Cloud Computing: AI-Driven Intrusion Detection and Mitigation Strategies," IEEE Access, vol. 13, pp. 108051–108058, 2025. doi: 10.1109/ACCESS.2025.3580569.
- [5] H. Holla, S. R. Polepalli, and A. A. Sasikumar, "Adversarial Threats to Cloud IDS: Robust Defense With Adversarial Training and Feature Selection," IEEE Access, vol. 13, pp. 84992–85003, 2025. doi:

10.1109/ACCESS.2025.3567038.

[6] S. Gong, J. Cho, and K. K. Choi, "Heterogeneous Data Fusion: A Scalable Approach to Intrusion Detection," *IEEE Access*, vol. 13, pp. 181058–181070, 2025. doi: 10.1109/ACCESS.2025.3620722.

[7] 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.

[8] L. Ashiku and C. Dagli, "Network intrusion detection system using deep learning," *Procedia Computer Science*, vol. 185, pp. 239–247, 2021. doi: 10.1016/j.procs.2021.05.025.

[9] S. Lata, D. Singh, and M. M. S. Beg, "Intrusion detection system in cloud environment: Literature survey and future research directions," *International Journal of Information Management Data Insights*, vol. 2, no. 2, Art. no. 100134, 2022. doi: 10.1016/j.jjime.2022.100134.

[10] E. E. Abdallah and A. E. Abdallah, "Intrusion detection systems using supervised machine learning techniques: A survey," *Procedia Computer Science*, vol. 201, pp. 205–212, 2022. doi: 10.1016/j.procs.2022.03.029.

[11] H. Attou, A. Guezzaz, S. Benkirane, M. Azrou, 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.

[12] Y. N. Kunang, S. Nurmaini, D. Stiawan, and B. Y. Suprpto, "Attack classification of an intrusion detection system using deep learning and hyperparameter optimization," *Journal of Information Security and*

Applications, vol. 58, Art. no. 102804, 2021. doi: 10.1016/j.jisa.2021.102804.

[13] D. K. K. Reddy, H. S. Behera, J. Nayak, B. Naik, U. Ghosh, and P. Sharma, "Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment," *Journal of Information Security and Applications*, vol. 60, Art. no. 102866, 2021. doi: 10.1016/j.jisa.2021.102866.

[14] M. Idhammad, K. Afdel, and M. Belouch, "Distributed intrusion detection system for cloud environments based on data mining techniques," *Procedia Computer Science*, vol. 127, pp. 35–41, 2018. doi: 10.1016/j.procs.2018.01.095.

[15] M. A. Ambusaidi, X. He, P. Nanda, and Z. Tan, "Building an intrusion detection system using a filter-based feature selection algorithm," *IEEE Transactions on Computers*, vol. 65, no. 10, pp. 2986–2998, 2016. doi: 10.1109/TC.2016.2519914.

[16] 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.

[17] 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.

[18] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things," *Journal of Network and Computer*

Applications, vol. 84, pp. 25–37, 2017. doi:
10.1016/j.jnca.2017.02.009.

[19] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, “Deep recurrent neural network for IoT intrusion detection system,” *Simulation Modelling Practice and Theory*, vol. 101, Art. no. 102031, 2020. doi:
10.1016/j.simpat.2019.102031.

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

[21] F. Chollet, *Deep Learning with Python*, 2nd ed. Shelter Island, NY, USA: Manning Publications, 2021.

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

[23] P. Kairouz et al., “Advances and Open Problems in Federated Learning,” *Foundations and Trends in Machine Learning*, vol. 14, nos. 1–2, pp. 1–210, 2021. doi: 10.1561/22000000083.

[24] R. L. L. Picot, F. Gohring de Magalhaes, A. Shahnejat Bushehri, M. Ben Atti, G. Nicolescu, and A. Quintero, “Protocol-Agnostic and Packet-Based Intrusion Detection Using a Multi-Layer Deep-Learning Architecture at the Network Edge,” *IEEE Access*, vol. 13, pp. 57867–57877, 2025. doi: 10.1109/ACCESS.2025.3555201.

[25] F. Al-Quayed, Z. Ahmad, and M. Humayun, “A Situation-Based Predictive Approach for Cybersecurity Intrusion Detection and Prevention Using Machine Learning and Deep Learning Algorithms in Wireless Sensor Networks of Industry 4.0,” *IEEE Access*, vol. 12, 2024. doi: 10.1109/ACCESS.2024.3372187.