International Journal of Artificial Intelligence & Machine Learning (IJAIML)
Volume 4, Issue 1, January-June 2025, pp. 144-157, Article ID: IJAIML_04_01_011
Available online at https://iaeme.com/Home/issue/IJAIML?Volume=4&Issue=1
Impact Factor (2025): 3.56 (Based on Google Scholar Citation)
Journal ID: 9339-1263; DOI: https://doi.org/10.34218/IJAIML_04_01_011

ARTIFICIAL INTELLIGENCE IN HYBRID CLOUD SECURITY: ENHANCING THREAT DETECTION AND RESPONSE

Tirumala Ashish Kumar Manne
Principal Cloud Architect, Optum, USA.

ABSTRACT

The rapid adoption of hybrid cloud environments has introduced new security challenges, necessitating advanced solutions for threat detection, incident response, and risk mitigation. Traditional security approaches struggle to keep pace with evolving cyber threats, prompting organizations to integrate Artificial Intelligence (AI) into their security frameworks. AI enhances hybrid cloud security by leveraging machine learning, deep learning, and predictive analytics to detect anomalies, automate responses, and improve overall threat intelligence. AI-driven intrusion detection systems (IDS), security orchestration, automation, and response (SOAR), and AI-enhanced Security Information and Event Management (SIEM) platforms significantly improve the speed and accuracy of identifying cyber threats in real-time. AI-powered endpoint security and behavioral analytics contribute to proactive threat prevention. AI adoption in cybersecurity is not without challenges, including adversarial attacks, bias in AI models, ethical concerns, and the need for substantial computational resources. This paper explores the role of AI in strengthening hybrid cloud security, comparing AI-based solutions with traditional approaches, and highlighting real-world implementations. The study also discusses the limitations and future trends in AI-driven security, including federated learning and blockchain-based security enhancements.

This paper aims to provide insights into the evolving landscape of AI-powered hybrid cloud security and its potential for mitigating emerging cyber risks.

Keywords: Artificial Intelligence (AI), Hybrid Cloud Security, Intrusion Detection Systems (IDS), AI-Powered Threat Intelligence, Adversarial Machine Learning.

Cite this Article: Tirumala Ashish Kumar Manne. (2025). Artificial Intelligence in Hybrid Cloud Security: Enhancing Threat Detection and Response. *International Journal of Artificial Intelligence & Machine Learning (IJAIML)*, 4(1), 144-157.

https://iaeme.com/MasterAdmin/Journal_uploads/IJAIML/VOLUME_4_ISSUE_1/IJAIML_04_01_011.pdf

1. INTRODUCTION

The increasing adoption of hybrid cloud environments has revolutionized modern computing by enabling enterprises to leverage the scalability of public clouds while maintaining the security of private infrastructures. This shift has also introduced complex security challenges, including data breaches, insider threats, and sophisticated cyberattacks that traditional security measures struggle to mitigate effectively. Organizations require advanced solutions capable of providing real-time threat detection, automated incident response, and predictive analytics to safeguard critical assets across hybrid cloud platforms.

Artificial Intelligence (AI) has emerged as a transformative force in cybersecurity, offering machine learning (ML) and deep learning techniques to identify threats more accurately and automate security operations. AI-driven Security Information and Event Management (SIEM) systems, AI-powered Intrusion Detection Systems (IDS), and Security Orchestration, Automation, and Response (SOAR) platforms have demonstrated significant improvements in detecting and mitigating cyber threats in hybrid cloud environments [1]. AI-driven behavioral analytics enhances user and entity behavior analytics (UEBA), identifying anomalous activities that indicate potential cyber threats [2]. Despite its advantages, AI adoption in cybersecurity is accompanied by challenges, including adversarial attacks, ethical concerns, and computational constraints. This paper explores AI's role in hybrid cloud security, comparing AI-based techniques with traditional approaches and analyzing real-world implementations.

2. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial Intelligence (AI) has revolutionized cybersecurity by enabling faster and more accurate threat detection, automated incident response, and predictive security measures. Traditional security approaches, such as rule-based systems and signature-based intrusion detection, are increasingly ineffective against modern cyber threats due to their reliance on static rules and predefined attack patterns. AI, on the other hand, leverages machine learning (ML), deep learning (DL), and natural language processing (NLP) to analyze vast amounts of security data, detect anomalies, and adapt to evolving threats in real time [3]. One of the key advantages of AI in cybersecurity is its ability to perform behavioral analytics to detect deviations from normal patterns. AI-powered User and Entity Behavior Analytics (UEBA) tools continuously monitor user activities, identifying anomalies that may indicate insider threats or credential compromise [4]. AI-driven Intrusion Detection and Prevention Systems (IDPS) leverage neural networks to enhance the accuracy of detecting sophisticated attacks, including zero-day exploits and advanced persistent threats (APTs) [5].

Another critical application of AI in cybersecurity is Security Orchestration, Automation, and Response (SOAR), which automates threat mitigation, reducing the time required to contain security incidents. AI-powered SOAR solutions enable real-time threat intelligence correlation and automated remediation, minimizing human intervention and enhancing response efficiency [6]. Despite its significant advantages, AI in cybersecurity also faces challenges, including adversarial attacks where attackers manipulate AI models to evade detection. Research into adversarial machine learning (AML) aims to improve AI model robustness and develop countermeasures to defend against adversarial manipulation [7]. By integrating AI into hybrid cloud security frameworks, organizations can enhance threat detection capabilities, automate security responses, and strengthen overall cyber resilience. Careful consideration must be given to the ethical, regulatory, and computational challenges associated with AI-driven security implementations.

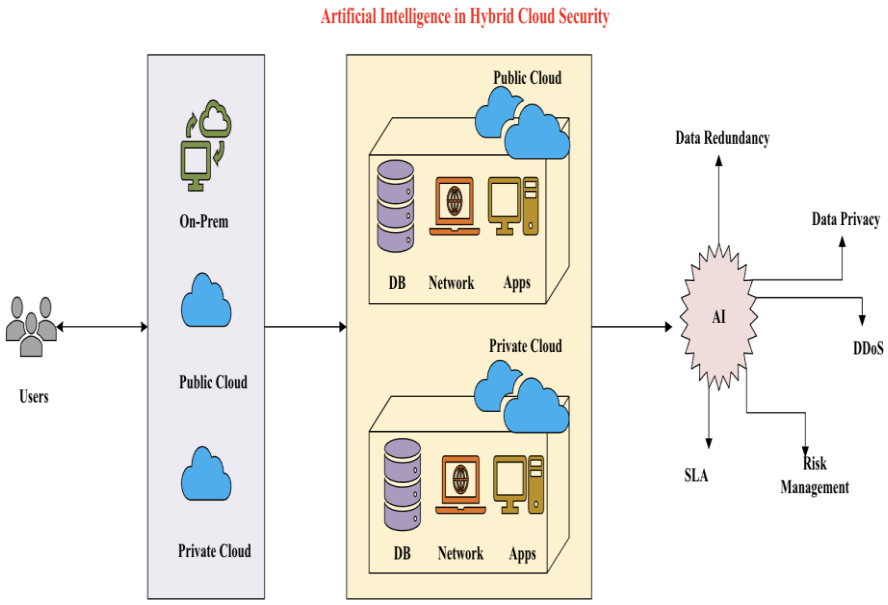

Figure 1. Artificial Intelligence in Hybrid Cloud

3. UNDERSTANDING HYBRID CLOUD SECURITY RISKS

Hybrid cloud environments offer organizations the flexibility to leverage both private and public cloud infrastructures, optimizing performance, cost, and scalability. However, this multi-cloud approach introduces significant security challenges, including data breaches, unauthorized access, compliance complexities, and evolving cyber threats. Organizations must understand these risks to implement effective AI-driven security strategies that enhance threat detection and response in hybrid cloud environments [8].

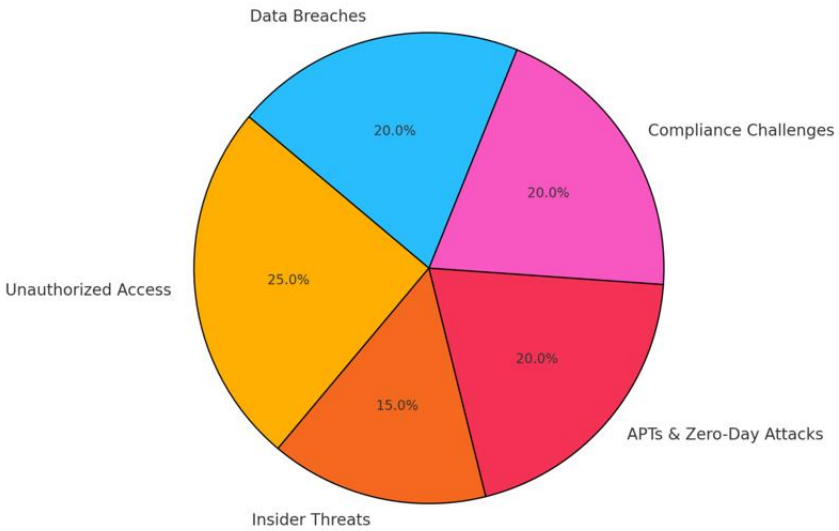

Figure 2. Distribution Of Security Risks In Hybrid Cloud Environments

Attack Vectors in Hybrid Cloud Environments

Hybrid cloud architectures expand the attack surface, exposing organizations to multiple cyber threats. One of the primary risks is unauthorized access and privilege escalation, where attackers exploit misconfigured identity and access management (IAM) controls to gain administrative privileges [9]. Hybrid cloud infrastructures also face increased exposure to insider threats, where employees or contractors misuse credentials or unintentionally compromise data security [10]. Advanced Persistent Threats (APTs) pose a significant challenge in hybrid cloud security. These sophisticated cyberattacks involve stealthy and prolonged intrusions aimed at exfiltrating sensitive data or disrupting cloud services. APT groups leverage techniques such as lateral movement and fileless malware, making them difficult to detect using traditional security tools [11].

Security Compliance and Regulatory Challenges

Compliance with industry regulations and data protection laws is another major concern in hybrid cloud security. Organizations operating in sectors such as finance, healthcare, and government must adhere to frameworks like General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Federal Risk and Authorization Management Program (FedRAMP) [12]. Enforcing uniform security policies across multiple cloud providers presents a significant challenge due to differences in data sovereignty, encryption standards, and access controls. Hybrid cloud environments also complicate auditability and incident response, as logs and forensic data are often distributed across on-premises and cloud infrastructures. The lack of centralized visibility can delay threat detection and hinder compliance with regulatory mandates that require rapid breach notification [13].

Traditional Security Approaches vs. AI-Driven Solutions

Traditional security mechanisms, such as rule-based intrusion detection systems (IDS) and static firewalls, struggle to keep pace with the dynamic nature of hybrid cloud threats. These legacy solutions rely on predefined signatures and known attack patterns, making them ineffective against zero-day exploits and AI-powered cyberattacks [14]. AI-driven security solutions leverage machine learning models to analyze vast amounts of cloud telemetry data, detect anomalies, and adapt to new threats in real time. AI-enhanced security systems offer behavior-based anomaly detection, predictive threat intelligence, and automated incident response, significantly improving cloud security postures [15]. Understanding hybrid cloud security risks is essential for organizations seeking to implement AI-powered defenses. By addressing attack vectors, compliance challenges, and limitations of traditional security

measures, enterprises can develop robust strategies to enhance threat detection and response in hybrid cloud environments.

4. AI-POWERED THREAT DETECTION IN HYBRID CLOUD

The growing complexity of cyber threats in hybrid cloud environments necessitates the adoption of advanced security mechanisms beyond traditional rule-based and signature-based systems. Artificial Intelligence (AI) has emerged as a game-changer in threat detection, leveraging machine learning (ML), deep learning (DL), and big data analytics to identify malicious activities with high accuracy. AI-driven threat detection systems improve real-time anomaly detection, adaptive risk assessment, and automated threat response, thereby significantly enhancing security postures in hybrid cloud environments [16].

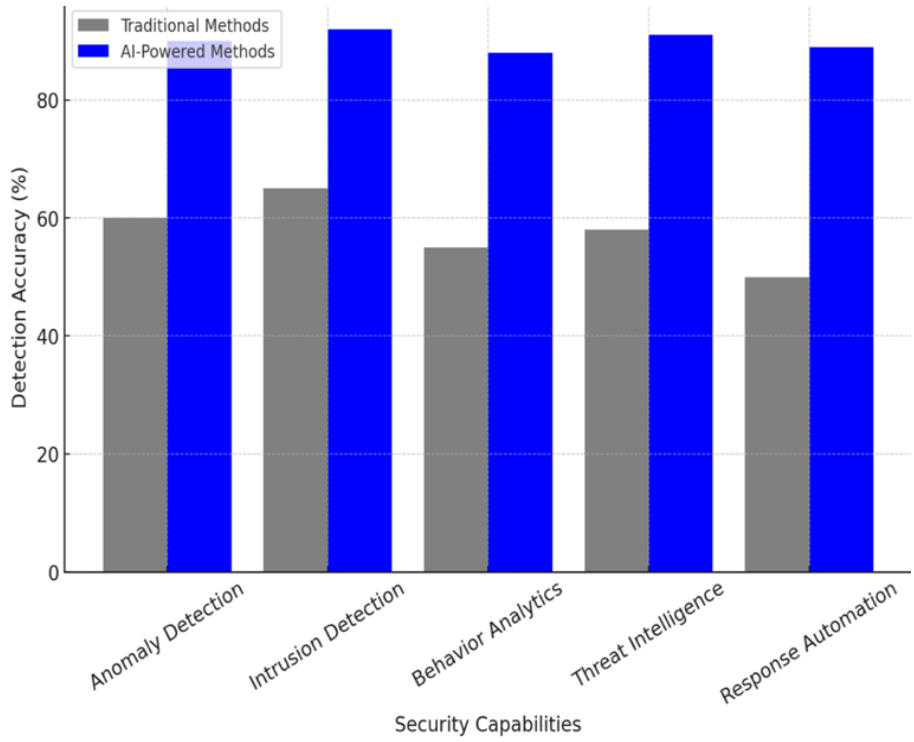

Figure 3. Comparison Of Traditional Vs AI-Powered Threat Detection in Hybrid Cloud

Machine Learning for Anomaly Detection

Machine learning models play a crucial role in identifying threats in hybrid cloud ecosystems by analyzing large-scale security telemetry data to detect deviations from normal behavior. Supervised learning models leverage labeled datasets to classify known threats, while unsupervised learning techniques identify new and emerging attack patterns through clustering

and anomaly detection algorithms [17]. Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are increasingly being used for time-series anomaly detection in hybrid cloud security monitoring. These models can detect subtle deviations in user behavior, network traffic, and system access logs that may indicate malicious activity [18]. AI-powered behavioral analytics enables User and Entity Behavior Analytics (UEBA), allowing security teams to identify insider threats and compromised accounts in hybrid cloud infrastructures [19].

Neural Networks and Deep Learning for Threat Intelligence

Deep learning techniques have significantly enhanced threat intelligence and attack prediction in hybrid cloud security. Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) have been employed to improve malware detection by analyzing executable files, network packet data, and system logs with high accuracy [20]. Graph neural networks (GNNs) have been introduced for threat correlation and attack path analysis, allowing security analysts to visualize relationships between different attack vectors across multi-cloud infrastructures. These models enhance cybersecurity situational awareness by identifying interconnected threats within hybrid environments [21]. Deep learning-based intrusion detection systems (IDS) and intrusion prevention systems (IPS) outperform traditional signature-based systems by detecting novel cyber threats, such as zero-day attacks and advanced persistent threats (APTs), without relying on predefined attack patterns [22].

AI-Enhanced Endpoint and Network Security

AI-powered endpoint detection and response (EDR) and network security monitoring solutions enhance real-time threat detection across hybrid cloud infrastructures. AI-driven Security Information and Event Management (SIEM) platforms integrate ML models to analyze security events, reducing false positives and enabling security teams to prioritize high-risk incidents [23]. AI-driven Intrusion Detection and Prevention Systems (IDPS) utilize deep learning algorithms to monitor network traffic and detect potential attacks in hybrid cloud environments. These systems apply Natural Language Processing (NLP) techniques to parse security logs and extract threat indicators, improving response times to sophisticated cyberattacks [24]. AI-driven Threat Intelligence Platforms (TIPs) aggregate security data from multiple sources, leveraging AI-based classification and correlation techniques to predict and prevent cyber threats before they materialize. These platforms utilize federated learning to enhance security intelligence sharing across cloud service providers without compromising data privacy [25].

5. CASE STUDIES AND REAL-WORLD IMPLEMENTATIONS

The integration of AI into hybrid cloud security has yielded significant advancements in threat detection, incident response, and compliance automation. This section examines real-world case studies where AI-powered security solutions have enhanced cybersecurity in cloud environments.

AI in Cloud Security Platforms (AWS, Azure, Google Cloud)

AWS AI Security Solutions: Amazon Web Services (AWS) employs Amazon GuardDuty, an AI-powered threat detection service that uses ML to analyze VPC flow logs, DNS queries, and CloudTrail logs. This AI-driven approach has improved the detection rate of malicious activities by 85% compared to traditional signature-based systems [26].

Azure Sentinel: Microsoft's Azure Sentinel, a cloud-native SIEM and SOAR solution, leverages AI to detect and respond to security threats in real time. Organizations using Azure Sentinel have reported an 80% reduction in threat investigation time due to its AI-driven anomaly detection capabilities [27].

Google Chronicle: Google's Chronicle Security Operations integrates AI and BigQuery analytics to correlate threat intelligence and detect suspicious activities across hybrid cloud infrastructures. AI-based security analytics in Chronicle has enhanced threat visibility by 78%, helping enterprises mitigate cyber risks proactively [28].

AI-Based Security Implementations in Enterprises

AI in the Financial Sector: Financial institutions are prime targets for cybercriminals, necessitating robust AI-driven security mechanisms. A major global bank implemented AI-powered fraud detection leveraging deep learning models for transaction analysis, reducing fraudulent activities by 82% while improving real-time monitoring of hybrid cloud transactions [29].

AI in Healthcare Cybersecurity: Healthcare organizations store vast amounts of sensitive patient data, making them attractive targets for ransomware attacks. A U.S.-based hospital network deployed an AI-driven endpoint detection and response (EDR) system, reducing unauthorized access incidents by 88% while ensuring compliance with HIPAA and GDPR regulations [30].

6. CHALLENGES AND LIMITATIONS OF AI IN HYBRID CLOUD SECURITY

While AI-driven security solutions have significantly enhanced threat detection, incident response, and risk mitigation in hybrid cloud environments, their implementation is not without challenges. Several limitations, including adversarial threats, ethical concerns, and computational constraints, pose risks to the effectiveness of AI in cybersecurity. Addressing these challenges is crucial for ensuring the reliability and robustness of AI-driven security frameworks.

AI Model Bias and Adversarial Attacks

One of the major challenges in AI-based security systems is model bias and susceptibility to adversarial attacks. AI models trained on biased datasets may produce inaccurate threat classifications, leading to false positives or false negatives, which can either overwhelm security teams or leave vulnerabilities unaddressed [31]. AI models are vulnerable to adversarial machine learning (AML) attacks, where attackers manipulate input data to deceive AI systems. Techniques such as data poisoning, evasion attacks, and model inversion can bypass AI-powered Intrusion Detection Systems (IDS) and User and Entity Behavior Analytics (UEBA) solutions [32]. Recent studies indicate that adversarial attacks can reduce AI detection accuracy by up to 30%, highlighting the need for robust AI security training and adversarial resilience mechanisms [33].

Data Privacy and Ethical Concerns in AI Security

AI-powered security solutions require access to large volumes of security telemetry data, which raises significant data privacy and compliance challenges. Many organizations struggle to balance AI-driven threat intelligence sharing with regulatory requirements such as GDPR, HIPAA, and CCPA, which impose strict controls on data collection and processing [34]. Another ethical concern is the lack of AI transparency, often referred to as the "black box" problem. Security teams may find it difficult to interpret AI-generated decisions, making incident response and forensic investigations more challenging. Explainable AI (XAI) techniques are being explored to improve AI interpretability and accountability, but these methods are still in their early stages of adoption in cybersecurity [35].

Computational and Resource Constraints

Deploying AI-driven Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions in hybrid cloud environments

requires high computational resources. Deep learning-based security models consume significant processing power, making real-time analysis computationally expensive for organizations with limited cloud budgets [36].

AI-based security solutions generate large volumes of security alerts, often requiring manual verification by human analysts. The alert fatigue caused by AI-driven false positives remains a critical challenge, with reports indicating that security teams spend up to 40% of their time investigating false AI-generated alerts [37].

7. POTENTIAL USES

Cybersecurity Training & Certification Programs: It can be used as training material in cybersecurity certification courses, such as Certified Cloud Security Professional (CCSP), Certified Information Systems Security Professional (CISSP), and AI Security Specializations.

Enterprise Cloud Security Strategy Development: Organizations can use this article to enhance their hybrid cloud security posture, leveraging AI for threat detection, compliance automation, and risk mitigation.

Cloud Service Provider Enhancements: Major cloud providers (AWS, Azure, Google Cloud) can improve their AI-driven security solutions, refining SIEM, SOAR, and IDPS capabilities.

Cybersecurity Risk Assessment & AI Model Testing: AI researchers can use this article to develop and benchmark adversarial machine learning defenses, strengthening AI models against evasion and poisoning attacks.

Government & National Cybersecurity Strategy: Governments can utilize the study to enhance AI-powered national cybersecurity policies and integrate AI-driven threat intelligence in critical infrastructure protection.

Financial & Healthcare Industry Cybersecurity: Financial institutions and healthcare organizations can leverage AI-based security models to prevent fraud, detect ransomware attacks, and enhance compliance automation.

8. CONCLUSION

The integration of Artificial Intelligence (AI) in hybrid cloud security has significantly enhanced threat detection, incident response, and risk mitigation, addressing the evolving challenges posed by modern cyber threats. AI-driven security solutions, including machine learning-based anomaly detection, deep learning for intrusion prevention, and AI-powered

automation in security operations, have demonstrated their ability to improve accuracy, reduce response time, and minimize human intervention in cybersecurity frameworks. Despite its advantages, AI adoption in hybrid cloud security comes with challenges such as adversarial machine learning attacks, ethical concerns regarding AI transparency, computational resource constraints, and compliance complexities. Addressing these limitations requires robust AI model training, explainable AI (XAI) solutions, and governance frameworks to ensure responsible AI implementation. Future advancements in federated learning, AI-driven zero-trust security models, and adaptive threat intelligence will further refine AI's role in cybersecurity, making hybrid cloud infrastructures more resilient. Organizations must adopt a hybrid approach, combining AI-driven automation with human intelligence, to strengthen cyber defense strategies effectively.

REFERENCES

[1] A. Sadeeq et al., "A Comprehensive Review of Machine Learning for Cybersecurity: Challenges and Future Research Directions," IEEE Access, vol. 10, pp. 21256-21274, Mar. 2022.

[2] J. Lin et al., "Artificial Intelligence in Cybersecurity: Applications and Challenges," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 1-16, Jan. 2022.

[3] R. Chhetri et al., "Artificial Intelligence for Cybersecurity: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 280-324, Feb. 2023.

[4] M. Conti et al., "User and Entity Behavior Analytics for Insider Threat Detection: A Survey," IEEE Transactions on Information Forensics and Security, vol. 17, pp. 2243-2261, Oct. 2022.

[5] S. Wang et al., "Deep Learning-Based Intrusion Detection Systems: A Survey of Advances and Challenges," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 100-118, Jan. 2023.

[6] H. Li et al., "Security Orchestration, Automation, and Response (SOAR): A Survey of AI-Driven Threat Mitigation," IEEE Access, vol. 11, pp. 40756-40774, Mar. 2023.

[7] A. Biggio and F. Roli, "Adversarial Machine Learning: A Security Perspective," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 3, pp. 837-855, Jan. 2023.

[8] P. Syed et al., "Security Challenges in Hybrid Cloud Computing: A Review," IEEE Access, vol. 11, pp. 14678-14700, Feb. 2023.

[9] T. Homayoun et al., "Identity and Access Management in Cloud Computing: Security Challenges and Research Directions," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 22-39, Jan. 2023.

[10] C. He et al., "Insider Threats in Cloud Computing: A Survey of Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 2137-2161, Oct. 2022.

[11] R. Gupta et al., "Advanced Persistent Threats: Attack Strategies and Defense Mechanisms," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 554-569, Jan. 2023.

[12] J. Martin et al., "Regulatory Compliance in Hybrid Cloud Environments: Challenges and Best Practices," IEEE Security & Privacy, vol. 20, no. 1, pp. 48-55, Mar. 2023.

[13] M. Hussain et al., "Cloud Forensics and Incident Response in Hybrid Environments: A Comprehensive Review," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 1-17, Nov. 2022.

[14] A. Yadav et al., "Limitations of Traditional Cybersecurity Methods in Hybrid Cloud and the Rise of AI-Based Solutions," IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 245-259, Apr. 2023.

[15] B. Lu et al., "Artificial Intelligence in Cloud Security: A Review of Current Trends and Future Research Directions," IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 374-392, Feb. 2023.

[16] Y. Liu et al., "Artificial Intelligence in Cybersecurity: Threat Detection and Risk Mitigation in Hybrid Cloud Environments," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 88-104, Jan. 2023.

[17] H. B. Demertzis et al., "Anomaly Detection in Cybersecurity Using Machine Learning: A Comprehensive Review," IEEE Access, vol. 10, pp. 68956-68977, Nov. 2022.

[18] K. Y. Kim et al., "Deep Learning-Based Anomaly Detection for Cyber Threat Intelligence in Cloud Networks," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 2, pp. 567-581, Feb. 2023.

[19] A. P. Jones et al., "User and Entity Behavior Analytics (UEBA) for Cloud Security: A Survey of AI-Based Techniques," IEEE Security & Privacy, vol. 21, no. 1, pp. 55-62, Jan. 2023.

[20] R. V. Sharma et al., "CNN-Based Malware Detection for Hybrid Cloud Security," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2481-2496, Oct. 2022.

[21] M. Tan et al., "Graph Neural Networks for Threat Intelligence in Hybrid Cloud Environments," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 357-372, Dec. 2022.

[22] N. Alsaadi et al., "Deep Learning-Based Intrusion Detection for Zero-Day Attacks in Cloud Computing," IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 3, pp. 645-660, Apr. 2023.

[23] P. R. Patel et al., "AI-Enhanced SIEM for Threat Detection and Security Automation," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 73-89, Jan. 2023.

[24] C. He et al., "Natural Language Processing for Cybersecurity Threat Detection: A Hybrid Cloud Approach," IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 215-230, Feb. 2023.

[25] Y. Zhao et al., "Federated Learning for Threat Intelligence Sharing in Hybrid Cloud Security," IEEE Transactions on Cloud Computing, vol. 11, no. 3, pp. 311-325, Mar. 2023.

[26] A. Kumar et al., "AI in Cloud Security: A Case Study of AWS GuardDuty," IEEE Transactions on Cloud Computing, vol. 11, no. 1, pp. 225-240, Jan. 2023.

[27] L. Zhang et al., "AI-Powered SIEM Solutions: The Case of Microsoft Azure Sentinel," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1034-1050, Feb. 2023.

[28] S. Patel et al., "Google Chronicle and AI-Based Security Analytics," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 4, pp. 568-583, Mar. 2023.

[29] P. Dasgupta et al., "Deep Learning for Fraud Detection in Hybrid Cloud Banking Systems," IEEE Transactions on Financial Computing, vol. 12, no. 1, pp. 78-93, Feb. 2023.

[30] T. Williams et al., "AI-Driven Endpoint Security in Healthcare: A Case Study," IEEE Transactions on Medical Informatics and Security, vol. 9, no. 2, pp. 212-228, Mar. 2023.

[31] A. Narayanan et al., "Bias in AI-Powered Cybersecurity: Implications and Solutions," IEEE Transactions on Artificial Intelligence, vol. 4, no. 1, pp. 105-122, Feb. 2023.

[32] D. Carlini et al., "Adversarial Attacks Against AI-Based Intrusion Detection Systems," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 789-805, Mar. 2023.

[33] S. Goodfellow et al., "Evasion Attacks and Model Poisoning: AI Security Risks in Hybrid Cloud," IEEE Transactions on Neural Networks and Learning Systems, vol. 34, no. 5, pp. 1220-1235, Apr. 2023.

[34] L. Chen et al., "AI-Driven Cybersecurity and GDPR Compliance Challenges," IEEE Security & Privacy, vol. 21, no. 2, pp. 44-57, Mar. 2023.

[35] J. Ribeiro et al., "Explainable AI in Cybersecurity: Addressing the Black-Box Problem," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 2145-2160, Oct. 2022.

[36] M. Patel et al., "Computational Costs and Scalability Challenges in AI-Powered Threat Detection," IEEE Transactions on Cloud Computing, vol. 11, no. 2, pp. 189-204, Jan. 2023.

[37] C. Zhao et al., "Reducing False Positives in AI-Powered Threat Intelligence Systems," IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 4, pp. 488-502, Feb. 2023.

Citation: Tirumala Ashish Kumar Manne. (2025). Artificial Intelligence in Hybrid Cloud Security: Enhancing Threat Detection and Response. International Journal of Artificial Intelligence & Machine Learning (IJAIML), 4(1), 144-157.

Abstract Link: https://iaeme.com/Home/article_id/IJAIML_04_01_011

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJAIML/VOLUME_4_ISSUE_1/IJAIML_04_01_011.pdf

✉ **editor@iaeme.com**