International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

The Dark Side of AI: How Cybercriminals are Leveraging Machine Learning for Attacks in Multi-Cloud Hosted Applications

Jayasudha Yedalla

Colorado Technical University, Colorado, USA

Abstract

Cybersecurity was brought to the next level by introducing the applications of AI and ML into the practice. However, hackers still use and abuse the same technologies when executing the hacks, especially those in the multi-cloud extension. This paper focuses on how emerging cyber threats like adversarial machine learning, deep fake phishing, and bot-like malware are evading conventional protection measures. It also explores some of the weaknesses in multi-cloud systems that make them prone to AI-generated hacking attacks. Drawing from real-life scenarios and essential trends of the present times, this paper establishes the importance of strong AI protection measures and preventive measures against AI-themed cyber criminality.

INTRODUCTION

Artificial intelligence and machine learning are trends that have positively affected society and many sectors, and cybersecurity is one of the benefiting sectors. From the perspective of security, AI has been beneficial in detecting and preventing security threats and counterattacking them before they are even launched, while on the other hand, with the advancement of these technologies, the attackers are also planning and launching more advanced and sly attacks. AI-based threats are particularly interested in multi-cloud settings since they are scalable and provide flexibility and increased risks due to the interconnectivity of the systems.

It is essential to know where cybercriminals are propagating AI as this shows that cybercriminals are subtle in implementing AI to automate their attacks and bypass detection from security solutions instituted in cloud-based systems. Among them, adversarial machine learning attacks the intelligence models, whereas deepfakes can be used for realistic phishing. Also, since advancements in AI technology create new vulnerabilities in security systems, malware will always look for ways to exploit these vulnerabilities. Since organizations are implementing multi-cloud architectures in their enterprises, more advanced AI-enabled threats are the new reality of the business environment.

This paper highlights the negative aspects of applying artificial intelligence in cybersecurity, specifically in multi-cloud environments, and how attackers utilize machine learning algorithms to create new threats. It discusses real-life examples and scenarios involving AI-based threats, the consequences of such attacks, and measures to prevent these incidents. Understanding these threats is crucial for developing preventive measures to protect critical information and systems in today's world.

1. Overview of AI and ML Advancements in Cybersecurity

AI and ML are vital in enhancing the cybersecurity landscape as we know it today. AI has enabled organizations to counter threats, respond to them, and even prevent them from occurring in real time. Artificial intelligence-based security systems are more effective in analyzing large datasets, identifying potential risks, and mitigating them more effectively than conventional security software (Alzoubi et al., 2024). Artificial intelligence-based security solutions are recommended for adequate data protection in cloud and multi-cloud environments as internet threats become more advanced (Singh et al., 2024).

1.1 The Dual Role of AI: Enhancing Security vs. Enabling Cybercrime

Although advisors like AI play a significant role in combating cyber threats, malicious actors also leverage AI to enhance their tactics. Ferdous et al. (2025) discuss several emerging AI-based cyber threats, including artificial intelligence-based phishing attacks, AI-powered malware, and adversarial machine learning, where a malicious actor alters the structure of an AI model to evade defensive measures. They achieve this by integrating AI into their phishing attempts: the attacks become more convincing through deep fakes, and reconnaissance is conducted mechanically (Sadaram et al., 2024). Furthermore, AI-powered botnets possess learning capabilities, enabling them to adapt to security defenses, which makes eliminating them even more challenging (Lekkala et al., 2022).

1.2 Why Multi-Cloud Environments Are Prime Targets for AI-Driven Attacks

Multi-cloud is a preferred deployment model for many organizations since it is flexible and elastic. Nevertheless, it has brought new threats in terms of information security. When using a multi-cloud model, the level of control and misconfigurations come with a higher risk, mainly because the vulnerabilities can be exploited by cybercriminals or hackers (Murthy et al., 2024). Unifying AI into the hybrid cyber-attacks makes it easy for the attackers to automate their work in the multi-cloud environment and access security blind spots and sensitive information leakage in various cloud environments (Hayat et al., 2024). Also, AI-involved malware can take advantage of and fully familiarize itself with the disparate security policies in cloud services, so the protective measures cannot be equally deployed consistently (Ahmed, 2024).

2. Purpose of the Article and Key Areas of Focus

Based on the above points, the rationale of this article is to examine the alarming trends of artificial intelligence backed up cyber threats in multi-cloud networks. It offers a detailed overview of how hackers use AI to achieve better accuracy, ever eluding identification and manipulating the cloud environment. The topics to be discussed will include adversarial machine learning, Artificial Intelligence-based phishing, and AI-based Malware automation. In addition, the article will also discuss the security issues associated with a multi-cloud environment and how organizations need to guard against AI attacks. As this paper outlines using recent academic works, there is a growing call for increased prevention and control of the emerging AI-based threats in multi-cloud environments.

2.1 The Role of AI in Cybercrime

Hackers now actively leverage AI in planning and executing numerous high-level, fully automated, and coordinated cyberattacks. On one hand, Artificial Intelligence is used to enhance protection measures against cyber-attacks; on the other hand, it equips adversaries with increased speed, scope, and precision for their cyber-attack tools. Malicious actors can shift strategies at any moment, making them a threat that doesn't correlate with traditional security methods (Ferdous et al., 2025). This section discusses how cyber criminals utilize AI for botnets, malware, adversarial ML, and real-world AI-enabled attacks in cyberspace.

2.2 How Cybercriminals Use AI to Automate and Enhance Attacks

Criminals also employ AI to enhance their operations and complicate cyber threats. This form of reconnaissance enables attackers to infiltrate target systems and quickly gather valuable information from various sources, including websites, ports, and configurations. It reduces the time required to identify security gaps, allowing cybercriminals to exploit vulnerabilities before security personnel can respond (Sadaram et al., 2024). Additionally, leveraging databases improves the process with machine learning models to enhance the accuracy of predicting weaknesses in multi-cloud environments (Singh et al., 2024). Social engineering attacks have become considerably nefarious due to the communication mimicry enabled by AI technologies. With the help of Natural Language Processing, forged phishing emails can be crafted in a target's writing style, making it difficult to distinguish fake messages from the originals (Peiris et al., 2021). Deepfake technology enhances these schemes by creating counterfeit videos and audio clips, enabling attackers to impersonate executives or other authorized personnel. Chatbots elevate the manipulation game by engaging with victims in real time, adjusting their responses based on the circumstances (Sadaram et al., 2024).

Credential theft and password attacks have evolved to exploit AI in executing some forms of brute-force attacks. Instead of using password lists sequentially, as in conventional password cracking, AI analyzes user behavior, past intrusions, and password patterns to generate highly probable credentials (Ferdous et al., 2025). This enhances the effectiveness of credential stuffing and enables targeting accounts with simple or reused passwords more efficiently. Similarly, AI helps attackers evade MFA by circumventing voice synthesis within security protocols and their real-time management (Alzoubi et al., 2024).

It can also be real-time and self-learning, utilizing artificial intelligence to enhance the intelligence of its design. It is no longer a matter of following a specific pattern to launch an attack, allowing malware to alter its code periodically. Two key forms can be executed in ransomware attacks: first, AI-powered ransomware identifies critical data before storing and encrypting it (Hayat et al., 2024). Self-learning evolves the analysis of security characteristics in real time, giving the attacker a direct view of the target's actions and defenses against the invasion. Such trends enhance the ability of AI-based malware to bypass standard security systems and persist within the target systems (Mamidi, 2024).

The combination of AI in cybercrime is becoming a significant problem for professionals in the cybersecurity field. Today's attacks are faster and more precise, allowing them to evade reliable shields and barriers. Therefore, as AI becomes more integrated into society, organizations must develop strategies to prevent new threats from materializing, utilizing AI security systems to identify and counter them early (Murthy et al., 2024).

2.3 The Rise of Adversarial Machine Learning in Bypassing Security Models

Adversarial machine learning is gradually gaining traction in the cybersecurity industry because it utilizes AI-based security systems that compel hackers to discover new methods to bypass those systems. In this way, cybercriminals provide inputs that alter how machine learning models perceive actual threats, thereby facilitating their illicit activities. This can occur at various stages of an AI system, including training and real-time or inference-making, which makes an adversarial machine learning attack challenging to prevent (Ferdous et al., 2024).

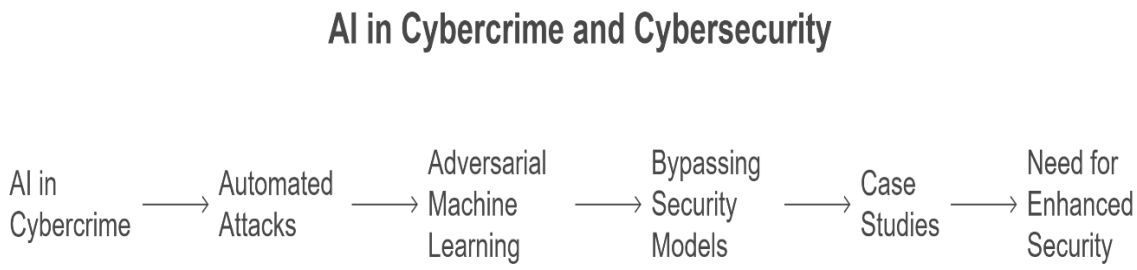
Consequently, the most common method related to attack vectors is known as adversarial perturbation. In this case, attackers introduce small and sometimes unnoticeable alterations to the inputs that feed into the models. This can mislead AI-based intrusion detection systems, malware classifiers, and biometric authentication systems, causing them to provide incorrect outcomes (Ahmed, 2024). For instance, with a

minor change to the construction of a malicious file, cybercriminals can enable it to slip through AI-based security platforms, making them deem it harmless (Ivaki & da Silva, 2024).

Another evolving threat is data poisoning, which involves an attacker supplying improper or malicious data to AI training sets to distort the development of security models. It is a well-documented fact that when an AI model's training data is poisoned, it creates a system that fails to recognize specific attack patterns, making an organization vulnerable to cyber threats. This technique has been used in spam detection, phishing prevention methods, and endpoint security, leading to a high likelihood of successful cyberattacks (Murthy et al., 2024).

In addition to misclassification and data poisoning, AML can lead to model inversion attacks, where cybercriminals extract information from AI models. Sometimes, AI replicates victims' login credentials, such as an encrypted or decrypted key, by observing how a specific security model handles data. This situation highlights the dangers of using AI to automate decision-making in cybersecurity, as adversaries are always seeking new ways to penetrate machine learning systems (Alzoubi et al., 2024).

As cybersecurity utilizes AI and such programs advance in skill, adversarial machine learning creates an ongoing cat-and-mouse game between the two sides. Possible countermeasures include adversarial training that involves exposing the model to adversarial inputs during development to ensure its resilience against real-world attacks. Moreover, it is crucial for security personnel to continuously monitor for adversarial manipulations and implement AI explainability tactics (Mala & Annapurna, 2023). These techniques have become apparent with the emergence of AML. This scenario pressures security engineers to create more adaptable security measures that cannot be compromised by newer hacking methods, which often undermine the effectiveness of artificial intelligence.



2.4 Case Studies of AI-Powered Cyberattacks

Some events indicate the vulnerabilities of multi-cloud environments and AI-based security frameworks to AI-driven cyberattacks for organizations.

Thus, AI-based attacks are more effective than traditional phishing strategies, exhibiting higher levels of efficiency. Criminals employ AI to send emails that are hard to distinguish from those written by legitimate sources, often including details gathered from the target. This happens because chatbots have been used in social engineering cases to interact with targets in real-time, enhancing the interactivity of the attack and making it extremely difficult to detect (Peiris et al., 2021).

Using AI to enhance botnets has enabled them to employ machine learning to analyze traffic patterns and develop more effective methods to avoid detection. Subsequent versions of the Mirai botnet have integrated AI to automate infecting IoT devices and launch large-scale DDoS attacks quickly and flexibly (Singh et al., 2024).

The attacks also highlight the weaknesses in the security models developed based on machine learning. A noteworthy real-world example occurred when the data of a large cloud services provider was poisoned by attackers who manipulated the AI-based script used for fraud detection. This manipulation altered the system so that it mistakenly identified fraudulent transactions as genuine, resulting in significant financial loss. Such attacks demonstrate that adversarial machine learning threatens other security models in cloud environments (Murthy et al., 2024).

Another equally dangerous type of artificial deep fakes has also been developed for cyberattacks. Hackers employed deep fake technology to pretend to be managers and chiefs, sign for the scams and negotiate biometric security structures. Being able to produce credible audio and video deep fake communication, it sadly becomes hard to identify phony communication from genuine communication. This has considerably impacted financial and reputational losses to the targeted organizations (Sadaram et al., 2024).

The examples in such cases explain the increasing risk of incorporating artificial intelligence in cybercrime, hence the importance of adopting better security measures to combat these new intelligence crimes. As cyber threats evolve, organizations must employ further defense strategies such as better detectors, adversarial training, and an artificial intelligence system for threat intelligence feeding.

3. Key AI-Powered Threats in Multi-Cloud Environments

Currently, organizations are employing multi-cloud architectures, while cyber threat actors leverage artificial intelligence to exploit their security. These threats are becoming more complex in this landscape, as they seek to target vulnerabilities in security algorithms and mechanisms, along with authentication and data protection protocols.

Adversarial Machine Learning Attacks

The most immediate risk in multi-cloud environments is adversarial machine learning, where attackers modify artificial intelligence models to circumvent defense mechanisms undetected. An example of this threat involves injecting poisoned data or subtly altering inputs to bypass intrusion detection systems, malware classifiers, and fraud detection models. This enables attackers to operate unnoticed and engage in unauthorized activities, including data theft, fraud, and unauthorized access (Alharbi & DFerdous, 2024). This issue is worsened by the reality that individuals constantly seek to exploit AI models to identify vulnerabilities and loopholes. Threats that demand adversarial robustness can bypass protections, as poorly trained models or those lacking adversarial robustness can easily be misled (Ahmed, 2024).

DKeep fake Phishing and Social Engineering

The content generated by artificial intelligence has dramatically enhanced the practicality and surprisingly boosted the sophistication of various phishing and social engineering threats. Deepfake technology is now used to create video and audio impersonations of executives, employees, or virtually anyone, allowing cybercriminals to deceive the public quickly. Cybercriminals utilize artificial intelligence to execute phishing attempts via email, phone calls, or recorded voice messages to trick recipients into divulging personal and organizational information, accepting seemingly fraudulent transactions, and downloading malicious software (Sadaram et al., 2024). This is due to AI's ability to imitate and replicate human speech, written communication, and other facial resemblances, making traditional verification methods less effective, particularly in multi-cloud scenarios where communication is often fragmented (Peiris et al., 2021).

As these threats evolve and change, potential countermeasures for organizations operating in multi-cloud

environments include adversarial training for AI models, multi-factor authentication (MFA), and behavioral analysis. Additionally, AI must be integrated into cybersecurity because attackers leverage artificial intelligence to reduce losses and execute effective attacks.

4. Vulnerabilities in Multi-Cloud Security

Various security challenges have emerged as organizations have transitioned to using multiple cloud environments for workload management, scalability, and business continuity. Managing numerous cloud environments introduces risks that cyber attackers exploit using AI-generated techniques. These challenges include non-compliance with security policies, misconfigurations, and the difficulty of detecting cross-cloud threats in real-time.

4.1 Security Challenges Unique to Multi-Cloud Infrastructures

The most intriguing issue, unique to multiple cloud environments, is the variation in security measures across different cloud services. This issue is significant because each provider has distinct security policies, authentication methods, and compliance requirements that must be satisfied, making it challenging to implement a unified, centralized security strategy. As a result, this increases vulnerability, as attackers can easily exploit misconfigurations to gain further access or move to other platforms within the cloud (Murthy et al., 2024).

Another critical risk factor cannot be associated with identity and access management (IAM) irregularities. Multiple providers force many organizations to face the issue of a lack of a unified control plane for permissions. As a result, there may be too many or mismanaged credentials. These vulnerabilities make cloud environments vulnerable to artificial intelligence attacks, including credential stuffing and adaptive brute force attacks (Peiris et al., 2021).

Another known issue of employing a multi-cloud environment is data protection, as data is often located and processed in different clouds with different levels of encryption. Even encrypted traffic can be vulnerable to attacks, and AI can be incorporated into techniques for analyzing patterns of encrypted traffic, weak implementations of encryption, and Cryptojacking or data exfiltration (Alzoubi et al., 2024). Therefore, supply chain risks are a significant threat in multiple cloud environments and may cause unexpected low-quality results. Hackers can leverage AI to detect vulnerabilities in cloud applications and related third-party software integration or cloud-based computational applications. These supply chain attacks become possible through the use of artificial intelligence. They combine the weaknesses of all the cloud tenants, which, when attacked, provides a bigger picture compared to a single attack (Singh et al., 2024).

As threats to multi-cloud infrastructures become more diverse and sophisticated, their security measures should integrate AI for threat detection, policy automation, and anomaly detection. To maintain security in multi-cloud environments, ongoing supervision and enhanced detection of threats that originate or spread across cloud environments should be prioritized over risk management plans that can address the AI-powered cyber threats in circulation.

4.2 Lack of Unified Security Controls Across Multiple Cloud Providers

This is especially true given that security controls in multiple clouds are not standard for various cloud service providers. Modern providers often use different security frameworks and key authentication approaches and have a set of compliance demands that complicate the use of security as a consistent and coherent system within an organization. This incoherence also threatens configurations, as security administrators are stuck with multiple sets of policies and tools to implement, leaving all prospective gaps

to be filled by attackers (Murthy et al., 2024).

The lack of centralized monitoring further increases the challenges in the early detection and management of threats. This absence will result in a disjointed security model, complicating correlation across cloud environments; actions in one setting may go unnoticed and potentially signal attackers in cloud environments until a considerable amount of time has passed. These blind spots are exploited by AI-driven attacks to evade detection, rendering traditional security solutions significantly less effective in a multi-cloud environment (Peiris et al., 2021).

4.3 AI-Driven Reconnaissance for Identifying Weak Points

Leveraging AI, especially at the planning stage of an attack, is one way modern-day hackers approach cloud environments. The bad actors use AI to look for possible misconfigurations, exposed log-in credentials, and open SAs in various cloud environments. Unlike conventional scans, AI-based reconnaissance techniques are online techniques where penetration tests do not have to stop moving after some time as they define the best routes to access an organization's system (Alzoubi et al., 2024).

Based on the metadata freely available on the Internet, AI can identify network errors such as misconfigured storage buckets, ports that remain open, or weak access controls. Also, AI-powered tools can navigate rate limits by learning from successful attack vectors and applying them as adversarial ML. This strategy enables attackers to launch exact attacks, making such attacks much more effective and successful (Singh et al., 2024).

4.4 The Role of Misconfigurations and Insecure APIs

Configuration mistakes are also still one of the most significant threats in cloud security, as AI attacks utilize misconfigurations to penetrate the security of cloud networks. Weak IAM policies, unsecured storage objects, and large numbers of permissions allow the adversary to gain privileges or transfer data out from the organization. This problem intensifies when working in a multi-cloud setting because it becomes highly challenging to simultaneously apply consistent security regulations across different providers (Ahmed, 2024).

Another vulnerability that multi-cloud infrastructures have is insecure APIs. Most cloud applications use APIs to interact or interface with other services; these APIs can also become a vulnerable entry point to the attacker. AI-powered attacks can automate API enumeration, meaning they are used to determine that interfaces are API-friendly or to discover what types of authentication mechanisms are ineffective. If the API has been infiltrated, attackers can alter the requests sent to the API, including changing configuration, obtaining sensitive data with malicious intent, or even simply degrading specified services (Ivaki & da Silva, 2024).

Hence, there is the need to develop proactive measures in handling security problems associated with AI cyber threats through AI and machine learning technologies. With technological support, threat can be accurately detected in real-time by garnering different patterns that point towards malicious acts. These systems incorporate anomaly detection algorithms that help security teams identify any variation in trends, hence enabling the security team to take action before the identified threats transform into severe cases (Murthy et al., 2024).

Security Challenge	Description	Key Risks
Variation in Security Measures	Different security policies, authentication methods, and	Increases vulnerability due to misconfigurations and allows attackers to move across platforms easily.

	compliance requirements across cloud providers.	
IAM Irregularities	Lack of a unified control plane for identity and access management across multiple providers.	Mismanaged credentials lead to AI-powered attacks like credential stuffing and adaptive brute force attacks.
Data Protection Challenges	Data located across different clouds with varied encryption levels.	Vulnerable to AI-based analysis of encrypted traffic, Cryptojacking, and data exfiltration.
Supply Chain Risks	Threats arising from vulnerabilities in third-party software and cloud applications.	AI-driven attacks exploit combined weaknesses of cloud tenants, leading to complex and widespread breaches.
Lack of Unified Security Controls	Different security frameworks and compliance requirements complicate unified security management.	Creates gaps in security configurations and makes centralized monitoring difficult, increasing susceptibility to AI-driven attacks.
AI-Driven Reconnaissance	Use of AI by attackers to identify misconfigurations, open ports, and weak access controls.	Enhances precision of attacks by learning from successful vectors, making traditional security measures less effective.
Misconfigurations and Insecure APIs	Mistakes in configuration and unsecured APIs that expose cloud networks to threats.	Allows privilege escalation and data breaches, especially in multi-cloud setups.

Table 1: This table highlights the key challenges and risks associated with securing multi-cloud infrastructures

5.1 The most advanced technique of defending AI is adversarial training: security prototypes are presented with crafted inputs specifically intended to fool the AI-based detectors. This signifies the enhancement of the robustness of those AI-based security models against likely evasion strategies like adversarial perturbation and data poisoning (Alzoubi et al., 2024). Therefore, adversarial training is a valuable way in which security solutions can boost their ability to recognize AI-based cyber threats.

Security ORCA systems enhance defense capabilities by bridging Artificial Intelligence threat intelligence with incident response. These systems can analyze security alerts, find correlations between multiple cloud environments, and trigger responses with low human intervention (Ferdous et al., 2025). AI in SOCs also provides quicker threat response times, which means a faster mean time to respond to cyber threats.

Honeypot and decoy environment are AI-based deception technologies that help trap attackers and gain more knowledge about their activities. Such systems provide emulated interfaces that mimic actual behavior but are fakes meant to lure attackers and the security teams to interact to gather new threat trends (Ahmed, 2024). Take what measure in this way is proactive, which enables an organization to be prepared for new threats and adapt the strategy used to the security threat.

5. Zero Trust Security Models in Multi-Cloud Environments

As the name suggests, the Zero Trust security model shifts how multi-cloud infrastructures are secured. It eliminates the existing trust and implements a continuous Trust Nothing concept where everyone and everything must be verified. Unlike the perimeter security model, Zero Trust considers that threats may be internal or external to the network, thus requiring constant scrutiny and authorization of access (Murthy et al., 2024).

Facility Management means that users, applications, and other devices must operate under the lowest privilege level necessary to perform tasks. In multi-cloud, PoLP reduces the reach of effecting security threats by putting a ring-fence to the movement within cloud networks (Murthy et al., 2024).

Continuous Verification: Automated methods monitor the repetitiveness of usage patterns and further actions at both the user and system ends, immediately responding to unauthorized access attempts, unusual information transfers, and logins from geographical regions. If a threat is detected, lockdown prompts are initiated to prevent continued exploitation (Alzoubi et al., 2024).

Micro-Segmentation: Another feature implemented in the cloud environment is AIS, which creates small isolated areas for workloads with defined risk levels. This makes it impossible for attackers to navigate through different domains of the cloud environment. Micro-segmentation, conversely, means that if a specific segment is penetrated, the harm produced is checked and will not affect other segments (Singh et al., 2024).

Zero Trust Network Access (ZTNA) is a security model that prohibits any access to the network until each request is thoroughly examined, validated, and authorized in real time. Other entities that require access to cloud systems are granted entry through AI-driven ZTNA solutions; however, their trustworthiness, geographical location, and behavior are evaluated beforehand (Ahmed, 2024).

Zero Trust security models, supported by AI, include frequent verification for every action penetrating deeper into cloud assets or roaming about the environment, even if it has compromised the initial barrier.

6. Enhancing the Sign-On Depending on the degree of risk an organization faces, the sign-on may be the most significant aspect that needs enhancement.

While cybercriminals have adopted AI as a potent weapon to evade conventional defense systems, concepts such as authentication and access control need to be revised to be effective in this new environment. AI improves the authentication process by applying intelligence to security checks that change over time and are hard for attackers to compromise (Peiris et al., 2021).

AI-Based Multi-Factor Authentication (MFA): Unlike static MFA, where customers use a password and receive an SMS code, AI-based MFA employs customer behavioral techniques. It effectively logs devices, locations, and body features about risk in real time. This is done if there is a login attempt that an organization or user did not initiate, for example, through an unknown device or placing from a different location; this makes the user undergo other layers of authentication to prevent invasion.

AI in Biometric Authentication: AI enhances biometric security features such as facial recognition, fingerprint scanning, and voice recognition. It can identify and thwart fakes and impostors since attackers cannot replicate other static MFA, where customers use a password and receive an SMS code. AI-based MFA employs customer behavioral techniques. It effectively logs aspects of user identity based on facial features, voice modulation, and even differing heartbeat rates through masks and mirroring techniques (Sadaram et al., 2024).

Adaptive Access Control: Unlike conventional MAC, which uses embedded rules concerning the user, the

device, the application type or any other factors, AAC decides access control by constantly and dynamically assessing the risks in the activity, the individual, the hardware and software environment of the respective user. For instance, an employee within a secured office environment connecting to the cloud to retrieve information may only need check-ins usually used by the company. At the same time, the same request from an unknown Wi-Fi connection, may require additional confirmation or even be denied (Ahmed, 2024).

AI-driven privileged Access Management (PAM) is essential due to the risk of cyberattacks on privileged users, such as system administrators and executives. PAM solutions for supervised accounts operate in real time, analyzing user behavior patterns for irregularities, such as logins from different time zones, access to restricted data, or attempts to gain additional privileges. AI can block access, enhance authentication, or notify security personnel (Lekkala et al., 2022).

By incorporating AI into authentication and access control measures, organizations can assess potential risks while preventing unauthorized access attempts from escalating into significant data breaches. Ensuring continuous access verification also reduces credential theft and unauthorized privilege escalation, thereby countering the role of AI in cyberattacks.

Privileged Account Management using Artificial Intelligence: System administrators or executive accounts can pose a significant risk to all attacks. AI-based PAM solutions track high-privilege accounts in real time, analyzing patterns like invalid login times, data access privileges, and attempts to increase privilege levels. Any unusual behavior can be counteracted by canceling access, stricter identification, or notification by security specialists (Lekkala et al., 2022). With the use of AI in authentication and access control, an organization can develop an understanding and ability to estimate risks and preemptively deny unauthorized access, which is highly likely to lead to full-blown system breaches. AI has enhanced security models for frequently checked credentials and privileged identities so that no one unauthorized can escalate their access and threaten to attack AI structures.

DISCUSSION

This discussion delves into the increasing use of AI in cyber threats in multi-cloud. It proclaims the duality of AI in improving security and as a tool in compromising security. With business-critical applications deploying in multiple, geographically distributed, interconnected clouds to achieve flexibility and mild equality, the application of artificial intelligence itself becomes a new opening for a cybercriminal. It is evident in this and other scenarios that there is dire need to enhance security measures to address AI threats.

The first of the highlighted threat categories is adversarial machine learning, when the attacker interferes with the AI model to get past the security measures freely. This attack proves to be rather dangerous for multi-cloud infrastructures as they are often built from various suppliers that can have somewhat different levels of security. Most artificial intelligence models are not adversarially robust, making them susceptible to having poisoned data or to being attacked by having their input changed slightly so as not to be detected by a system. This is because the development of AI techniques is far more progressive than the security measures that can be implemented to guard against.

Another crucial one is that AI is employed in deepfake phishing and social engineering schemes. AI applications of deepfake technology are effective; therefore, it is easier for fraudsters to create a reliable phishing message or use a credible identity. In multi-silo environments where information sharing is usually limited, these attacks are executed to effectively embrace standard confirmation techniques,

thereby resulting in losses through theft as well as identity fraud. This modern strategy showcases the weakness of the current security measures in handling today's increasing form of intelligent attacks.

These challenges include safety defects unique to the multi-cloud environment, like misconfiguration, non-compliance with policies, and weak identity and access management. The lack of integration of various security controls across multiple cloud providers makes it even harder since attackers will capitalize on flaws between cloud provider systems. AI-driven attacks can utilize these weaknesses to launch organized attacks, including second-tier attacks focusing on third-party software and cloud applications comprising a multi-cloud stack.

CONCLUSION

The conclusion emphasizes the urgent need for organizations to rethink their security strategies in the face of AI-powered threats targeting multi-cloud environments. It underlines the importance of enhancing the organization's security measures because of the new AI-based threats in multi-cloud environments. Hypertext is a way in which artificial intelligence has improved the cybersecurity situation by enhancing the development of cybersecurity threats by the attackers. It is crucial to understand that AI serves as a shield and weapon when speaking about multi-cloud environments, where unifying the rules and eliminating misconfiguration is often challenging.

Such problems must involve a multilevel solution that incorporates AI for threat detection and prevention and for designing adversarial resistance to AI models. The security leaders are reporting that such measures as identity and access improvement, consolidating security across cloud environments, and adopting techniques like adversarial training are also moving in the right direction. For this reason, organisations will have to constantly evolve in their attempt to ward off both threats from AI security and those from AI attackers. Many organizations understand the potential risks of AI and how these systems can be used as a threat rather than a shield, and that is why a great effort will have to be made to properly transform AI into a security mechanism that can guarantee a secure multi-cloud environment.

REFERENCE

1. Dhayanidhi, G. (2022). Research on IoT threats & implementation of AI/ML to address emerging cybersecurity issues in IoT with cloud computing.
2. Ferdous, J., Islam, R., Mahboubi, A., & Islam, M. Z. (2025). A survey on ML techniques for multi-platform malware detection: Securing PC, mobile devices, IoT, and cloud environments. Sensors, 25(4), 1153. https://doi.org/10.3390/s25041153
3. Ferdous, J., Islam, R., & Mahboubi, A. (2024). A survey on machine learning techniques in multi-platform malware detection: Securing PC, mobile devices, IoT, and cloud environments. Preprints. https://doi.org/10.20944/preprints202412.0348.v1
4. Ahmed, W. (2024). Trends and challenges in securing cloud computing environments: An overview of current techniques. Premier Journal of Computer Science. Retrieved from premierscience.com
5. Murthy, J. S., Lai, W. C., & Dhanashekar, K. (2024). Fortifying cyber resilience in the ever-changing sky of cloud security. Cloud Security.
6. Singh, N., Buyya, R., & Kim, H. (2024). Securing cloud-based internet of things: Challenges and mitigations. Sensors, 24(15), 5234. https://doi.org/10.3390/s24155234
7. Hayat, M. A., Islam, S., & Hossain, M. F. (2024). Securing the cloud infrastructure: Investigating multi-tenancy challenges, modern solutions, and future research opportunities.

8. Otta, S. P. (2023). Novel multi-factor authentication approach for multi-cloud computing systems. BITS Pilani.
9. Akhtar, S. I. (2025). Inter-cloud security framework for handling of data. National University of Sciences and Technology.
10. Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat hunting in the cloud: Defending AWS, Azure, and other cloud platforms against cyberattacks. John Wiley & Sons.
11. Ivaki, N. R., & da Silva, P. M. G. (2024). AI-based intrusion detection mechanisms for cloud-native services.
12. Smirnova, T., & Ivanov, P. (2024). Mitigating cyber threats in cloud computing: A comprehensive review of security strategies. Eastern-European Journal of Cybersecurity.
13. Murthy, J. S., Siddesh, G. M., & Srinivasa, K. G. (2024). Cloud security: Concepts, applications and practices.
14. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57(3), 2021-2056. https://doi.org/10.1007/s10462-023-10234-5
15. Mamidi, S. R. (2024). Dynamic security policies for cloud infrastructures: An AI-based framework. Journal of Artificial Intelligence General Science (JAIGS).
16. Mala, K., & Annapurna, H. S. (2023). Cloud network traffic classification and intrusion detection system using deep learning. Proceedings of the International Conference on Integrated Intelligence Systems.
17. Lekkala, S., Avula, R., & Gurijala, P. (2022). Big data and AI/ML in threat detection: A new era of cybersecurity. Journal of Artificial Intelligence and Big Data.
18. Sadaram, G., Karaka, L. M., & Maka, S. R. (2024). AI-powered cyber threat detection: Leveraging machine learning for real-time anomaly identification and threat mitigation. MSW Management Journal.
19. Varney, A. (2019). Analysis of the impact of artificial intelligence on cybersecurity and protected digital ecosystems.