ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr1143

AI Driven Zero Trust Security for Hybrid Clouds

Kishan Raj Bellala[1]

[1]Independent Researcher
Austin, Texas, U.S.A.

ORCID ID: https://orcid.org/0009-0007-2327-0993

Publication Date: 2025/04/28

Abstract: Enterprises face a critical security challenge when they deploy hybrid cloud systems because these systems combine public cloud scalability with private cloud data control. Zero-trust security frameworks must be adopted because traditional perimeter-based security methods no longer work in hybrid cloud environments with their dynamic and decentralized nature. Every person's system and device must prove their identity under the zero-trust model because no entity should receive unconditional trust regardless of its location. The hybrid cloud environment demands advanced security approaches because it handles massive amounts of data while facing complex modern cyber threats. This paper investigates the implementation of artificial intelligence (AI) systems to boost zero-trust security protection within hybrid cloud infrastructure. The research investigates present trends and upcoming directions to develop an extensive framework which uses artificial intelligence for zero-trust security protection of hybrid cloud systems against modern cyber threats. We analyze the advantages and obstacles and ethical aspects of implementing zero trust for AI together with its actual usage in hybrid cloud systems. The research provides a complete method to use artificial intelligence for improving Zero Trust security in hybrid cloud systems through analysis of present trends and future development possibilities. Such measures will establish an active intelligent and strong defense mechanism against present and future cyber threats.

Keywords: *Hybrid Cloud, Public Cloud, Private Cloud, Zero Trust, Zero Trust Security Framework, Perimeter-Based Security, Decentralized Security, Cyber Threats, Artificial Intelligence (AI), Scalability, Flexibility, Resilient Defense, Security Challenges, Ethical Considerations, Future Developments.*

How to Cite: Kishan Raj Bellala (2025). AI Driven Zero Trust Security for Hybrid Clouds. *International Journal of Innovative Science and Research Technology,* 10(4), 1492-1497. https://doi.org/10.38124/ijisrt/25apr1143

I. INTRODUCTION TO ZERO TRUST SECURITY MODEL

Zero Trust security model functions like cybersecurity paradigm which presumes threats exist inside as well as outside an organization's network (Parisa, Banerjee, & Whig, 2023). Traditional security models establish two network zones where external networks remain untrusted but internal networks maintain trusted status.

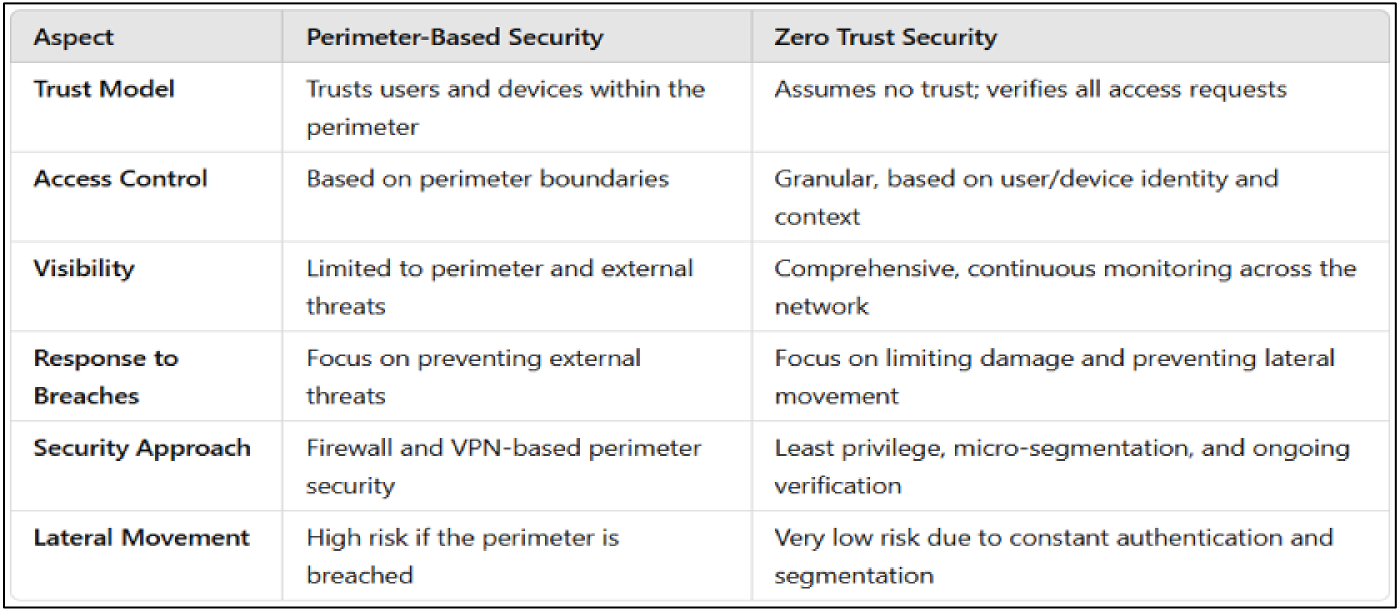
Zero Trust functions on the fundamental belief that verification should always happen because trust should never be given (Parisa, Banerjee, & Whig, 2023). The Zero Trust model requires authentication for every access request since no person or device receives automatic trust regardless of network connection status. The system requires authentication for all access requests since no user or device receives automatic permission regardless of their location (Parisa, Banerjee, & Whig, 2023).

➢ *Key Principles of the Zero Trust Model Include:*

- **Least Privilege Access:** Users and devices receive only essential access rights needed to perform their duties because this restriction minimizes damage from breaches (Horne & Nair, 2021).
- **Micro-Segmentation:** The technique of micro-segmentation divides network resources into smaller protected sections (Horne & Nair, 2021). The network lateral movement capability of attackers becomes lower because of this approach.
- **Continuous Monitoring and Authentication:** Systems and data undergo constant examination and tracking through authentication processes beyond the initial verification step. The system detects abnormal behavior through this method (Horne & Nair, 2021).
- **Assumption of Breach**: The Zero Trust framework operates under the assumption that a breach may occur at any time, so it implements strong authentication systems and access controls to minimize breach impacts (Horne & Nair, 2021).

- **Data Protection:** The encryption along with strict data access policies provides complete protection for sensitive information during a breach (Horne & Nair, 2021).

Table 1 Zero Trust vs. Traditional Perimeter-Based Security (Capili, 2024).



Aspect	Perimeter-Based Security	Zero Trust Security
Trust Model	Trusts users and devices within the perimeter	Assumes no trust; verifies all access requests
Access Control	Based on perimeter boundaries	Granular, based on user/device identity and context
Visibility	Limited to perimeter and external threats	Comprehensive, continuous monitoring across the network
Response to Breaches	Focus on preventing external threats	Focus on limiting damage and preventing lateral movement
Security Approach	Firewall and VPN-based perimeter security	Least privilege, micro-segmentation, and ongoing verification
Lateral Movement	High risk if the perimeter is breached	Very low risk due to constant authentication and segmentation

The Zero Trust security model functions as an advanced solution which overcomes traditional perimeter-based security restrictions thus representing an essential approach for protecting hybrid cloud environments with their dispersed user base and devices and data locations (Horne & Nair, 2021). Zero Trust strengthens organizational resilience through continuous access verification and reduced trust to defend against external and internal cyber threats (Capili, 2024).

➢ *Architecture of Zero Trust*

ZTA operates under the principle that you should never believe any request source or identity presentation or device or application seeking network or data access (Tiwari, Sarma, & Srivastava, 2022). ZTA operates on the premise that breaches will occur which need to be managed whereas traditional methods depend on geographic location or pre-verified authentication to establish identities. The ZTA model has become widely adopted by industrial and government entities because it provides flexible risk management for new decentralized and hybrid computer system designs (Tiwari, Sarma, & Srivastava, 2022).

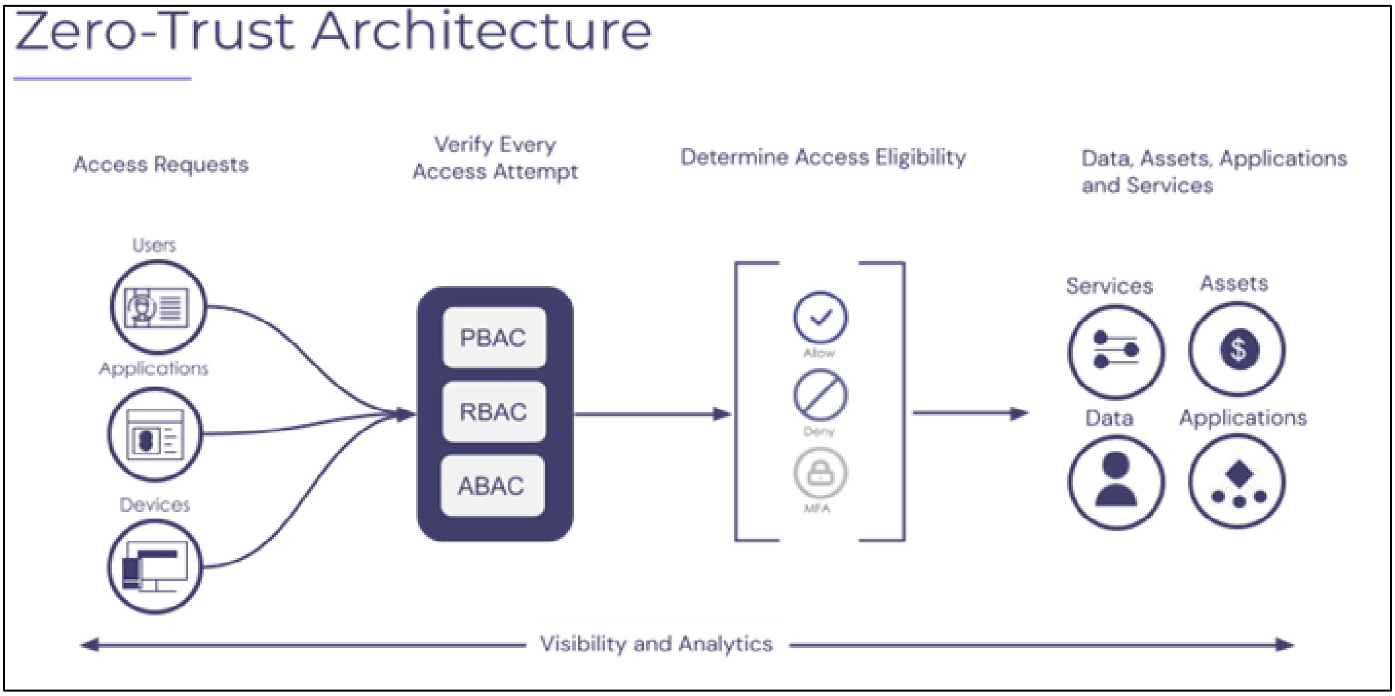


Fig 1 Zero Trust Architecture (Tiwari, Sarma, & Srivastava, 2022).

Key elements of ZTA include segmentation, monitoring, and identity and access management. These elements reflect the growing and changing demands of businesses in terms of managing cloud systems, more remote workers, and ways to integrate IoT technologies (Tiwari, Sarma, & Srivastava, 2022).

➢ *Market Trend for Zero Trust*

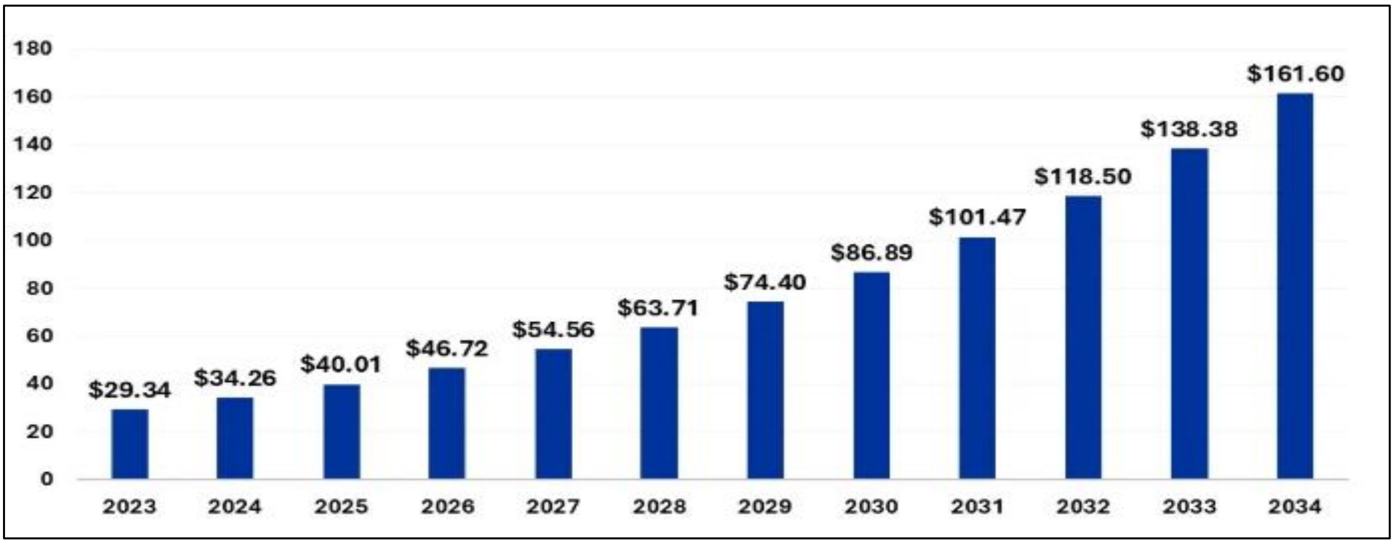
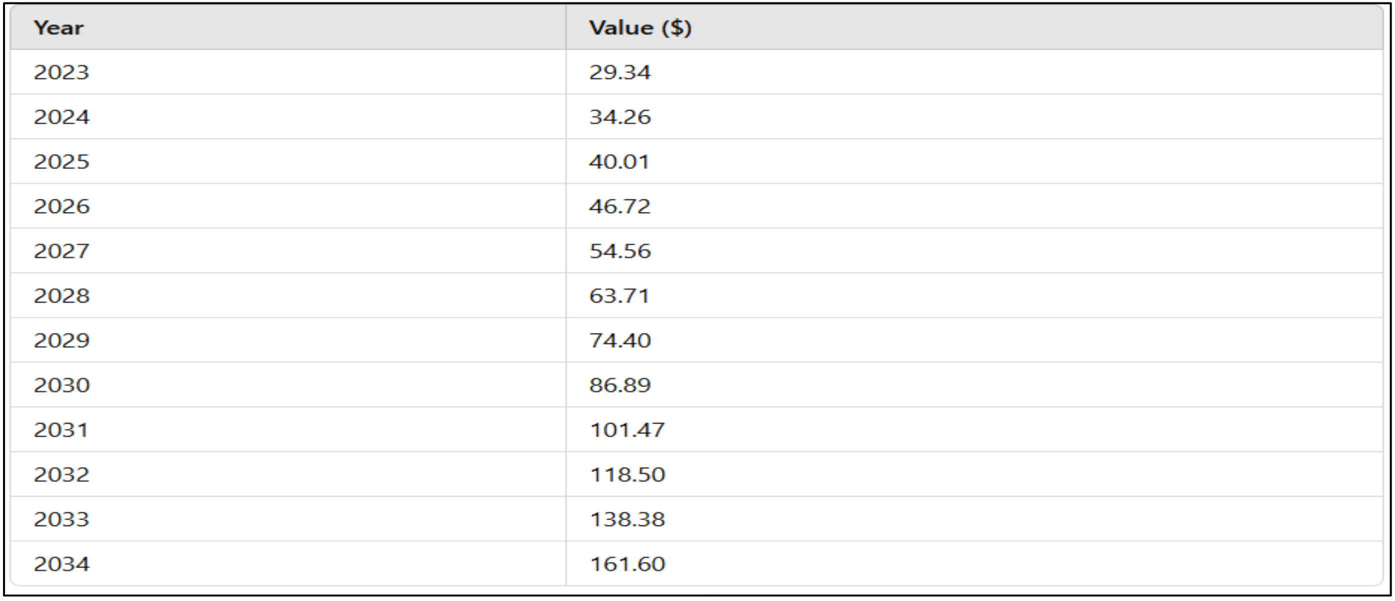


Fig 2 Market Size and Forecast for Zero Trust Security, 2024–2034 (Zoting, 2024).

Table 2 Year by Year Zero Trust Security Market Growth Rate (Zoting, 2024).



Year	Value ($)
2023	29.34
2024	34.26
2025	40.01
2026	46.72
2027	54.56
2028	63.71
2029	74.40
2030	86.89
2031	101.47
2032	118.50
2033	138.38
2034	161.60

The market size of zero trust security is expected to increase from $34.26 billion (2024) to about $161.60 billion in 2034 with 16.78% compound annual growth rate (CAGR) between 2024 and 2025 (Zoting, 2024).

II. AI'S CONTRIBUTION TO IMPROVING ZERO TRUST REGULATIONS

➢ *Identity and Access Management (IAM) Powered by AI*

AI-powered IAM plays a crucial role because it makes adaptive authentication, risk-based access control, and continuous monitoring possible (Ofili, Erhabor, & Obasuyi, 2025). Dynamic security policies that AI-driven IAM adjusts based on real-time risk assessments protect against sophisticated cyber threats that traditional IAM solutions with static policies cannot defend against (Stolworthy RV, 2024).

AI-powered IAM solutions validate access requests by analyzing contextual information together with device attributes and user behavior patterns (Stafford, 2020). An AI-driven IAM system detects unusual login attempts from unexpected geographic locations or irregular access patterns which results in additional authentication challenges or session termination (Ofili, Erhabor, & Obasuyi, 2025).

The implementation of AI-driven facial recognition and behavioral analytics for biometric authentication provides an additional authentication step which strengthens zero-trust security (Ofili, Erhabor, & Obasuyi, 2025). AI-enhanced IAM implementation enables federal agencies to decrease access attempts while improving their adherence to the Zero Trust Framework as per National Institute of Standards and Technology (NIST) (Ofili, Erhabor, & Obasuyi, 2025).

➢ *Analytics of user Behavior and Automatic Anomaly Detection*

The implementation of artificial intelligence (AI) enhances zero-trust security strategies by using automated anomaly detection and behavior-based risk assessment (Radanliev, 2024). Traditional security models depend on predetermined rule sets to identify advanced persistent threats (APTs) and zero-day vulnerabilities, but these rule sets prove insufficient. AI-driven security solutions learn from network traffic patterns to adapt their defenses against new threats (Ofili, Erhabor, & Obasuyi, 2025).

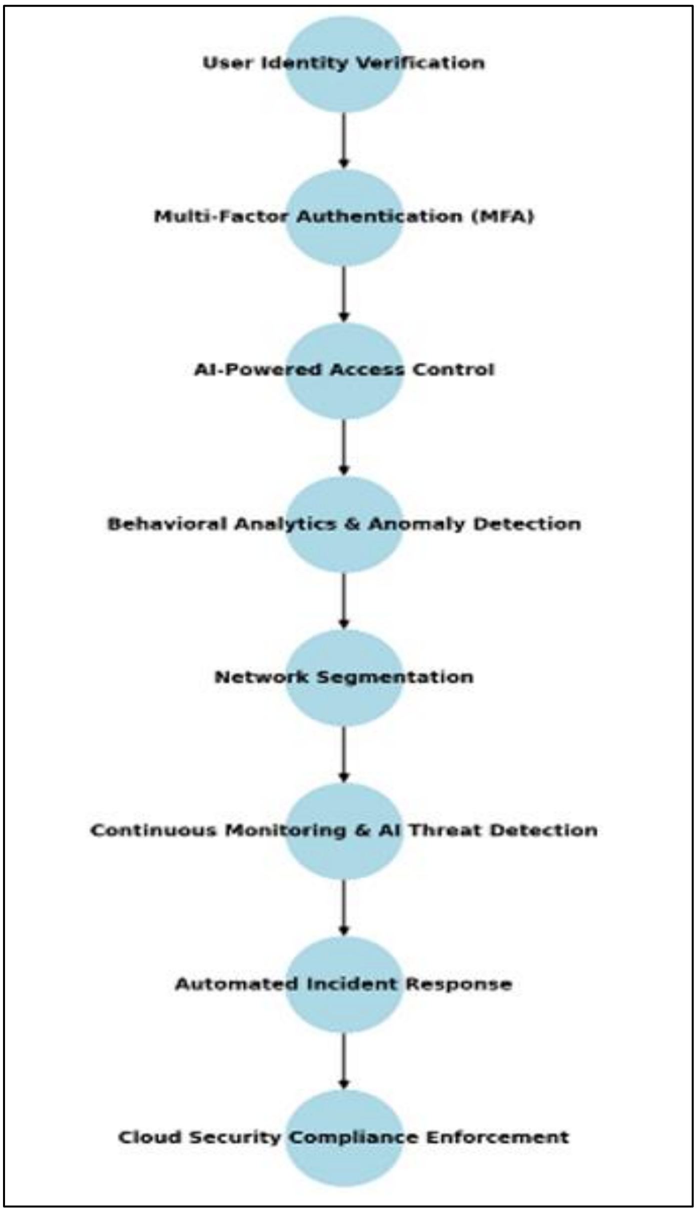

User Identity Verification
Multi-Factor Authentication (MFA)
AI-Powered Access Control
Behavioral Analytics & Anomaly Detection
Network Segmentation
Continuous Monitoring & AI Threat Detection
Automated Incident Response
Cloud Security Compliance Enforcement

Fig 3 AI-Integrated Zero Trust Framework.

AI-driven user and entity behavior analytics (UEBA) detects anomalous activity through the establishment of normal user behavior patterns which enables real-time detection of behavioral deviations. The system would detect and flag government employee activities such as large sensitive material downloads or prohibited file access attempts for human investigation or automatic access restrictions (Ali, 2025).

Federal agencies should implement AI within zero-trust models to achieve predictive security capabilities which enable proactive risk mitigation and automated incident response procedures (Echols, Thomas, Seckman, & Belcher, 2023). AI security solutions enhance the zero-trust framework through their ability to decrease human mistakes and boost operational efficiency (Ofili, Erhabor, & Obasuyi, 2025).

III. EVALUATING AI'S PERFORMANCE IN HYBRID CLOUD SECURITY

Artificial intelligence (AI) integration with hybrid cloud security systems transforms cybersecurity through improved threat identification features and automated mitigation processes and risk reduction. Evaluating its effectiveness requires understanding AI capabilities and limitations together with measurable security improvements that occur in hybrid cloud environments (Paul, 2023).

➢ *Artificial Intelligence Improves Security in Hybrid Cloud:*

- *Threat Detection and Prevention Driven by AI*

AI uses algorithms to monitor network behavior for detecting emerging threats. Behavioral analytics detects suspicious activity immediately to prevent credential-based attacks. The AI-powered IDS and IPS systems use network traffic analysis to detect abnormal behavior patterns (Anandharaj, 2024).

- *Automated Threat Mitigation & Incident Response*

Security orchestration, automation, and response (SOAR) systems can use artificial intelligence to contain threats without human intervention (Anandharaj, 2024). Security teams can respond to threats more quickly through the execution of pre-set activities by automated playbooks. AI can enforce security guidelines across hybrid environments by reducing human error (Anandharaj, 2024).

- *Using Zero Trust in Hybrid Cloud Security*

AI monitors network traffic alongside devices and identities before granting access (Paul, 2023). The system adjusts permissions through Context-Aware Access Control based on observed behavior and risk assessment. The micro segmentation approach divides tasks to prevent lateral movement (Paul, 2023).

IV. AI-POWERED RISK AND COMPLIANCE MANAGEMENT

Cloud security posture management (CSPM) is automated by AI through the detection of setup errors and policy infractions. By keeping a complete report of threats, AI audit logs can help companies meet compliance standards. By examining user access patterns and identifying anomalous activities, AI lessens insider dangers (Inaganti, Ravichandran, Nersu, & Muppalaneni, 2021).

To evaluate the effectiveness of AI in hybrid cloud security, it is important to conduct a detailed analysis of threat detection precision, response effectiveness, compliance enhancements, and risk reduction. (Inaganti, Ravichandran, Nersu, & Muppalaneni, 2021) Although AI has enhanced automated response, threat intelligence, and zero-trust security, enterprises still face challenges such as data bias, adversarial threats, and integration complexity. The future of AI in hybrid cloud security will be more flexible, intelligent, and proactive in countering cyberattacks (Inaganti, Ravichandran, Nersu, & Muppalaneni, 2021).

V. AI-DRIVEN SECURITY MODELS: ETHICAL ISSUES AND DIFFICULTIES

Cybersecurity opportunities and problems are presented by AI-driven security models. These models improve the ability of analysts, automate responses, and improve threat detection (Familoni, 2024). They do, however, present weaknesses and moral issues that should be considered. AI systems face major challenges because biases and mistakes continue to persist in their operations. The use of historical data during machine learning model training enables discriminatory security practices to persist through biased outcomes. (Osasona, 2024). This raises ethical concerns about fairness and potential marginalization of vulnerable groups (Blonder & Feldman-Maggor, 2024).

Another difficulty with AI algorithms is their opacity. It may be challenging to understand security decisions due to the intricacy of AI decision-making, which raises issues of transparency and accountability (Osasona, 2024). In high-stakes security situations when the reasoning behind decisions must be evident, this lack of explainability is significant. Many strategies are put out to address these issues. For AI-driven security solutions to be transparent and trustworthy, explainable AI (XAI) must be developed (Jeyaraman et al., 2023). Responsible AI development and deployment in cybersecurity requires the use of ethical frameworks and regulatory requirements (Familoni, 2024).

The AI Trust Framework and Maturity Model developed by (Mylrea and Robinson, 2023) provides a solution to enhance trust in AI systems. The paper tackles ethical issues in AI-driven security models by applying an "entropy lens" to increase transparency in "black box" AI systems.

AI-driven security models have the potential to greatly enhance cybersecurity, but they also raise ethical issues (Mylrea and Robinson, 2023). A multi-pronged strategy that includes technical fixes, ethical principles, and legal frameworks is required to address these issues and ensure AI is used responsibly (Mylrea and Robinson, 2023).

VI. FUTURE TRENDS

AI plays a vital role in zero-trust security by improving threat detection and security frameworks and enabling automated response (Shahana et al., 2024). Zero-trust architecture (ZTA) with AI integration solves security problems in cloud networks and IoT (Ahmadi, 2024; Li et al., 2022). The ZTA depends on AI systems to analyze massive data sets and find anomalies and patterns that traditional systems would otherwise overlook (Folorunso et al., 2024). The ZTA benefits from machine learning and deep learning technologies which predict threats better and decrease response times and boost detection precision (Folorunso et al., 2024; Shahana et al., 2024). Integration with AI brings new security challenges through adversarial AI and AI-based attacks which need additional research and regulatory oversight to develop strong ZTA systems (Folorunso et al., 2024). The implementation of AI in ZTA creates ethical problems and transparency issues with AI decision systems which need solutions before AI can be widely adopted (Mylrea & Robinson, 2023; Sontan & Samuel, 2024). AI technology in ZTA shows promise because predictive analytics and quantum computing and autonomous systems will transform the field according to (Folorunso et al., 2024). The Trust Framework and Maturity Model for AI offers a solution for AI systems operating within the ZTA (Mylrea & Robinson, 2023). AI technologies will strengthen cybersecurity and maintain regulatory compliance especially in zero-trust security (Ahmadi, 2024; Folorunso et al., 2024; Li et al., 2022).

VII. CONCLUSION

Together, Zero Trust security and artificial intelligence (AI) offer a revolutionary approach to protecting hybrid cloud setups, wherever-changing cyber threats and workloads require proactive, intelligent, and adaptive defenses. Zero Trust, a "never trust, always verify" paradigm, is crucial for safeguarding decentralized cloud systems because traditional perimeter-based security methods are insufficient (Capili, 2024). Enterprises can leverage AI-driven analytics, behavioral monitoring, and automated threat detection to improve authentication, access control, and real-time response. This will greatly improve the security posture. Key findings from this paper highlight: AI enhances Zero Trust by enabling continuous authentication, anomaly detection, and predictive threat intelligence (Horne & Nair, 2021). AI's scalability improves hybrid cloud security by decreasing false positives and speeding up incident response. There are still some issues, such as ethical concerns, adversarial AI attacks, and the requirement for explainable AI in environments where compliance is critical (Paul, 2023). As cyber threats become more sophisticated, building a strong self-learning security architecture for hybrid cloud requires a combination of AI and zero trust. Future research should focus on overcoming legal issues, enhancing adversarial robustness, and standardizing the AI-Zero Trust framework. For hybrid cloud ecosystems, enterprises can implement a proactive, flexible, and future-proof approach to security by implementing AI-driven Zero Trust (Ahmadi, 2024; Li et al., 2022).

REFERENCES

[1]. Parisa, S. K., Banerjee, S., & Whig, P. (2023). AI-Driven Zero Trust Security Models for Retail Cloud Infrastructure: A Next-Generation Approach. *International Journal of Sustainable Development in the field of IT*, *15*(15).

[2]. Horne, D., & Nair, S. (2021). Introducing zero trust by design: Principles and practice beyond the zero-trust hype. Advances in security, networks, and internet of things, 512-525.

[3]. Capili, M. (2024). Simulation-Based Evaluation of Perimeter-Based and Zero Trust Security Implementation on Internet of Things (Doctoral dissertation, The George Washington University).

[4]. Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape. INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS, 9, 712-728.

[5]. Zoting, S. (2024, October 17). Zero Trust Security market size to hit USD 161.60 BN by 2034. https://www.precedenceresearch.com/zero-trust-security-market.

[6]. Ofili, B. T., Erhabor, E. O., & Obasuyi, O. T. (2025). Enhancing Federal Cloud Security with AI: Zero Trust, Threat Intelligence, and CISA Compliance. World Journal of Advanced Research and Review.

[7]. Stolworthy RV, Morgan JC, Combe G, Woodruff NL, Stewart EM. Enhancing Cloud Cybersecurity: Prescriptive Controls for Operational Technology. Idaho National Laboratory (INL), Idaho Falls, ID (United States); 2024 Oct 22.

[8]. Stafford V. Zero-trust architecture. NIST special publication. 2020 Aug;800(207):800-207.

[9]. Radanliev P. Digital security by design. Security Journal. 2024 Dec;37(4):1640-79.

[10]. Ali H. Reinforcement learning in healthcare: optimizing treatment strategies, dynamic resource allocation, and adaptive clinical decision-making. Int J Comput Appl Technol Res. 2022;11(3):88-104. doi:10.7753/IJCATR1103.1007.2399. World Journal of Advanced Research and Reviews, 2025, 25(02), 2377-2400.

[11]. Echols M, Thomas B, Seckman K, Belcher S, Cybersecurity M, Transit RI. Cybersecurity Resilience Assessment Tool to Enhance Public Confidence in Transit. United States. Department of Transportation. Federal Transit Administration; 2023 Aug 1.

[12]. Paul, F. (2023). AI-Powered Threat Detection in Hybrid and Multi-Cloud Environments: Overcoming Security Challenges.

[13]. Anandharaj, N. (2024). AI-Powered Cloud Security: A Study on the Integration of Artificial Intelligence and Machine Learning for Improved Threat Detection and Prevention. J. Recent Trends Comput. Sci. Eng. (JRTCSE), 12, 21-30.

[14]. Inaganti, A. C., Ravichandran, N., Nersu, S. R. K., & Muppalaneni, R. (2021). Cloud Security Posture Management (CSPM) with AI: Automating Compliance and Threat Detection. Artificial Intelligence and Machine Learning Review, 2(4), 8-18. Artificial Intelligence Improves Security in Hybrid Cloud.

[15]. Blonder, R., & Feldman-Maggor, Y. (2024). AI for chemistry teaching: responsible AI and ethical considerations. Chemistry Teacher International, 6(4), 385–395. https://doi.org/10.1515/cti-2024-0014.

[16]. Osasona, F., Farayola, O., Ayinla, B., Atadoga, A., Amoo, O., & Abrahams, T. (2024). REVIEWING THE ETHICAL IMPLICATIONS OF AI IN DECISION, MAKING PROCESSES. International Journal of Management & Entrepreneurship Research, 6(2), 322–335. https://doi.org/10.51594/ijmer.v6i2.773.

[17]. Familoni, B. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. Computer Science & IT Research Journal, 5(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930.

[18]. Mylrea, M., & Robinson, N. (2023). Artificial Intelligence (AI) Trust Framework and Maturity Model: Applying Entropy Lens to Improve Security, Privacy, and Ethical AI. Entropy, 25(10), 1429. https://doi.org/10.3390/e25101429.

[19]. Jeyaraman, M., Balaji, S., Yadav, S., & Jeyaraman, N. (2023). Unraveling the Ethical Enigma: Artificial Intelligence in Healthcare. Cureus, 15(8). https://doi.org/10.7759/cureus.43262.

[20]. Folorunso, A., Olawumi, T., Okonkwo, R., Adewumi, T., & Adewa, A. (2024). Impact of AI on cybersecurity and security compliance. Global Journal of Engineering and Technology Advances, 21(1), 167–184. https://doi.org/10.30574/gjeta.2024.21.1.0193

[21]. Ahmadi, S. (2024). Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. Journal of Engineering Research and Reports, 26(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083.

[22]. Shahana, A., Johora, F. T., Mahmud, M. A. A., Farabi, S. F., Hasan, R., Akter, J., & Suzer, G. (2024). AI-Driven Cybersecurity: Balancing Advancements and Safeguards. Journal of Computer Science and Technology Studies, 6(2), 76–85. https://doi.org/10.32996/jcsts.2024.6.2.9.

[23]. Sontan, A., & Samuel, S. (2024). The intersection of Artificial Intelligence and cybersecurity: Challenges and opportunities. World Journal of Advanced Research and Reviews, 21(2), 1720–1736. https://doi.org/10.30574/wjarr.2024.21.2.0607.

[24]. Li, S., Iqbal, M., & Saxena, N. (2022). Future Industry Internet of Things with Zero-trust Security. Information Systems Frontiers, 26(5), 1653–1666. https://doi.org/10.1007/s10796-021-10199-5.