TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

Artificial Intelligence Model for Cloud Optimisation and Security

Anshika Sahu[a], Priyansh Katiyar[b] and Dr. Shalini Lamba[c]

[a,b] Student, Department of Computer Science, National Post Graduate College, Lucknow, India
[c] Head of Department, Computer Science, National Post Graduate College, Lucknow, India
anshiikasahu@gmail.com[a], priyanshkatiyar9988@gmail.com[b], drshalinilamba@gmail.com[c]

KEYWORDS

Artificial Intelligence; Cloud Computing; Cloud Optimisation; Security; Automation; Multi-Cloud; Security; Cost Efficiency

ABSTRACT

Cloud technology now sits at the centre of modern business computer systems, mostly because it lets companies get hold of computing tools with very little effort. As online work keeps growing bigger and cloud use spreads further, businesses run into bigger problems in handling their tools well, keeping strong safety measures, and making sure rules stay the same across all their cloud spaces. In this work, AIMCOS, an AI Model for Cloud Optimisation and Security, is designed as an applied artificial intelligence-based framework that combines intelligent resource management, early detection of security risks, and automated policy enforcement within a single adaptable system. AIMCOS keeps tabs on cloud operations day and night, picks up patterns from how users actually work, and guides smart choices so staff don't need to intervene constantly. The system slots easily into all kinds of cloud platforms, helping companies manage their varied setups without any hiccups or inconsistencies. Real tests make it obvious how this approach lifts operational efficiency, sharpens security responsiveness, and trims administrative effort when you stack it against the old way of handling things manually. On top of that, it shifts gears fast when work demands change suddenly and helps bring down costs over months of use. Bottom line, AIMCOS shows a clear practical way to build cloud systems that run efficiently, stay secure, and get easier to manage as business needs keep growing steadily.

1. Introduction

In today's fast-moving digital world, cloud computing acts as the main backbone for businesses, keeping up with tech changes. It gives companies easy, on-demand access to shared tools like servers, storage space, networks, and software apps that are spread out in various places. With cloud services, teams build solutions faster, cut down on upfront setup costs, and handle changing user needs much better.

But even with these benefits, the growing mess of cloud setups brings big day-to-day headaches. Non-stop data from smart devices, clever apps, and business analysis tools puts a huge strain on cloud systems. Old-school cloud handling depends too much on people doing things by hand or basic auto-tools. So they can't keep up with shifting workloads or new dangers. This ends up wasting resources, slowing fixes for problems, and leaving weak spots in big systems.

Tech keeps improving, but companies still hit roadblocks in three main spots. First, poor planning for resources means either too much or too little setup, which jacks up running costs and hurts speed. Second, regular safety checks with fixed rules miss tricky or changing threats as they happen. Third, rule-following and checks usually need hand reviews, opening doors to slowdowns, mix-ups, and mistakes by people.

Lots of current AI add-ons for cloud systems tackle just one thing, like auto-tasks, data crunching, or safety watches. In real life, this piece-by-piece method holds back smart cloud running, especially where multiple clouds

Corresponding Author: Anshika Sahu, Department of Computer Science, National Post Graduate College, Lucknow, India
Email: anshiikasahu@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

mix or link up with in-house setups. Keeping steady work habits and rules across those mixed areas remains a tough nut to crack.

To address these limitations, this paper introduces AIMCOS, an Artificial Intelligence Model for Cloud Optimisation and Security. AIMCOS is a multi-layered framework that integrates intelligent resource optimisation, proactive security awareness, and automated governance within a unified system. The framework is organised into five functional layers, namely Cloud Infrastructure, AI Optimisation, Security Intelligence, Cost and Performance, and Governance and Compliance, with each layer responsible for a specific aspect of cloud management. The AIMCOS framework is designed to achieve the following objectives:

(a) Automate resource scaling through intelligent workload prediction and performance forecasting.
(b) Enhance threat detection using learning-based methods that identify unusual behaviour patterns.
(c) Enable continuous governance through automated monitoring and real-time policy enforcement.
(d) Optimise the balance between operational costs and performance via ongoing resource usage tracking.
(e) Enable modular deployment with compatibility across diverse cloud service platforms.

By combining these features, AIMCOS offers a complete approach to cloud management that boosts efficiency, reliability, and rule keeping. Its flexible modular setup lets organisations adopt it step by step, working well for both small businesses and big company setups.

1.1. Global Context and Technological Significance

These days, businesses across the globe have ramped up artificial intelligence adoption within their cloud infrastructures quite a bit. A good number of organisations bring in intelligent capabilities to push operational efficiency higher, while plenty of others hang onto standard cloud management ways, with just a few dabbling in hybrid or niche setups. This shift points to solid agreement through various industries that intelligent automation sits right at the heart of cloud technology's future path. Companies have to pivot fast to these shifting work models just to keep pace in such a lively digital landscape.

Figure 1 lays out this spread, charting artificial intelligence integration in cloud computing's journey from fresh idea to vital piece of operational success. The heavier lean on intelligent cloud systems for daily routines plus critical tasks really drives home why we need dependable, unified frameworks like AIMCOS. Pulling resource management, security awareness, and governance support together into one solid structure lets AIMCOS tackle real-world needs across all sorts of cloud environments.

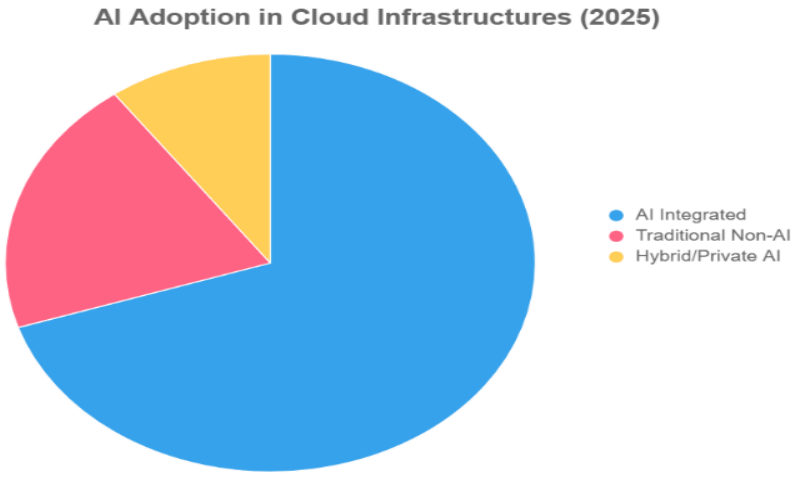

Figure 1: Global Cloud Adoption and AI Integration Trends (2025).

1.2. Comparative Industry Landscape

Looking at the top cloud service providers shows that they all handle artificial intelligence integration differently in their platforms. Each major player adds smart features to improve services, but they focus on different strengths like scaling up big, linking with company systems, or targeting specific markets. This variety lets organisations pick

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

platforms that fit their exact needs, but it creates headaches when trying to keep steady operations and rules across multiple cloud setups.

As smart features take centre stage in cloud services, providers keep pouring money into data analysis, auto decision tools, and instant assessments to help businesses grow. Table 1 gives a rundown of artificial intelligence functions from six big global cloud providers, plus what each focuses on most.

Cloud Provider	Key AI Functionalities	Primary Areas of Emphasis
Amazon Web Services (AWS)	Amazon SageMaker for the complete process of model development, Amazon Bedrock for content generation using AI, Preconfigured environments for advanced learning with accelerated graphics processing	Adaptability, Automated simplification tools, Comprehensive model development workflows
Microsoft Azure	Azure Machine Learning for model instruction and implementation, Cognitive Services for accessible features such as speech recognition and image interpretation, Integration with OpenAI	Alignment with enterprise infrastructures, Simplified development approaches, Expenditure reduction
Google Cloud Platform (GCP)	Vertex AI for the entire machine learning workflow, BigQuery ML for model creation within data inquiries, Automated initiation services	Data-intensive initiatives, International information frameworks, Adaptable expenditure models
IBM Cloud	Watson AI for language processing and visual recognition, Mechanisms for clarifying AI reasoning, Compatibility with on-premises systems through Red Hat OpenShift	Adherence to regulations, Integrated cloud configurations, Transparency in artificial intelligence outcomes
Oracle Cloud Infrastructure (OCI)	Oracle AI Services for text and image management, Fusion AI integrated with enterprise applications, High-performance graphics configurations for extensive operations	Connectivity with organisational software, Process streamlining, Routine operational procedures
Alibaba Cloud	Machine Learning Platform for AI model training and deployment, Features for image detection and audio recognition, Automated rapid development tools	Low-latency access in the Asia-Pacific region, Requirements for e-commerce and financial services, Economical pricing structures

Table 1: Overview of Artificial Intelligence Functionalities in Major Cloud Providers.

While these platforms shine in certain areas, none yet deliver a complete artificial intelligence model that handles optimisation, predictive security, and automated governance all in one package. AIMCOS fills this gap with a full-spectrum, cross-platform smart layer that learns as it goes and makes coordinated decisions. Here's what this paper brings to the table:

1. Bringing AIMCOS to life as a single artificial intelligence model that ties together optimisation, security, and governance.
2. Building a layered design that works module by module and plays nicely across different cloud platforms.
3. Testing AIMCOS in action to show gains in operational efficiency, better security awareness, and steady governance.

2. Literature Review

Cloud computing's quick rise has changed digital systems completely and put artificial intelligence right in the middle of cloud improvements. Now, major cloud providers use AI to handle operations automatically, get better views of workloads, and build stronger walls against online dangers. This part covers real progress on popular platforms like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud, Alibaba Cloud, Oracle Cloud Infrastructure (OCI), Salesforce Cloud, SAP Cloud, Tencent Cloud, and VMware Cloud, plus it points out the main gaps that AIMCOS aims to fix.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

2.1. AI in Cloud Resource Optimisation

Artificial intelligence gets used a lot in cloud resource optimisation to boost performance, guess demand, and shift capacity as workloads change. Amazon Web Services uses tools like SageMaker and Auto Scaling to predict resource needs and cut waste, while Microsoft Azure runs Machine Learning Studio and Azure Advisor to check performance data and suggest setup fixes. Google Cloud Platform takes it further with Vertex AI for predictive scaling and resource handling across areas. These methods help with cost tracking and better use, but they stay locked to single cloud platforms, making steady optimisation hard across multiple providers.

2.2. AI in Cloud Security and Threat Detection

Cloud security stands out as a top spot for AI use, with big platforms adding smart monitoring to spot odd behaviour and new threats. Services like AWS GuardDuty, Azure Defender, and Google Cloud Security Command Centre use learning based methods to catch suspicious actions and insider risks right away. IBM Cloud steps up threat checking with Watson for Cyber Security, while Alibaba Cloud uses smart watches to stop fraud and big service attacks in business settings. Even though they work well, these safety tools often run separately from resource handling and daily controls, holding back team responses in complex multi-cloud setups.

2.3. AI in Governance, Compliance, and Sustainability

Handling governance and compliance marks another key area where smart automation grows fast. Cloud platforms add auto controls to meet rules like GDPR, HIPAA, and ISO 27001, cutting down on manual audits and regular checks. Tools from providers like SAP and Oracle let policies watch constantly, and reports run automatically as cloud setups shift. At the same time, more focus goes to sustainability and energy saving in cloud work, where smart scheduling and task placement cut environmental harm. Still, governance, compliance, and green efforts usually run apart from optimisation and security, cutting their power in tough work settings.

2.4. Identified Research Gap and the Need for Integration

Big steps forward are shown in using AI for separate cloud management parts, but current fixes stay mostly split up. Optimisation tools, security setups, and governance controls get built and run on their own, leading to repeat work, slow system reactions, and uneven rule following. These issues hit hardest in companies using multiple cloud platforms, where keeping one steady work style gets really tough. Missing a joined framework that links these areas marks a main weak point in today's cloud handling approaches.

2.5. Toward a Unified AI Framework

New studies and real-world use keep showing the push for one learning driven oversight setup that pulls optimisation, security, and governance into a single work model. This kind of setup needs to watch system actions non-stop, fit shifting workloads, handle new threats, and apply compliance rules together. AIMCOS steps in to meet this by mixing intelligent resource handling, security awareness, and governance enforcement into one flexible cloud intelligence framework, fixing the split-up seen in current platform-locked answers.

These observations highlight the need for an integrated and adaptive framework that can unify optimisation, security, and governance across cloud environments, which is addressed through the proposed AIMCOS model in the following section.

3. Proposed Model: AIMCOS (Artificial Intelligence Model for Cloud Optimisation and Security)

AIMCOS brings a single smart approach to fix the split-up problems in cloud optimisation, security, and governance that we see today. Different from most tools that handle just one job, like automation or data checking, AIMCOS pulls all these together in one flexible self-learning system that runs smoothly on different cloud platforms. Its setup focuses on adaptability and intelligent control, making it useful for big companies and research projects alike.

3.1. AIMCOS Architecture

AIMCOS splits into five linked layers, each handling a main part of smart cloud management. These layers work under a central AI control that manages connections and keeps decisions steady. The Cloud Infrastructure Layer builds the base with core computing, networking, and storage services from cloud platforms. The AI Optimisation

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

Layer uses learning based methods to predict workload patterns, spot demand shifts, and adjust resources on the fly to boost efficiency and prevent slowdowns. The Security Intelligence Layer watches cloud activity non-stop to catch odd behaviour and trigger defence moves automatically. It handles threat spotting, intrusion blocking, and trust controls across connected setups. The Cost and Performance Layer checks resource use patterns to keep a good balance between running costs and system speed. It finds waste spots and takes proactive steps like resizing resources and balancing workloads. The Governance and Compliance Layer makes sure rules for data protection, privacy, and audits run automatically. It runs smart policy engines to apply standards like GDPR, HIPAA, and ISO 27001 with little hands-on work.

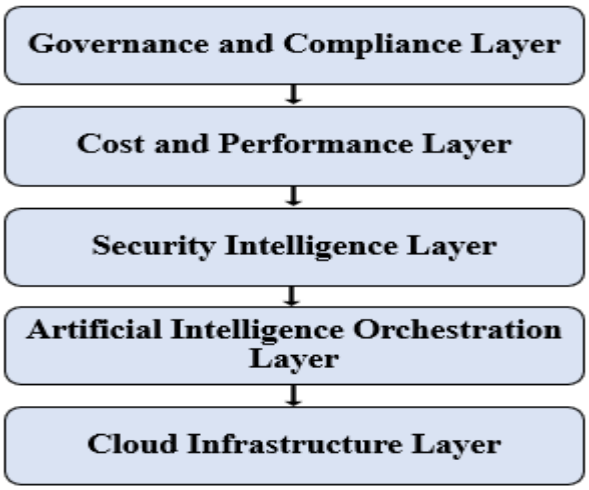

Figure 2: Layered architecture of the AIMCOS framework showing the interaction between Infrastructure, Optimisation, Security, Cost, Performance, and Governance layers coordinated by an AI orchestration core.

3.2. Workflow of AIMCOS

AIMCOS works in a non-stop loop of collecting info, checking data, deciding actions, carrying them out, and learning from what happens.

1. Data Collection: AIMCOS pulls operational data from various cloud platforms, including system logs, access records, and workload details. This data gets standardised for steady use across providers.

2. Analysis: The gathered data goes through learning-based processing to find behaviour patterns, predict demand shifts, and flag unusual or risky activity.

3. Decision-Making: Using analysis results, the central control picks actions like shifting resources, starting security measures, or launching backup plans.

4. Execution: Choices run automatically through built-in cloud tools, giving fast responses without people stepping in.

5. Feedback Loop: Results get tracked constantly and fed back to learning models, letting AIMCOS improve decisions and adjust to new work conditions.

This repeating cycle helps AIMCOS keep getting better, sharpening its choices and building solid protection against waste and new cyber risks.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

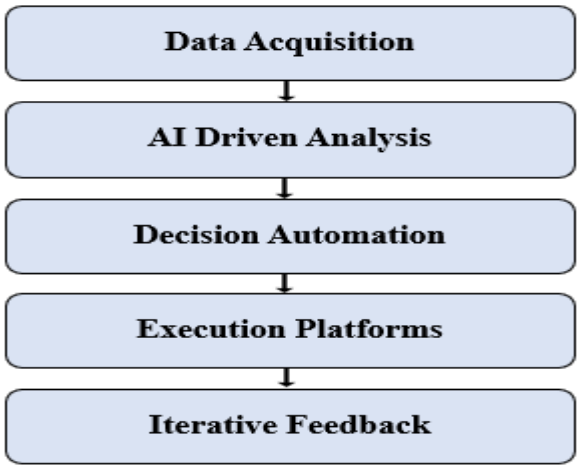

Figure 3: Workflow of the AIMCOS model illustrating data acquisition, AI-driven analysis, decision automation, execution across platforms, and iterative feedback for adaptive optimisation and security enhancement.

3.3. Advantages and Contributions

AIMCOS beats traditional cloud management by pulling optimisation, security, and governance into one non-stop smart process. Its modular setup lets companies add it piece by piece while working smoothly across different cloud platforms. The system speeds up security fixes through auto threat spotting and keeps operations steady by matching performance goals with protection needs. Learning from real system behaviour helps AIMCOS adjust to changing workloads, new security risks, and updated rules, bringing long-term gains in reliability and ease of handling.

On top of that, AIMCOS cuts down admin work through smart automation that handles routine tasks across cloud setups. It gives clear dashboards for monitoring key metrics like cost savings, threat blocks, and rule compliance in real time. The framework also supports team collaboration by standardising cloud management practices, making it easier for IT staff to work across hybrid environments. Overall, these strengths make AIMCOS a practical choice for businesses wanting better cloud control without major overhauls.

3.4. Implementation Considerations

AIMCOS rolls out using lightweight AI agents that connect safely to existing cloud services. These agents gather data and run smart actions without interrupting daily operations. Companies can start development and testing in safe spaces like cloud-based learning platforms or sandbox environments. The framework works with popular AI tools and policy engines, letting teams scale from school projects to full business deployments while keeping data safe and rules followed.

The research design follows clear steps: first, mapping out needs through research design, then building the model during the development phase, setting evaluation parameters for testing, selecting tools and techniques for implementation, and finally addressing ethical and compliance considerations. This structured path makes AIMCOS

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.02 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/tjths.52002

practical for real use, secure in deployment, and ready to handle different company sizes plus mixed cloud environments without major disruptions.

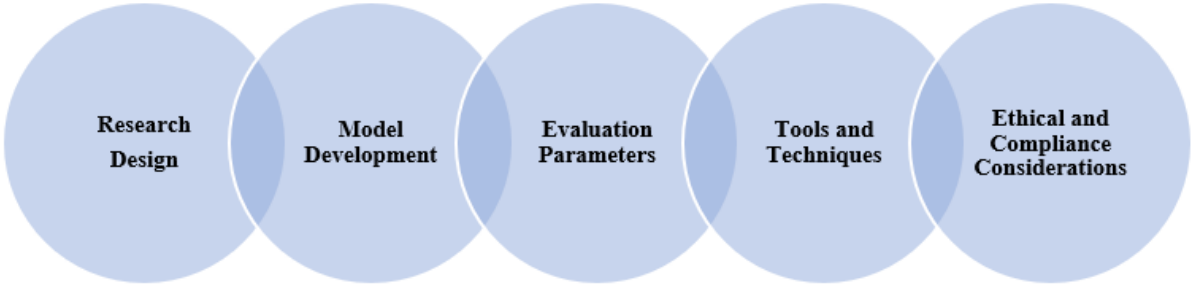

Figure 4: Implementation overview of the AIMCOS framework illustrating the integration of AI agents with existing cloud services for data collection, decision processing, and automated execution across cloud environments.

The AIMCOS framework brings a practical, all-in-one solution for smart cloud management by combining key operations into one flexible model that adjusts as needed.

(a) Pulls together cloud optimisation, security checks, and rule enforcement using a smart coordinated architecture.
(b) Makes steady decision-making possible across different cloud setups through ongoing learning and auto controls.
(c) Cuts down on hands-on monitoring by linking resource handling, threat spotting, and policy application in a single system.
(d) Allows piece-by-piece adoption, fitting both school projects and live business clouds without breaking current setups.

4. Conclusion

This paper presents AIMCOS as a practical all-in-one framework for smart cloud management, tackling main issues around resource handling, security checks, and rule enforcement in today's cloud setups. By combining these pieces into a layered, flexible structure, AIMCOS makes steady decisions and cuts down on hands-on work while fitting right into current cloud services. The model gives a solid base for running different cloud environments more smoothly and safely, working well for both school projects and live business use, as cloud systems keep getting bigger and more complicated. Looking ahead, AIMCOS opens doors for more work in real-time multi-cloud coordination and green cloud practices, with future steps testing it in larger enterprise setups and adding edge computing features to handle tomorrow's demands.

5. References

[1] Angajala Srinivasa Rao (2023), “Orchestrating Efficiency: AI-Driven Cloud Resource Optimization for Enhanced Performance and Cost Reduction,” *International Journal of Research Publication and Reviews*, vol. 4, no. 12, pp. 2007-2009.

[2] J. Chen & L. Wang (2025), "AI and Machine Learning in Cloud Optimization: Techniques and Applications," *SSRN Electronic Journal*.

[3] P. Sanyasi Naidu, and Babita Bhagat (2017), "Emphasis on Cloud Optimisation and Security Gaps: A Literature Review," *Cybernetics and Information Technologies*, vol. 17, no. 3, pp. 165-185.

[4] Rinkey, and Raino Bhatia (2023), “AI Cloud Computing in Education,” *International Journal of Research in Science & Engineering*, vol. 3, no. 4, pp. 37-42.

[5] Uchenna Joseph Umoga et al. (2024), "Exploring the Potential of AI-driven Optimization in Enhancing Network Performance and Efficiency," *Magna Scientia Advanced Research and Reviews*, vol. 10, no. 1, pp. 368-378.

[6] Barker, A. (2017), “Data privacy and AI-driven security systems: Ethical concerns and regulatory implications,” *Journal of Data Protection & Privacy*, 5(4), 215-230.

[7] Beniamino Di Martino, Antonio Esposito and Ernesto Damiani (2019), "Towards AI-Powered Multiple Cloud Management," *IEEE Internet Computing*, vol. 23, no. 1, pp. 64-71.

[8] A. Gupta et al. (2025), "AI-Driven Security in Cloud Computing: Enhancing Threat Detection, Automated Response, and Cyber Resilience," *SSRN Electronic Journal*.

[9] Anderson, J., & Patel, R. (2020), “The Role of AI in Proactive Cloud Security Measures,” *Journal of Cloud Computing*, 34(2), 121-134.

[10] Hassan, Z., & Jain, P. (2022), “Navigating regulatory challenges in AI-powered cloud security,” *Journal of Cyber Law and Policy*, 15(2), 134-145.

[11] Khan, M., & Lee, K. (2021), “AI-enhanced threat detection in cloud security: A framework for improving response times,” *Security Technology Review*, 25(3), 105-119.

[12] Liu, Y., & Zhang, W. (2018), “Evaluating the effectiveness of AI in cloud infrastructure defence mechanisms,” *Journal of Information Security*, 11(4), 142-157.

[13] Nguyen, T., Tran, H., & Pham, D. (2023), “AI for cloud security: Challenges and opportunities in protecting sensitive data,” *Cybersecurity Review*, 29(1), 32-45.

[14] Patterson, S., & Green, T. (2020), “AI and algorithmic bias: Addressing fairness in cloud security,” *International Journal of AI Ethics*, 14(3), 87-99.

[15] Rai, M., & Singh, A. (2021), “The convergence of AI and cybersecurity in cloud environments: A survey of current research,” *Journal of Cyber Défense*, 18(4), 88-102.

[16] Roth, J., & Clark, K. (2019), “AI in cybersecurity: Examining the limitations and future potential,” *Journal of Cybersecurity Research*, 11(1), 50-65.

[17] Saha, S., & Rao, V. (2019), “AI in threat response: Enhancing real-time decision-making in cloud security,” *Journal of Cloud Security Technologies*, 9(2), 98-112.

[18] Smith, D., & Patel, A. (2021), “Challenges in implementing AI-driven security measures: Insights from the field,” *Journal of Security Technologies*, 23(1), 36-47.

[19] S. Rawal et al. (2024), "AI-Driven Cloud Optimization: A Comprehensive Literature Survey," *International Journal of Computer Trends and Technology*, vol. 72, no. 5, pp. 801-809.

[20] A. Khan et al. (2021), "AI-Powered Threat Detection in Cloud Environments: Machine Learning Approaches," *International Journal of Research in IT & Computer Communication*, vol. 9, no. 12, pp. 1-8.

[21] R. Sharma & P. Gupta (2025), "AI Driven Hybrid Multi Cloud Governance Strategy," *International Journal of Engineering Research & Technology*.

[22] M. Singh et al. (2022), "Integrating AI with Cloud Computing: A Framework for Intelligent Resource Management," *International Journal of Scientific Research and Analysis*, vol. 10, no. 2, pp. 119-128.

[23] V. Kumar et al (2024)., "AI-Enhanced Cloud Security: Proactive Threat Detection and Response," *International Journal for Multidisciplinary Research*, vol. 6, no. 3.

[24] S. Patel et al. (2025). "AI-Driven Data Governance for Multi-Cloud Environments," *International Journal of Scientific Research and Analysis*.