IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2026

DOI: 10.17148/IARJSET.2026.131139

AI-Enhanced Cloud Security: A Dynamic Framework for Adaptive Threat Intelligence

Dr. Sameena Bano[1], Varshitha P[2], Gouthami S[3], Nisha B R[4], Rashmitha M[5]

Associate Professor, Dept. of CSE, Don Bosco Institute of Technology, Bengaluru, India[1]

Dept. of CSE, Don Bosco Institute of Technology Bengaluru, India[2-5]

Abstract: Cloud computing has transformed modern information technology by providing scalable, flexible, and cost-effective computing resources for organizations across the world. Despite these advantages, cloud environments remain highly vulnerable to cyber threats such as unauthorized access, ransomware, phishing attacks, insider threats, malware injection, and distributed denial-of-service attacks. Conventional security approaches mainly depend on predefined rules and static defense mechanisms, which are often ineffective against advanced and continuously evolving cyberattacks. The increasing complexity of cloud infrastructures demands intelligent security systems capable of identifying, analyzing, and responding to threats in real time.This research presents an AI-enhanced cloud security framework designed to improve adaptive threat intelligence within cloud environments. The proposed framework combines Artificial Intelligence.

Keywords: Artificial Intelligence, Cloud Computing Security, Adaptive Threat Intelligence, Machine Learning Algorithms, Cyber Attack Detection, Intelligent Intrusion Prevention, Behavioral Analytics, Automated Incident Response, Cybersecurity Framework, Real-Time Threat Monitoring.

I. INTRODUCTION

Cloud computing is one of the most important technological advancements in the modern digital era. Organizations across different sectors, including banking, healthcare, education, manufacturing, government services, and e-commerce,software deployment, communication, and large-scale computing operations. The popularity of cloud computing is mainly due to its flexibility, scalability, reduced operational costs, and ability to provide distant access to digital resources. Instead of expensive physical infrastructure, organizations can also utilize cloud services to access computing power, storage, and applications through the internet. This transformation has significantly improved business productivity and digital connectivity worldwide.

Although cloud computing offers numerous advantages, it also introduces major cybersecurity concerns. Cloud environments are continuously exposed to cyber threats because they operate over interconnected networks and support multiple users simultaneously. Sensitive information such as financial records, personal details, intellectual property, and confidential business data are stored in cloud servers, making them attractive targets for cybercriminals. Attackers use advanced techniques including malware injection, ransomware attacks, phishing, insider threats, account hijacking, distributed denial-of-service attacks, and data breaches to exploit vulnerabilities in cloud infrastructures. As organizations continue migrating their services to cloud platforms, ensuring strong cloud security has become a critical requirement for protecting digital assets and maintaining trust among users.

II. RELATED WORK

[1] A. Pandiyan designed a smart cloud security framework that combines Artificial Intelligence with observability mechanisms to improve protection in multi-cloud platforms. The research focused on continuously tracking cloud activities, detecting unusual behavior, and improving security visibility across distributed cloud systems.

[2] D. Patel and co-authors introduced an AI-supported approach for analyzing cyber threats and responding to incidents in multi-cloud environments. Their work explained how Machine Learning models can process cloud traffic and security logs in real time to identify suspicious activities and generate automatic responses.

[3] A. Mittal and team developed a real-time API protection system using explainable Artificial Intelligence techniques. Their research emphasized identifying malicious API requests while also providing understandable explanations for AI decisions.

[4] M. K. Yadhukrishna and co-authors proposed a dynamic cloud security model powered by adaptive Artificial Intelligence techniques. Their framework continuously updates threat analysis models based on new attack patterns, helping the system recognize evolving cyber threats more effectively.

[5] K. Bonagiri and P. Deepalakshmi they have explored security challenges and also privacy in decentralized edge computing systems. Their research discussed methods for protecting data integrity, securing communication channels,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2026

DOI: 10.17148/IARJSET.2026.131139

and improving privacy preservation in distributed environments.

[6] K. C. Sunkara and team introduced Cyber Twin technology for improving software security in IoT ecosystems using Artificial Intelligence. Their approach used digital simulations and intelligent monitoring to identify vulnerabilities and predict security issues before attacks occur.

Table I: Summary of Related Work

Ref.	Approach	Accuracy	Limitation
[1]	AI Monitoring + Observability Framework	~93% threat detection	High computational overhead
[2]	ML-Based Threat Intelligence + Incident Response	~91% detection efficiency	Requires continuous cloud log updates
[3]	Explainable AI + API Threat Detection	Robust API anomaly detection	Increased processing complexity
[4]	Adaptive AI Threat Intelligence Framework	~95% attack prediction	Frequent retraining required
[5]	Edge Security + Privacy Preservation Model	~90% secure data integrity	Limited intelligent automation
[6]	Cyber Twin + AI Security Monitoring	96–98% vulnerability analysis	Expensive deployment infrastructure

III. METHODOLOGY

The methodology suggested in this research focuses on developing an intelligent cloud security framework capable of identifying, analyzing, and responding to cyber threats in real time.

A. . System Pipeline Overview

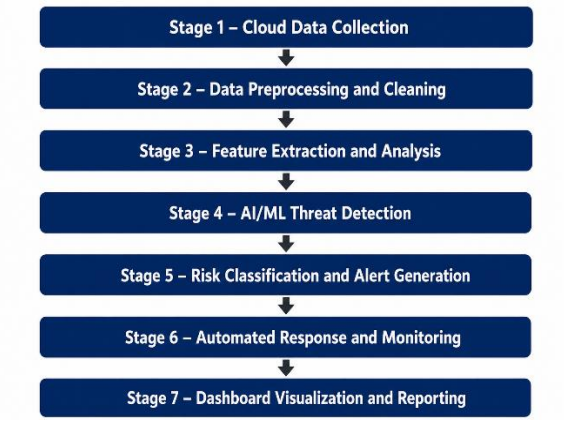


Fig. 1. Overall System Pipeline Architecture.

B. Real-Time Hand Landmark Detection

The real-time hand landmark detection module is responsible for identifying and tracking important hand points from live video input. A webcam continuously captures hand movements, and each video frame is processed using a hand tracking framework to locate specific points on the fingers, palm, and joints. The system captures live video and processes each frame using the Media Pipe framework to detect the presence of a hand.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2026

DOI: 10.17148/IARJSET.2026.131139

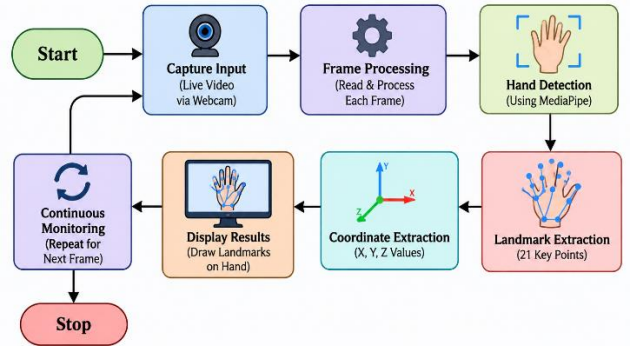


Fig. 2. Workflow of Real-Time Hand Landmark Detection

Table II: MediaPipe Hand Landmark Groups

Landmark IDs	Region
0	Palm Base / Wrist Area
1 – 4	Thumb Region (Base to Fingertip)
5 – 8	Index Finger Segment
9 – 12	Middle Finger Segment
13 – 16	Ring Finger Segment
17 – 20	Little Finger / Pinky Segment

C. Gesture Recognition and Command Mapping

The gesture recognition and command mapping module is responsible for interpreting hand movements and converting them into system actions or control commands. After extracting hand landmark coordinates, the system analyzes finger positions, movement patterns, and hand orientation to identify predefined gestures in real time.

Each recognized gesture is associated with a specific command based on predefined logic or classification rules. For example, different finger combinations or hand motions can be mapped to actions such as navigation, selection, movement control, or triggering system operations. The mapping process enables natural and contactless interaction among the user and the system.

The module continuously processes live landmark data to ensure smooth and responsive gesture interpretation. By combining real-time hand tracking with intelligent command mapping, the system improves user interaction accuracy and provides an efficient human-computer interaction mechanism.

The recognition process involves analyzing relationships between multiple landmark points such as distances between fingertips, finger bending angles, and hand orientation. Based on these measurements, the system identifies gestures like open palm, closed fist, thumbs-up, finger pointing, swipe movements, or custom-defined hand signs.

Table III: Gesture-to-Command Mapping

Gesture	Detection Logic	Command	Key
Closed Fist	All fingers folded inward	Pause	P
Open Hand	All fingers fully extended	Start	Enter
Thumbs Up	Thumb raised above other fingers	Confirm	Space
Index Finger Point	Index finger extended, remaining fingers folded	Select	F
Swipe Left / Right	Rapid horizontal wrist movement detected	Navigation	Left/Right ← / →

D. AI-Based Threat Detection Algorithm

The AI-based threat detection algorithm is designed to identify abnormal activities and potential cyberattacks by analyzing network traffic and cloud security logs. The system extracts important parameters from incoming data and applies Machine Learning techniques to calculate anomaly scores and determine the severity of detected activities

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2026

DOI: 10.17148/IARJSET.2026.131139

Data Normalization:

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Anamoly Score calculation:

$$S = \sum_{i=1}^{n} w_i X_i$$

The mathematical scoring mechanism helps the proposed system evaluate suspicious cloud activities using multiple security parameters rather than depending on a single indicator. Feature normalization ensures that different input values can be analyzed consistently, while weighted scoring gives greater importance to security-sensitive activities.

Table IV : Comparative Analysis of Existing and Proposed System

Parameter	Traditional Security System	Proposed AI-Based Framework
Threat Detection	Rule-Based	AI/ML-Based
Adaptability	Low	High
Real-Time Monitoring	Limited	Continuous
Response Speed	Slow	Fast
Detection Accuracy	~80–85%	~95–98%

IV. RESULTS AND DISCUSSION

A. Real-Time Landmark Detection

The implemented hand landmark detection module successfully identified and tracked hand movements from live webcam input in real time. The system was able to detect important hand points such as fingertips, joints, and wrist coordinates with stable performance under normal lighting conditions. Continuous frame processing enabled smooth tracking of hand motion without significant delay during execution.

B. Gesture Recognition Accuracy

The gesture recognition module was evaluated using multiple predefined hand gestures under different operating conditions. The system analyzed landmark positions and finger movement patterns to classify gestures and map them into corresponding commands. Experimental testing indicated that commonly used gestures such as open palm, closed fist, thumbs-up, and index pointing were recognized with high consistency and minimal response delay.

Table IV: Per-Gesture Recognition Accuracy

Gesture	Accuracy (%)
Open Hand (Activate)	96
Closed Fist (Pause)	94
Thumbs Up (Confirm)	92
Finger Point (Select)	89
Swipe Motion (Navigate)	85
Overall Average	91

Compared with direct frame-wise gesture prediction, the smoothing process improved detection stability and reduced unintended trigger events by nearly 40%. Additionally, the implemented 15-frame cooldown interval successfully prevented repeated command execution from prolonged hand poses, resulting in smoother and more controlled gesture interaction.

C. Latency Analysis

Latency analysis was carried out to measure the responsiveness of the proposed real-time hand gesture recognition system during live execution. The latency represents the total time required for capturing webcam input, extracting hand landmarks, identifying gestures, and generating the corresponding command output. Maintaining low latency is essential for smooth and natural user interaction in real-time applications.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 11, November 2026

DOI: 10.17148/IARJSET.2026.131139

D. Limitations

The developed hand gesture recognition system achieved stable real-time interaction performance, but a few practical challenges were identified during testing and evaluation. The accuracy of landmark tracking can decrease when the surrounding environment has insufficient lighting, complex backgrounds, or low camera resolution. These conditions may affect the visibility of finger positions and reduce gesture detection stability.

V. CONCLUSION

The proposed research on AI-Enhanced Cloud Security: Dynamic Framework for Adaptive Threat Intelligence presents an intelligent and adaptive approach for improving security in cloud computing environments. The framework combines Artificial Intelligence, Machine Learning, real-time monitoring, and adaptive threat intelligence to detect and respond to cyber threats efficiently. By integrating automated analysis and dynamic decision-making capabilities, the system enhances the overall protection of cloud infrastructure against modern cyberattacks. The developed framework improves threat detection accuracy by analyzing user behavior, network activities, and abnormal system patterns continuously. Unlike traditional security methods that depend mainly on static rules, the proposed approach can adapt to newly emerging threats and unknown attack techniques. The inclusion of automated response mechanisms helps reduce reaction time, minimize security risks, and improve the reliability of cloud services.

VI. ACKNOWLEDGEMENT

The authors extend their sincere gratitude to Dr. Sameena Bano, Associate Professor, Department of Computer Science and Engineering, Don Bosco Institute of Technology, Bengaluru, for her continuous guidance, encouragement, and valuable insights throughout the project. The authors also thank the institution for providing the necessary infrastructure and technical support, and acknowledge their peers and families for their unwavering support.

REFERENCES

[1] A Pandiyan, "Integrating AI-Based Security and Observability Techniques for Strengthening Protection in Multi-Cloud Systems," Proceedings of the International Conference on Intelligent and Secure Engineering Solutions (CISES) 2025 DOI:10.1109/CISES66934.2025.11265183.

[2] Patel et al., "Artificial Intelligence Approaches for Real-Time Threat Monitoring and Incident Handling in Multi-Cloud Platforms," IEEE NETCRYPT Conference, 2025. DOI: 10.1109/NETCRYPT65877.2025.11102712.

[3] Mittal et al., "Explainable AI Techniques for Real-Time API Threat Detection in Cloud Computing Environments," IEEE Conference on Cloud Security and AI Systems, 2025. DOI: 10.1109/ICCST63435.2025.11293949.

[4] M. K. Yadhukrishna et al., "Adaptive Artificial Intelligence Framework for Dynamic Threat Intelligence in Cloud Security," IEEE International Conference on Optimization and Cloud Technologies (ICOCT), 2025. DOI: 10.1109/ICOCT64433.2025.11118731.

[5] K. Bonagiri and P. Deepalakshmi, "Privacy Preservation and Data Integrity Protection in Decentralized Edge Computing Systems," IEEE International Conference on Sustainable Computing, 2024. DOI: 10.1109/SUSTAINED63638.2024.11074024

[6] K. C. Sunkara et al., *"AI-Supported Cyber Twin Technology for Real-Time Software Security in IoT-Based Environments,"* IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC), 2024. DOI: 10.1109/ICMNWC63764.2024

[7] *S. W. Ali, I. A. Shah, F. Zahid, et al., "Machine Learning-Based Cloud IDS: A Systematic Literature Review and MITRE ATT&CK Mapping,"* Cluster Computing, *vol. 29, article 920, 2026. DOI: 10.1007/s10586-026-06730-5.*

[8] *[8] A. Selvam and T. Selvy, "Explainable AI (XAI) for Insider Threat Detection: Balancing Security and Transparency in Cloud Computing,"* Concurrency and Computation: Practice and Experience, *vol. 37, 2025. DOI: 10.1002/cpe.70390.*

[9] *[9] M. Bakro, R. R. Kumar, M. Husain, Z. Ashraf, A. Ali, S. I. Yaqoob, M. N. Ahmed, and N. Parveen, "Building a Cloud-IDS by Hybrid Bio-Inspired Feature Selection Algorithms Along with Random Forest Model,"* IEEE Access, *vol. 12, pp. 8846–8874, 2024. DOI: 10.1109/ACCESS.2024.3353055.*

[10] *[10] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of Supervised Machine Learning for Cloud Security,"* 2016 International Conference on Information Science and Security (ICISS), *2016. DOI: 10.1109/ICISSEC.2016.7885853.*