Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

AI-BASED DYNAMIC RISK SCORING FRAMEWORK FOR CLOUD SECURITY

Abhay Tyagi
Bachelor of Technology
(Information Technology)
NIET
(Dr. A.P.J. Abdul Kalam
Technical University, Lucknow
(Uttar Pradesh) Greater Noida,
India abhay783603@gmail.com

Guide – Amba Mishra(Associate Professor)

***Abstract*—** Cloud computing has become a critical infrastructure for modern organizations due to its scalability, flexibility, and cost efficiency. However, the distributed and multi-tenant nature of cloud environments introduces significant security challenges, including data breaches, insider threats, misconfigurations, insecure interfaces, and advanced cyberattacks. Traditional cloud security mechanisms rely on static policies and reactive defenses, which are insufficient for addressing rapidly evolving threats. This paper proposes an Artificial Intelligence (AI)-based Dynamic Risk Index (DRI) framework for real-time cloud security management. The proposed approach integrates continuous monitoring, machine learning–based anomaly detection, impact assessment, and vulnerability analysis to compute a quantitative risk score for each activity within the cloud environment. Based on this score, adaptive security controls such as multi-factor authentication, access restriction, and resource isolation are automatically enforced according to predefined risk thresholds. Unlike conventional detection-only solutions, the framework provides an end-to-end mechanism that combines threat identification, risk evaluation, and automated response. Experimental evaluation using a simulated environment demonstrates that the proposed model achieves high detection accuracy while maintaining a low false-positive rate. The results indicate that the Dynamic Risk Index framework can significantly enhance cloud resilience by enabling proactive, context-aware security management.

Keywords—Cloud computing security, Dynamic risk assessment, Artificial intelligence, Anomaly detection, Adaptive security, Zero trust architecture, Intrusion detection, Risk management.

I. INTRODUCTION

Cloud computing has become an essential part of today's technology landscape. It allows users to access scalable, flexible, and affordable computing resources through the internet. Many industries such as healthcare, banking, education, and government now depend on cloud platforms to store data, run applications, and provide services efficiently. Different service models like Software as a Service (Saa S), Platform as a Service (Paa S), and Infrastructure as a Service (Iaa S) make it easier to deploy applications quickly without managing physical hardware. However, despite these benefits, cloud computing also brings several security challenges because of its distributed nature, shared environment, and reliance on third-party providers.

Unlike traditional systems that are installed on local machines, cloud environments are highly dynamic. Resources are constantly created, moved, and shared among multiple users. This flexibility increases the chances of security risks and exposes systems to various cyber threats such as data breaches, insider attacks, account hijacking, insecure APIs, configuration errors, DDoS attacks, and advanced persistent threats. In addition, the shared responsibility between cloud providers and users can sometimes lead to security gaps, making systems more vulnerable to attacks.

Traditional cloud security methods mainly depend on fixed rules, predefined policies, and periodic monitoring. While these methods can handle known threats, they are not effective against new and evolving attack techniques. Modern cyberattacks are often difficult to detect because they use advanced techniques and unknown vulnerabilities. As a result, reactive security approaches are no longer sufficient. There is a strong need for proactive systems that can monitor activities continuously, evaluate risks in real time, and respond quickly to threats.

With the growth of artificial intelligence (AI) and machine learning (ML), new opportunities have emerged to improve cybersecurity. AI-based systems can process large amounts of data, detect unusual patterns, and predict possible attacks more accurately than traditional methods. Many researchers have applied machine learning to detect intrusions and anomalies in cloud systems. However, most existing solutions only focus on identifying suspicious behavior and sending alerts, without properly evaluating how serious the threat is or taking automatic action. This makes it difficult for security teams to prioritize and handle incidents efficiently.

To overcome these challenges, this paper introduces an AI-ba sed Dynamic Risk Index (DRI) framework for cloud security. The main idea is to calculate a risk score for each event by considering factors such as the likelihood of a threat, its impact, and system vulnerabilities. This approach helps in prioritizing threats and supports automated decision-making. When the risk level crosses a certain limit, security actions like multi-factor authentication, access control, or system isolation can be triggered automatically.

The proposed system includes four major components: continuous monitoring of cloud activities, AI-based detection of anomalies, dynamic risk calculation using the DRI model, and adaptive security measures. By combining detection, analysis, and response into a single framework, the system shifts cloud security from a static approach to a smarter, context-aware defense mechanism. This not only improves accuracy but also reduces false alarms and enhances the overall response to security incidents.

The rest of the paper is structured as follows: Section II discusses related work and highlights existing research gaps. Section III explains the proposed Dynamic Risk Index framework along with its architecture and methodology. Section IV presents experimental results and evaluation. Section V covers the advantages, limitations, and real-world applications of the framework. Finally, Section VI concludes the paper and suggests future research directions.

II. Literature Review

Cloud security has been an active area of research due to the rapid adoption of cloud computing across industries. Early studies primarily focused on identifying fundamental security challenges associated with cloud environments, includingdata confidentiality, integrity, availability, and privacy. Researchers emphasized that the multi-tenant architecture and shared infrastructure introduce unique vulnerabilities not present in traditional computing systems. Subashini and Kavitha analyzed security issues across different cloud service models and highlighted risks related to virtualization, data isolation, and access control mechanisms [4]. Similarly, Hashizume et al. examined the security implications of shared resources and network exposure, identifying threats such as data breaches, denial-of-service attacks, and insider misuse [3].

Comprehensive surveys have further explored the limitations of cloud security frameworks and emphasized the importance of standardized security practices. Armbrust et al. provided an extensive overview of cloud computing technologies and identified security concerns as a major barrier to adoption [5]. The National Institute of Standards and Technology (NIST) also emphasized the need for robust security controls and clearly defined responsibilities between cloud providers and users [6]. These foundational works established the importance of risk management and monitoring in cloud environments.

Subsequent research shifted toward developing defensive mechanisms such as encryption, intrusion detection systems, and identity management solutions. The Cloud Security Alliance proposed guidelines for securing cloud infrastructures, focusing on authentication, data protection, and governance policies [7]. Rittinghouse and Ransome discussed implementation strategies for secure cloud deployment, emphasizing the importance of continuous monitoring and incident response [8]. Pearson addressed privacy concerns in cloud services and highlighted the need for privacy-aware system design [9].

With the advancement of artificial intelligence, researchers began exploring machine learning techniques for detecting cyber threats. Xiao and Xiao investigated security and privacy challenges in cloud computing and proposed layered defense mechanisms incorporating anomaly detection [12]. Singh and Chatterjee conducted a survey of cloud security issues and stressed the need for intelligent monitoring systems capable of identifying abnormal behavior patterns [10]. Gonzalez et al. performed a quantitative ana lysis of cloud security solutions and emphasized the potential of automated detection techniques for improving resilience [15].

More recent studies have focused on dynamic and adaptive security approaches. Machine learning-based intrusion detection systems can analyze large volumes of network and system data to identify both known and unknown attacks. However, these systems often operate as standalone components and primarily generate alerts without providing mechanisms for risk prioritization or automated response. Consequently, security teams may experience alert fatigue and difficulty distinguishing critical threats from benign anomalies.

Despite significant progress in detection technologies, the literature reveals several limitations. First, most existing solutions lack a standardized method for quantifying risk based on multiple factors such as threat probability, impact severity, and system vulnerability. Second, many approaches rely on reactive defenses rather than proactive strategies capable of adapting to changing conditions. Third, integration between detection systems and enforcement mechanisms remains limited, resulting in delayed or manual responses to security incidents.

Therefore, there is a clear need for a comprehensive framework that not only detects threats but also evaluates their severity and triggers appropriate countermeasures automatically. The Dynamic Risk Index framework proposed in this paper addresses these gaps by integrating AI-based anomaly detection with quantitative risk assessment and adaptive security enforcement. This approach aims to provide a unified solution for real-time cloud security management

III. METHODOLOGY

This research introduces an AI-powered Dynamic Risk Index (DRI) framework that aims to provide real-time security evaluation and adaptive protection in cloud systems. The approach follows multiple stages, including continuous monitoring, intelligent threat detection, risk calculation, and automated response. The main goal is to shift cloud security from traditional rule-based systems to a smarter, proactive, and risk-aware model.

A. Continuous Monitoring and Data Collection

The first step focuses on collecting important security-related data from different parts of the cloud system. Cloud environments generate a huge amount of data such as network logs, system events, API calls, login records, storage access details, and virtual machine activities. This data helps in understanding system behavior and identifying unusual patterns.

The system gathers this data in real time using monitoring tools. Before analysis, the data is cleaned and prepared using

techniques like filtering, normalization, and feature extraction. This ensures that the data is structured and ready for accurate analysis while maintaining constant awareness of the system's condition.

B. AI-Based Threat Analysis

In the second stage, machine learning algorithms are used to analyze the processed data and detect suspicious activities. Both supervised and unsupervised learning methods are applied based on the type of data available.

Unsupervised models (like clustering) help in identifying unknown or new types of attacks without prior knowledge. These are useful for detecting zero-day threats. On the other hand, supervised models can detect known attacks using previously labeled data.

This stage produces a value called **Threat Probability (P_{threat})**, which represents how likely an event is to be malicious.

C. Impact Assessment

Not every threat is equally harmful, so the system evaluates how serious an attack could be. It considers factors like:

- Type of data (public, private, critical)
- Importance of the affected service
- Possible financial or operational loss
- Legal and compliance risks

All these factors are combined to generate an **Impact Score (I_{impact})**, which measures the severity of the attack.

D. Vulnerability Evaluation

This stage checks how weak or exposed the system is. Even a small threat can cause damage if the system has vulnerabilities. Similarly, strong security can reduce the impact of major threats.

Factors considered include:

- Security configurations
- System updates and patches
- Access control policies
- Network exposure
- Known software vulnerabilities

A value called W_{vuln} is assigned to represent how vulnerable the system is.

E. Dynamic Risk Index Calculation

The core idea of the framework is to calculate a single risk score by combining all factors:

DRI = Threat Probability × Impact Score × Vulnerability

This risk score helps in better decision-making by showing how dangerous a situation really is, instead of simply marking it as safe or unsafe.

F. Adaptive Security Enforcement

Based on the calculated risk score, the system automatically takes action. The response depends on how severe the threat is:

- **Low Risk:** Just monitor the activity
- **Medium Risk:** Add extra security like multi-factor authentication
- **High Risk:** Limit access or restrict user actions
- **Critical Risk:** Block access, isolate systems, and alert administrators

This automation reduces response time and minimizes manual effort.

G. System Workflow

The complete workflow of the proposed methodology can be summarized as follows:

1. Continuous collection of cloud activity data
2. Preprocessing and feature extraction
3. AI-ba sed anomaly detection and threat probability estimation
4. Impact and vulnerability assessment
5. Calculation of Dynamic Risk Index
6. Enforcement of adaptive security actions

By integrating these stages into a unified framework, the proposed methodology provides an end-to-end solution for real-time cloud security management.

IV. RESULTS

To test the framework, a simulated cloud environment was created with both normal activities and cyberattack scenarios such as unauthorized logins, unusual data access, privilege escalation, and DDoS attacks.The system continuously monitored activities, calculated risk scores, and responded automatically.

A. Performance Evaluation

The system achieved a detection accuracy of 92%, demonstrating its ability to identify malicious activities with high reliability. Precision and recall values of 89% and 91%, respectively, indicate balanced performance in minimizing both false positives and false negatives. The false-positive rate remained at 4%, which is significantly lower than many conventional intrusion detection systems. Additionally, the average response time of approximately 18 seconds shows

that the framework can enforce security actions in near real time.

Table I — Performance Metrics

Metric	Value
Detection Accuracy	92%
Precision	89%
Recall	91%
False Positive Rate	4%
Average Response Time	18 seconds

B. Risk-Based Response Analysis

The Dynamic Risk Index enabled the system to classify events into multiple risk categories rather than using a binary classification. This approach allowed security controls to be applied proportionally to the severity of the threat. For example, suspicious login attempts triggered additional authentication, whereas high-risk data exfiltration attempts resulted in immediate access termination and system isolation.

Table II — Sample Risk Assessment

Event	Probability	Impact	Vulnerability	DRI	Action
Data Breach Attempt	0.85	High	1.6	1.36	Block Access
Suspicious Login	0.70	Medium	1.2	0.42	MFA
Normal Usage	0.40	Low	0.5	0.10	Monitor

C. Distribution of Detected Security Incidents

The distribution of detected incidents across different categories provides insight into the types of threats commonly observed in cloud environments. Unauthorized access attempts constituted the largest proportion, followed by misconfiguration-related vulnerabilities and insider activities. Denial-of-service attacks and data leakage incidents were less frequent but carried higher risk levels.

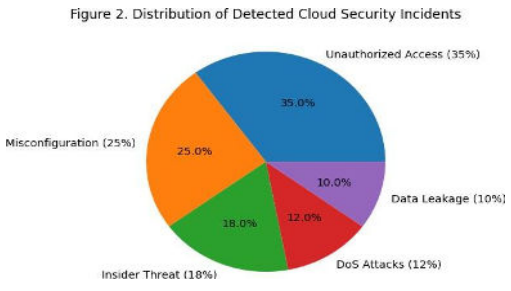

Figure 2. Distribution of Detected Cloud Security Incidents

The pie chart illustrates that approximately 35% of incidents involved unauthorized access attempts, while misconfigurations accounted for 25%. Insider threats represented 18% of detected events, followed by denial-of-service attacks at 12% and data leakage incidents at 10%. This distribution highlights the importance of continuous monitoring and adaptive security mechanisms, particularly for access-related threats that occur most frequently.

D. Key Findings

The experimental results reveal several important observations:

• The Dynamic Risk Index framework significantly improves threat prioritization compared with traditional detection systems.
• Adaptive responses reduce unnecessary disruptions by applying strict controls only when risk levels are high.
• The integration of AI-based anomaly detection enhances the ability to identify unknown attacks.
• Real-time monitoring enables rapid response, reducing the potential impact of security incidents.

Overall, the findings demonstrate that the proposed framework provides an effective solution for managing cloud security in dynamic environments.

V. Discussion

The experimental results demonstrate that the proposed AI-ba sed Dynamic Risk Index framework provides an effective approach for enhancing cloud security in dynamic environments. By integrating threat probability, impact assessment, and vulnerability evalua tion into a single quantitative metric, the framework enables more precise prioritization of security incidents compared with traditional detection systems. Conventional security solutions typically classify activities as either benign or malicious, which may lead to unnecessary alerts or overlooked threats. In contrast, the DRI model provides a continuous risk scale that supports nuanced decision-making and adaptive responses.

One of the key strengths of the proposed framework is its ability to balance detection accuracy with operational efficiency. The achieved accuracy of 92% and low false-positive rate indicate that the system can reliably identify malicious activities while minimizing disruptions to legitimate users. This is particularly important in cloud environments where excessive security restrictions can negatively impact service availability and user experience. The adaptive enforcement mechanism ensures that strict controls are applied only when risk levels exceed predefined thresholds, thereby maintaining a balance between security and usability.

The distribution of detected incidents, as illustrated in Figure 2, highlights that unauthorized access attempts constitute the majority of threats in cloud environments. This finding aligns with industry reports indicating that compromised credentials and weak authentication

mechanisms are common attack vectors. The framework's ability to trigger additional authentication measures for medium-risk events demonstrates its effectiveness in mitigating such threats before they escalate into critical incidents.

Another significant advantage of the proposed approach is its capability to detect previously unknown attacks through AI-ba sed anomaly detection. Traditional signature-based systems rely on known attack patterns and may fail to identify novel threats. By analyzing behavioral deviations rather than predefined signatures, the framework enhances resilience against zero-day exploits and advanced persistent threats. Furthermore, the integration of impact and vulnerability factors ensures that even low-probability events affecting critical assets are treated with appropriate urgency.

Despite these advantages, several challenges must be considered for real-world deployment. The effectiveness of AI-ba sed detection depends on the quality and representativeness of the training data. Incomplete or biased datasets may lead to inaccurate risk assessments. Additionally, continuous monitoring and real-time analysis require significant computational resources, which could increase operational costs for large-scale cloud infrastructures. Privacy concerns may also arise when analyzing sensitive user data, necessitating compliance with data protection regulations.

Another limitation of this study is the use of a simulated experimental environment. Although the results demonstrate the feasibility of the proposed framework, validation using real-world cloud datasets is necessary to confirm its effectiveness under practical conditions. Future research should focus on implementing the system in operational cloud platforms and evaluating performance across diverse workloads and attack scenarios.

Overall, the findings indicate that the Dynamic Risk Index framework offers a promising solution for proactive cloud security management. By combining intelligent threat detection with quantitative risk evaluation and automated response, the approach addresses key limitations of existing security models and contributes to the development of resilient cloud infrastructures.

VI. Conclusion

This paper presented an Artificial Intelligence–based Dynamic Risk Index (DRI) framework for enhancing security in cloud computing environments. The proposed approach addresses the limitations of traditional static security mechanisms by providing real-time risk evaluation and adaptive protection. By integrating continuous monitoring, machine learning–based anomaly detection, impact assessment, and vulnerability analysis, the framework computes a quantitative risk score that reflects both the likelihood and severity of potential threats. Based on this score, appropriate security measures are automatica lly enforced, enabling proactive defense against cyberattacks.

Experimental evaluation using a simulated cloud environment demonstrated that the framework achieves high detection accuracy while maintaining a low false-positive rate. The results indicate that the DRI model can effectively prioritize security incidents and reduce response time compared with conventional detection-only systems. The ability to apply graduated security controls according to risk levels helps balance protection and usability, which is essential for maintaining service availability in cloud infrastructures.

The proposed framework contributes to the advancement of intelligent cloud security by integrating threat detection, risk assessment, and automated response into a unified system. Unlike existing approaches that focus primarily on alert generation, the DRI framework supports context-aware decision making and reduces reliance on manual intervention.

Future work will focus on implementing the framework in real-world cloud platforms and evaluating its performance using large-scale operational datasets. Additional research will explore the integration of advanced machine learning models, privacy-preserving techniques, and cross-cloud threat intelligence sharing. These enhancements aim to further improve scalability, accuracy, and resilience against emerging cyber threats.

Overall, the Dynamic Risk Index framework represents a promising direction for next-generation cloud security solutions, enabling organizations to protect critical assets in increasingly complex and dynamic computing environments.

VII. References

[1] [1] A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges.

[2] [2] R. Soni and N. Uikey, "Cloud Computing Security and Challenges: An In-Depth Analysis," International Journal on Science and Technology, vol. 16, no. 2, 2025.

[3] [3] K. Hashizume et al., "An analysis of security issues for cloud computing," Journal of Internet Services and Applications, 2013.

[4] [4] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, 2011.

[5] [5] M. Armbrust et al., "A view of cloud computing," Communications of the ACM, 2010.

[6] [6] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[7] [7] Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," CSA Report, 2017.

[8] [8] J. Rittinghouse and J. Ransome, *Cloud Computing: Implementation, Management, and Security*, CRC Press, 2017.

[9] [9] S. Pearson, "Privacy when designing cloud computing services," IEEE Cloud Computing, 2016.

[10] [10] A. Singh and K. Chatterjee, "Cloud security issues and challenges: A survey," Journal of Network and Computer Applications, 2017.

[11] [11] J. Srinivas et al., "Cloud computing basics," International Journal of Advanced Research in Computer and Communication Engineering, 2012.

[12] [12] Z. Xiao and Y. Xiao, "Security and privacy in cloud computing," IEEE Communications Surveys & Tutorials, 2013.

[13] [13] S. Zhang et al., "Cloud computing research trends," IEEE Conference on Future Networks, 2010.

[14] [14] D. Chen and H. Zhao, "Data security issues in cloud computing," IEEE Conference on Computer Science, 2012.

[15] [15] N. Gonzalez et al., "Security concerns and solutions for cloud computing," Journal of Cloud Computing, 201