

A Review on Real Time Security Risk Assessment on Cloud Computing

Bhor Shravani R.¹, Prof. Bangar Abhishek P.², Prof. Karad Vandana A.³, Prof. Bhosale Sachin B.⁴

^{1,2,3,4,5}Department of Computer Engineering /Jaihind College of Engineering/SPPU, Pune, India

Abstract- Cloud computing gives organizations flexible storage, computing power, and access to services, but it also creates security risks that can change quickly. A one-time security check may miss a new attack, a dangerous configuration change, or a threat that moves from one connected system to another. This paper reviews six supplied re-search papers and develops a practical model for real-time security risk assessment in cloud computing. The reviewed work covers holistic risk scoring across cloud and edge layers, searchable encryption and secure data deletion, artificial neural networks for threat detection, secure network design, AI-based anomaly detection with Zero Trust, and a systematic mapping of cloud risk assessment methods. Based on these sources, the paper proposes a continuous cycle that identifies important assets, collects security signals, detects unusual activity, combines technical findings with business impact, assigns a risk level, and supports an appropriate response. The model uses simple and explainable risk scoring alongside optional machine-learning alerts, identity checks, network segmentation, encryption, and audit records. The paper is a literature-based design and does not claim to have run a new experiment. It also identifies practical challenges, including false alarms, limited visibility, data privacy, model drift, and the cost of continuous monitoring. The main conclusion is that real-time assessment works best when monitoring, vulnerability information, access control, and response actions are connected in one process rather than operated as separate tools.

Keywords— cloud computing; real-time risk assessment; cloud security; anomaly detection; artificial intelligence; Zero Trust; continuous monitoring; risk scoring.

I. INTRODUCTION AND RESEARCH OBJECTIVES

Cloud computing is widely used to host applications, store business records, run analytics, and support digital services. It can reduce the need for organizations to purchase and maintain all computing equipment themselves. However, cloud services also depend on networks, identity systems, virtual machines, containers, storage, provider controls, and user configuration. A weakness in one area can affect other connected services. The cloud therefore needs security assessment that reflects not only individual devices or applications, but also the relationships between them [1], [6].

Security risk assessment is the process of identifying assets, threats, weaknesses, possible consequences, and the controls needed to reduce risk. In a traditional assessment, an organization may scan its systems at a planned time and prepare a report. This remains useful, but the result can become outdated

when software changes, a new service is deployed, access rights are altered, or an attacker begins unusual activity. Real-time assessment seeks to update the risk picture continuously or at short intervals using current information from the cloud environment.

The challenge is not simply to generate more alerts. Security teams need to know which events matter, how serious they are, what other systems may be affected, and what action should be taken first. A high number of isolated alerts can overwhelm staff. At the same time, a single alert may look minor until it is connected with a vulnerable service, an unusual login, or a critical data store. Gatti et al. emphasize that risk can propagate across layers and administrative domains, and that platform-health signals should be considered together with service-level security information [1].

This paper brings together six supplied studies to present a simple, integrated approach to real-time

cloud security risk assessment. The aim is to explain the ideas in accessible language and show how they can be combined in a practical framework. The paper is a literature-based synthesis and design proposal; it does not report a newly conducted deployment or experimental results.

1. Objectives

The main objectives are: (i) to explain why cloud risks need continuous assessment; (ii) to review the main contributions of the six supplied papers; (iii) to propose a layered workflow for collecting evidence, calculating risk, and responding to threats; (iv) to describe suitable measures for evaluating the workflow; and (v) to identify limitations and directions for future work.

2. Scope

The discussion covers infrastructure, platform, software, network, identity, data, and connected edge or IoT components where they interact with cloud services. It considers machine-learning detection as one source of evidence, not as a replacement for basic security controls or human judgement. The framework is intended as a general model that can be adapted to different organizations and cloud service models.

II. REVIEW METHODOLOGY

This paper presents a structured narrative review of six research papers supplied for the topic "Real-Time Security Risk Assessment in Cloud Computing." The selected papers cover multi-layer cloud cyber-risk assessment, searchable encryption for cloud-assisted IoT, artificial neural networks for cloud security, secure cloud networking, intrusion detection and mitigation, and a systematic mapping study of cloud security risk assessment. These papers were chosen to represent complementary areas of cloud security that are relevant to identifying, evaluating, monitoring, and reducing security risks. The papers were reviewed by examining their research objectives, proposed methods, reported findings, and stated limitations. The review focused on five themes: (i) cloud risk assessment and risk modelling, (ii) real-time threat and intrusion detection, (iii) artificial intelligence and machine-

learning techniques, (iv) data protection and access control, and (v) secure cloud networking and risk mitigation. Findings were compared across these themes to identify shared ideas, differences between approaches, and issues that may affect practical deployment.

Studies were retained when they directly addressed cloud computing security or a closely related cloud-assisted environment and provided methods or findings relevant to risk assessment or mitigation. Information was taken from the six supplied papers and their bibliographic details. No additional database search, duplicate-screening process, or formal quality-scoring procedure was conducted for this review. Therefore, the paper is a focused narrative review of the selected sources rather than an exhaustive systematic review of all research in the field.

The review identified a need to connect continuous monitoring, risk scoring, threat detection, and response within one process. Based on the reviewed literature, this paper outlines a conceptual framework for real-time cloud security risk assessment. The framework is a proposed design derived from the literature; it should not be interpreted as an experimentally validated system. Further evaluation using real cloud workloads, measurable detection performance, and response-time testing would be required to establish its effectiveness.

III. LITERATURE REVIEW

1. Holistic risk assessment across cloud layers

Gatti et al. present a multi-layer and multi-domain approach for the cloud continuum [1]. The cloud continuum includes connected cloud, edge, IoT, physical, and virtual resources that may belong to different administrative domains. Their framework combines trust assessment based on platform-health indicators with service-level assessment of vulnerabilities and exposures. The paper describes automated data collection, semantic enrichment, quantitative risk metrics, and anomaly detection within and between layers. Its central lesson for real-time assessment is that an event should be

interpreted in context: a local anomaly may become more serious if the affected node supports a critical service or connects to other vulnerable components. This approach supports a broad view of risk instead of treating every virtual machine or service as a separate island. For practical use, an organization can build an asset relationship map and update it when workloads, network paths, or service dependencies change. Such a map can help estimate the possible spread and impact of an incident.

2. Encryption, searchable data, and secure deletion

Ghopur studies attribute-based searchable encryption for cloud-assisted IoT [2]. The proposed puncturable CP-ABSE scheme combines fine-grained access rules, keyword searching over encrypted information, and a method for withdrawing the ability to search for data that should no longer be available. The paper discusses security against chosen-plaintext and chosen-keyword attacks and reports implementation work to examine efficiency. Although this is not a complete real-time risk scoring system, it highlights important data risks: who may access information, whether data remains searchable after deletion is requested, and how security can be maintained when cloud storage is used by devices with limited resources.

For risk assessment, encryption and access controls should be treated as evidence about the strength of data protection, not as proof that all risk has disappeared. The system still needs to monitor permission changes, failed access attempts, key management, data retention rules, and whether the implemented controls continue to operate as expected.

3. Deep learning and artificial neural networks

Hasimi et al. examine the use of deep learning and an artificial neural network (ANN) approach for cloud security [3]. Their discussion describes the use of network traffic, system logs, and user behaviour to identify patterns that may indicate intrusions, malware, or other anomalies. It also outlines practical implementation concerns such as defining objectives, preparing datasets, tuning a model, checking compatibility, and considering

computation and maintenance costs. The paper supports using machine learning to help process large volumes of signals, but it also shows that model quality depends on data quality and careful evaluation.

An ANN can identify patterns that are difficult to express through fixed rules. However, a model output should be treated as a detection signal with a confidence level, rather than a final decision about the total business risk. Unusual behaviour may be legitimate, and a familiar pattern may still be harmful if the environment has changed. Combining model outputs with vulnerability information, identity events, and asset importance can make alerts more useful.

4. Secure cloud network design

Wang, Wang, and Wang describe an industry-specific cloud networking plan that uses software-defined networking (SDN), network separation, firewalls, load balancing, and dedicated security services [4]. Their design considers different customer requirements, including local deployment, isolation, and centralized management. The study illustrates that network architecture is an important part of security. Segmentation can limit unnecessary communication between workloads, while firewalls and monitoring points can help enforce and observe traffic rules.

For real-time assessment, the network design provides context for interpreting events. A connection from a public-facing service to a database may be expected, while the same connection from an unrelated workload may be suspicious. Assessment systems should therefore know which network paths are allowed and whether observed communication differs from the approved design.

5. AI-based anomaly detection and Zero Trust

Mathivanan and Lanitha propose a two-layer security architecture combining AI-based anomaly detection with an Extended Zero Trust model [5]. Their reported approach uses datasets including CIC-IDS2018, TONIoT, UNSW-NB15, and CICIOT2023, and incorporates controls such as role-

based access control, multi-factor authentication, and micro-segmentation. The paper reports detection accuracy of 98.6% and adversarial resilience of 93.4% for its evaluated setup. These figures belong to that study and should not be assumed to apply to every cloud environment. Its broader lesson is that detection and mitigation should work together: analytics can identify suspicious behaviour, while Zero Trust controls continuously verify requests and limit unnecessary access.

Zero Trust does not mean that every request is malicious. It means that access should not be granted solely because a user or workload is already inside a network boundary. Each request should be checked against identity, device or workload context, permissions, and policy. In a risk workflow, failed or unusual verification can raise the risk score and trigger additional review or restriction.

6. Systematic mapping of cloud risk assessment

Anunziata et al. conduct a systematic mapping study of cloud security risk assessment and analyze 21 primary studies published between 2010 and 2023 [6]. They examine research topics, cloud delivery models, standards, and evaluation approaches. The study notes that security testing and risk assessment should support one another: risk findings can guide vulnerability scanning, penetration testing, code review, and architecture review. It also identifies the need for stronger and more consistent evaluation practices. This finding is relevant because a proposed real-time model should

not only produce scores; it should also be evaluated using a repeatable method and evidence that other teams can understand.

7. Summary

Together, the papers suggest that no single technique covers every part of cloud risk. Continuous platform monitoring provides operational signals; vulnerability and configuration checks identify weaknesses; encryption and access control protect data; network segmentation limits movement; AI can help detect unusual patterns; and risk assessment connects these findings to impact and response. The key gap addressed in this paper is the need to describe these parts as one understandable, continuously updated process. The proposed model is a synthesis of the supplied studies, not a claim that any one source already implements every element exactly as presented here.

IV. COMPARATIVELY ANALYSIS

Table 1 compares six representative research papers related to real-time security risk assessment in cloud computing. The studies address different aspects of cloud security, including risk assessment, data protection, artificial intelligence, secure networking, and intrusion detection. Their methods and reported findings are not directly comparable because they address different problems and use different evaluation approaches.

Table 1. Comparison of representative cloud security studies

Author,year	Objective	Method/Technology	Major reported findings	Limitations
Wang et al., 2023 [4]	Develop a secure cloud networking plan for an industry-specific cloud platform.	Security-oriented cloud network design and planning.	Emphasises organising network security according to the needs of a specific industry platform.	A network plan alone does not provide continuous risk scoring across all cloud components.

Ghopur, 2024 [2]	Protect data searched in cloud-assisted IoT environments.	Attribute-based searchable encryption with forward security.	Addresses secure search and protection of encrypted data as system updates occur.	Focuses mainly on encryption and searchable access, rather than complete real-time cloud risk assessment.
Annunziata et al., 2024 [6]	Map research on security risk assessment in cloud computing.	Systematic mapping study of published research.	Organises the research landscape and highlights areas and approaches studied in cloud risk assessment.	A mapping study synthesises existing work but does not itself implement a real-time assessment system.
Hasimi et al., 2024 [3]	Explore deep learning for cloud-computing security.	Artificial neural network (ANN) approach.	Examines how neural-network techniques can support identifying security-related patterns.	Detection quality depends on the data, training process, and evaluation conditions.
Gatti et al., 2025 [1]	Assess cyber risk across the cloud continuum.	Multi-layer, multi-domain cyber-risk assessment approach.	Presents a holistic approach for considering risks across different layers and domains.	The framework's practical effectiveness depends on validation in real deployment settings.
Mathivanan & Lanitha, 2026 [5]	Improve intrusion detection and mitigation in cloud environments.	Integrated intrusion-detection and mitigation methodology.	Combines detection and response; the paper reports performance results for its proposed approach.	Reported performance must be interpreted in the context of its datasets, experiments, and evaluation setup.

V. PROPOSED CONCEPTUAL FRAMEWORK AND ARCHITECTURE

1. Framework

The proposed framework uses a continuous cycle with six main stages: asset and dependency discovery, evidence collection, event normalization, risk calculation, response selection, and feedback. The stages can be implemented using existing cloud logs, security scanners, identity services, monitoring agents, and ticketing or response tools. The exact products may differ, but the workflow remains similar.

Stage 1: identify assets and relationships

The organization first lists the assets it needs to protect. These may include customer records, databases, virtual machines, containers, APIs,

identity services, encryption keys, storage buckets, network gateways, and edge devices. Each asset should have an owner, purpose, sensitivity level, and business importance. The inventory should also record relationships: which applications depend on a database, which workloads can reach the internet, and which identities can administer each service. Without this context, a monitoring system may detect an event but fail to estimate its real impact.

Stage 2: collect current security evidence

Evidence can come from cloud audit logs, authentication events, network flow records, operating-system and container logs, vulnerability scans, configuration checks, endpoint protection, resource-use metrics, and data-access records. Examples include a sudden increase in failed logins, a new administrator role, a service exposed to the public internet, a known vulnerable package,

unexpected outbound traffic, or unusual CPU use. Collection should be proportionate to the sensitivity of the environment and should avoid collecting unnecessary personal information.

Stage 3: normalize and connect events

Different tools often describe the same event in different formats. The framework converts events into a common record containing at least a timestamp, asset identifier, event type, severity or confidence, source, and related identity or service. Events are then connected to the asset map. For example, an unusual login can be linked to the account's permissions, the resource accessed, and the sensitivity of the stored data. Time synchronization and reliable asset identifiers are important; otherwise, separate events may be incorrectly combined or a real sequence may be missed.

Stage 4: calculate risk

A simple starting point is to rate likelihood and impact on a scale from 1 to 5. Likelihood reflects how plausible or strongly indicated the event is, based on the evidence. Impact reflects possible harm to confidentiality, integrity, availability, legal obligations, or business operations. A basic score is calculated as:

$$\text{Risk Score} = \text{Likelihood} \times \text{Impact}.$$

The result ranges from 1 to 25. Organizations may define 1–4 as low, 5–9 as moderate, 10–16 as high, and 17–25 as critical, but these bands are proposed examples and should be adapted to the organization's risk appetite.

The score should also consider the strength of evidence and the possibility of risk spreading through connected systems. A vulnerability on a low-value isolated test system may receive a lower priority than the same vulnerability on an internet-facing service connected to a sensitive database. To prevent false precision, the system should store the reason for each score, the evidence used, and any assumptions. A numerical score is a decision aid, not an exact measurement of future loss.

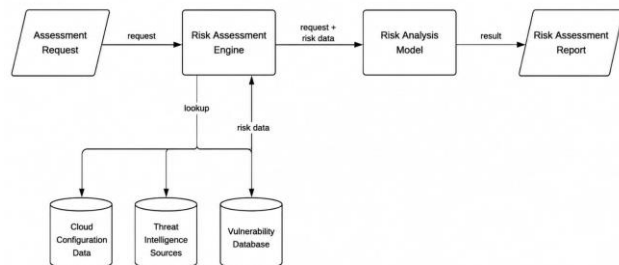
Stage 5: choose a proportionate response

Response actions should match the level of risk and the confidence in the evidence. Low-risk events may be recorded and watched. Moderate risks may create a ticket, request owner confirmation, or initiate a focused scan. High risks may require blocking suspicious traffic, revoking a temporary token, isolating a workload, or escalating to an analyst. Critical actions should follow approved emergency procedures and include safeguards against disrupting essential services. Automated action is most suitable when the signal is reliable, the action is reversible, and the potential harm from acting incorrectly is controlled.

Stage 6: learn and update

After an event is reviewed, the system should record whether it was malicious, benign, or unresolved. Analysts can use this feedback to improve rules, tune alert thresholds, and retrain machine-learning models where appropriate. Changes to cloud architecture, business priorities, and attacker behaviour should also update the asset map and risk rules. A continuous process is only useful if it remains maintained and if lessons from incidents are applied.

2. Architecture



VI. RESEARCH CHALLENGES AND GAPS

Real-time security risk assessment in cloud computing is an important research area because cloud environments face different types of security threats, including unauthorised access, data breaches, network attacks, and malicious activities.

1. Integration of Different Security Layers

Cloud computing consists of multiple layers, including infrastructure, networks, applications, storage, and access management. Security threats at

one layer may affect other parts of the cloud environment.

Research gap: A coordinated method is needed to collect and analyse security information from different cloud layers and present it as one overall risk assessment.

2. Real-Time Threat Detection

Cloud environments change continuously because users access services, applications process data, and resources are created or removed dynamically. Security risks may therefore change over time.

Research gap: Further research is needed to connect continuous monitoring, threat detection, risk evaluation, and security alerts in a unified process.

3. Accuracy of Artificial Intelligence-Based Security Methods

Artificial intelligence and machine-learning methods can help identify unusual patterns in cloud activity. However, their effectiveness depends on the quality of training data, the types of attacks represented, and the conditions under which the models are tested.

Research gap: AI-based security models need broader evaluation using different workloads and threat scenarios. Evaluation should consider detection accuracy, false-positive rates, missed threats, and processing time.

4. Data Privacy and Confidentiality

Cloud providers store and process large amounts of information, including sensitive business and personal data. Security monitoring must identify suspicious activities without unnecessarily exposing confidential information.

Research gap: Future systems should combine privacy-preserving data protection with effective risk assessment, ensuring that only authorised users and services can access sensitive security information.

5. Secure Cloud Network Management

Network configuration plays an important role in cloud security. Incorrect access rules, insecure

connections, and poorly configured network resources can create opportunities for attacks.

Research gap: Research is needed to connect network security information with application monitoring, access-control events, vulnerability information, and overall risk scoring.

VI. PROPOSED RESEARCH DIRECTIONS

Based on the research challenges and gaps identified above, several directions can be explored to improve real-time security risk assessment in cloud computing. These directions combine ideas from the six reviewed papers into a proposed approach. They should be considered research proposals rather than experimentally validated results.

1. Development of an Integrated Cloud Security Framework

Future research can develop a framework that combines security information from different cloud components, including networks, applications, storage systems, user identities, and infrastructure. The framework could collect information from monitoring tools, access logs, intrusion-detection systems, and configuration-management systems.

2. Dynamic and Continuous Risk Scoring

Traditional risk assessments may be performed periodically. However, cloud security conditions can change quickly, making it important to update risk levels when new information becomes available.

The risk score could be updated when new alerts, configuration changes, or suspicious activities are detected.

3. Artificial Intelligence for Threat Identification

Artificial neural networks and other machine-learning techniques could be used to analyse cloud activity and identify suspicious behaviour.

The model could examine patterns in login attempts, network traffic, system logs, and access requests.

4. Automated but Controlled Security Responses

Future cloud security systems could connect risk levels with predefined response policies. The response should depend on the severity of the threat

and the importance of the affected service. High-impact actions should include appropriate safeguards, audit logs, and authorised review.

5. Privacy-Preserving Security Assessment

Data confidentiality should remain a priority when monitoring cloud environments. Security assessment should not create unnecessary exposure of sensitive information.

Future research could investigate how encryption, attribute-based access control, and data minimisation can be combined with risk assessment.

6. Real-Time Cloud Network Risk Assessment

Secure cloud networking should be treated as an ongoing process rather than a one-time configuration task. Network changes, newly created services, and modifications to access rules may introduce new risks.

A future system could continuously review network configurations, identify unexpected communication patterns, and connect network-related alerts with the overall cloud risk score.

7. Standardized Testing and Performance Evaluation

A proposed framework should be tested before its effectiveness can be established. Testing could be conducted in a controlled cloud environment using normal workloads, simulated attacks, configuration errors, and changing resource demands.

VII. CONCLUSION AND FUTURE SCOPE

1. Conclusion

Cloud computing has become an important technology because it provides flexible computing resources, storage, and application services. However, its distributed nature creates several security challenges, including unauthorised access, data confidentiality risks, insecure network configurations, malicious activities, and delayed threat detection. These challenges make continuous security monitoring and risk assessment important for maintaining the reliability and protection of cloud services.

A key finding of this review is that these security functions should be considered together rather than as completely separate activities. Continuous monitoring, threat detection, dynamic risk evaluation, privacy protection, and appropriate mitigation can contribute to a more coordinated cloud security process.

Improving real-time cloud security requires not only detecting threats but also understanding their severity, updating risk levels as conditions change, protecting sensitive information, and responding appropriately. Combining these capabilities provides a useful direction for future cloud security research.

2. Future Scope

The future scope of this research includes the development and evaluation of an integrated real-time cloud security risk-assessment system.

First, a working prototype could be developed to collect security information from cloud networks, applications, identity services, and storage systems. Second, future work could investigate dynamic risk-scoring algorithms that update risk levels as new threats and system changes are detected. Such methods could help security teams prioritise incidents according to their severity and potential impact. Third, artificial intelligence could be investigated for identifying unusual patterns in cloud activity. Further research should examine the reliability of these methods under different workloads and attack conditions. Explainable AI could also help administrators understand why a particular event has been classified as risky. Fourth, future systems could connect risk assessment with controlled mitigation. Depending on the severity of an incident, the system could recommend alerts, additional authentication, access restrictions, or temporary workload isolation. Safeguards would be necessary to prevent incorrect automated decisions from disrupting legitimate services. Finally, the proposed approach should be tested using controlled cloud environments and, where possible, real-world operational data. Future evaluation should measure detection accuracy, false-positive rates, detection and response times, scalability, resource consumption, and cost. Comparisons with

existing security methods would help determine the practical benefits and limitations of the proposed approach.

These future research activities could support the development of cloud security systems that are more adaptive, explainable, privacy-aware, and responsive to changing security threats.

REFERENCES

1. G. Gatti et al., "Holistic Cyber Risk Assessment in the Cloud Continuum: A Multi-Layer, Multi-Domain Approach," IEEE Access, 2025. DOI: 10.1109/ACCESS.2025.3622915.
2. D. Ghopur, "Attribute-Based Searchable Encryption With Forward Security for Cloud-Assisted IoT," IEEE Access, 2024. DOI: 10.1109/ACCESS.2024.3418886.
3. L. Hasimi et al., "Cloud Computing Security and Deep Learning: An ANN approach," Procedia Computer Science, vol. 231, pp. 40–47, 2024. DOI: 10.1016/j.procs.2023.12.155.
4. Q. Wang et al., "Research on Secure Cloud Networking Plan Based on Industry-Specific Cloud Platform," IEEE Access, 2023. DOI: 10.1109/ACCESS.2023.3279409.
5. N. Mathivanan and B. Lanitha, "An integrated methodology for intrusion detection and mitigation to optimize cloud security," Journal of Cloud Computing, vol. 15, article 18, 2026. DOI: 10.1186/s13677-026-00858-w.
6. G. Annunziata et al., "Security Risk Assessment on Cloud: A Systematic Mapping Study," in Proceedings of the Evaluation and Assessment in Software Engineering (EASE), 2024. DOI: 10.1145/3661167.3661287.