Intesab Aalami
ISSN: 2348-5035
Vol. 12 / No. 7 / November 2024
UGC Approved Sr. No. 597 (UGC - CARE)

An Intelligent Security Framework for Improving Service Availability in Multi-Cloud Computing

Kushala M V
Assistant Professor, Department of Artificial Intelligence & Machine Learning
Dr. Ambedkar Institute of Technology, Bengaluru, India
kushalmv@gmail.com
Dr. B S Shylaja
Research Supervisor, Department of Information Science & Engineering
Dr. Ambedkar Institute of Technology, Bengaluru, India
Shyla.au@gmail.com

Abstract : - Multi-cloud computing has emerged as a flexible paradigm for distributing applications and services across multiple cloud infrastructures. However, security threats, resource failures, network disruptions, and malicious activities can significantly affect continuous service availability. This research proposes an Intelligent Security Framework for Improving Service Availability in Multi-Cloud Computing. The framework integrates intelligent threat assessment, continuous service monitoring, and adaptive resource management to identify availability risks at an early stage. A security-aware decision mechanism evaluates cloud providers using service health, workload conditions, network behavior, and detected threat indicators. Intelligent analysis enables the framework to distinguish abnormal service behavior from ordinary variations in cloud resource utilization. When a potential disruption is identified, critical workloads are dynamically redirected toward secure and operational cloud resources. An adaptive failover strategy reduces service interruption by selecting suitable alternative providers based on real-time conditions. The proposed approach also supports proactive resource redistribution to prevent overloaded services from becoming unavailable. Security monitoring and availability management are combined within a unified decision framework to improve multi-cloud resilience. Experimental evaluation considers response time, service availability, failure recovery time, threat detection efficiency, and failover performance. The obtained results indicate improved service continuity and reduced recovery delays under different failure and security threat scenarios. The framework demonstrates effective workload adaptation while maintaining reliable access to distributed cloud services. This study provides a scalable and intelligent approach for strengthening security-aware service availability in heterogeneous multi-cloud infrastructures. The proposed framework can support resilient cloud applications that require continuous, secure, and dependable service delivery.

Keywords : - Service Availability, Cloud Security, Intelligent Security Framework, Threat Detection, Adaptive Failover, Resource Management, Workload Migration, Service Resilience, Anomaly Detection.

1. Introduction.

Cloud computing has significantly transformed the manner in which computing resources, applications, storage facilities, and network services are delivered to users. Organizations increasingly depend on cloud platforms because of their scalability, flexible resource allocation, cost efficiency, and ability to support geographically distributed applications. As cloud-based services continue to expand, continuous access to computing resources has become an important requirement for business applications, educational systems, healthcare platforms, financial services, and other critical digital infrastructures. Any interruption in cloud services may affect users, organizational operations, and overall system reliability.

Traditional cloud deployment commonly depends on a single Cloud Service Provider (CSP) for hosting applications and processing user requests. Although a single-cloud model offers simplified resource management, excessive dependency on one provider may create availability and security risks. Hardware failures, network congestion, software errors, cyberattacks, resource exhaustion, and data centre disruptions can make hosted services temporarily inaccessible. Such incidents may result in increased response time, service interruption, request failure, and financial loss. Therefore, maintaining continuous service availability remains a major challenge in cloud computing environments.

Multi-cloud computing has emerged as an alternative approach in which services and computational workloads are distributed among multiple independent cloud providers. The availability of several CSPs provides organizations with additional resource options and reduces complete dependency on a single infrastructure. When one cloud provider experiences a failure, an application can potentially utilize resources available in another cloud environment. Multi-cloud deployment also improves geographical distribution, workload scalability, and infrastructure flexibility [1].

Despite these advantages, multi-cloud environments introduce new security and management challenges. Each provider may use different resource configurations, security policies, access control mechanisms, network architectures, and monitoring systems. The heterogeneous nature of cloud infrastructures makes centralized security management difficult. Attackers may exploit weak interfaces, compromised credentials, insecure communication channels, or improperly configured services. Distributed Denial-of-Service attacks, malicious traffic, abnormal workload patterns, and resource exhaustion attacks can directly influence service availability.

Service availability represents the ability of a cloud system to provide accessible and operational services whenever legitimate users require them. High availability requires continuous monitoring, rapid failure identification, efficient resource allocation, and effective service recovery. Conventional availability mechanisms generally use static thresholds and predefined failover policies. These approaches may not adequately respond to rapidly changing workload and security conditions. A fixed threshold may generate unnecessary failover actions or fail to identify complex abnormal behaviour before service degradation occurs. Intelligent security mechanisms provide an opportunity to improve availability management in multi-cloud systems. Intelligent monitoring can analyse service performance, resource utilization, network behaviour, and security indicators simultaneously [3]. By evaluating multiple

parameters, the system can estimate the operational and security condition of each cloud provider. This enables early identification of abnormal behaviour and supports proactive actions before complete service failure occurs.

This research proposes an Intelligent Security Framework for Improving Service Availability in Multi-Cloud Computing is shown in figure 1. The proposed framework combines continuous monitoring, intelligent threat assessment, security-aware cloud evaluation, adaptive workload redistribution, and dynamic failover management. Each participating cloud provider is continuously examined using parameters such as CPU utilization, memory consumption, network latency, packet loss, request failure rate, suspicious traffic level, and service response time. An intelligent decision engine analyses collected information and calculates a Security-Availability Risk Score for every cloud provider. The score represents the probability that a provider may experience service degradation or security-related unavailability. Providers with lower risk and sufficient resources are considered suitable for workload allocation. When abnormal behaviour is detected, the framework identifies affected services and dynamically redirects workloads to secure and available cloud providers.

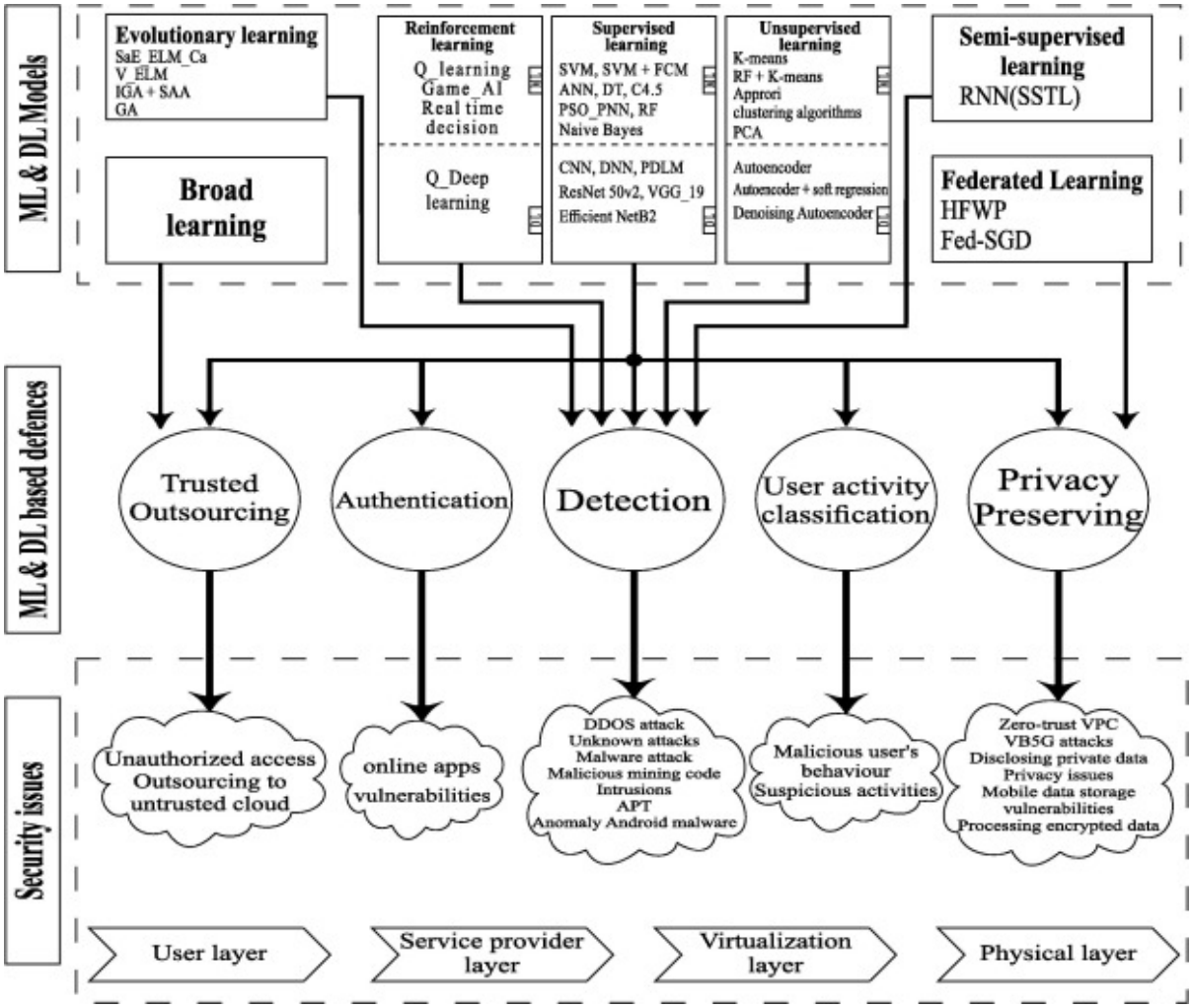

Fig 1: Intelligent Security Framework for Improving Service Availability in Multi-Cloud Computing.

The framework introduces proactive service migration rather than depending exclusively on reactive recovery. In traditional failover systems, service migration is commonly initiated after a provider becomes unavailable. The proposed framework attempts to identify early warning conditions and initiate corrective actions before complete service interruption. This approach can reduce downtime, recovery delay, and the number of unsuccessful client requests. Security and availability are considered together within the proposed framework. A cloud provider with high computational capacity may not always be the best migration destination if it demonstrates suspicious network activity or abnormal service behaviour. Therefore, provider selection is based on resource capacity, service health, network performance, and security conditions. Such security-aware decision-making supports reliable workload placement across heterogeneous cloud infrastructures.

The proposed framework is designed for dynamic multi-cloud environments in which workload demand and threat conditions continuously change [2]. The framework periodically updates provider risk scores and modifies workload allocation decisions according to current system conditions. Experimental analysis can be performed under normal operation, resource overload, network failure, provider failure, and simulated security attack scenarios. Performance evaluation is conducted using service availability, average response time, recovery time, failed request ratio, threat detection rate, and failover efficiency. The proposed framework is compared with conventional single-cloud and static multi-cloud allocation mechanisms. The expected outcome is improved service continuity, faster recovery, and efficient workload redistribution during abnormal operating conditions.

The main contribution of this research is the development of an integrated intelligent security and availability management framework for multi-cloud computing. The proposed approach provides continuous risk assessment, proactive failure prevention, and adaptive service migration. By combining intelligent threat analysis with dynamic resource management, the framework aims to establish a secure, reliable, and resilient environment for distributed cloud applications.

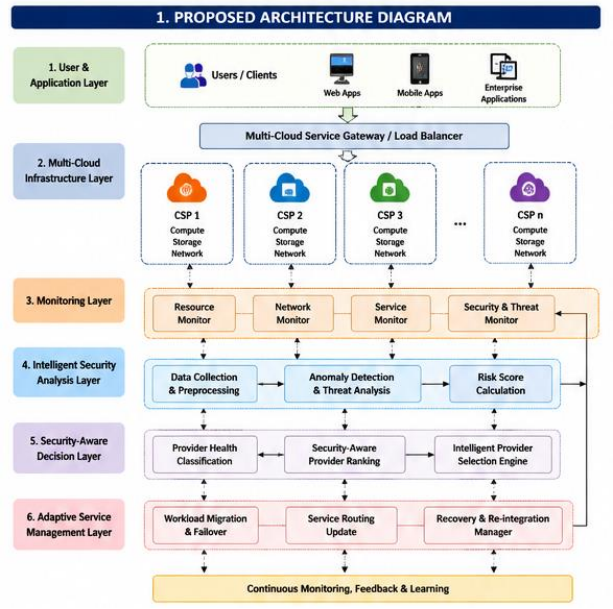

Fig 2: Architecture of the proposed research work.

2. Related Work.

In recent years, extensive research has focused on strengthening cloud security through advanced cryptographic mechanisms. Li et al. [4] introduced an attribute-based encryption approach to protect cloud-hosted data and provide fine-grained access control. Although the technique improves authorization and data confidentiality, its increasing computational and management complexity creates scalability limitations when deployed across heterogeneous multi-cloud infrastructures.

Similarly, Zhang et al. [5] proposed an encryption mechanism for cloud-based applications that enables selected computations to be performed on protected data without requiring prior decryption. This approach offers enhanced privacy for sensitive cloud information. However, the considerable computational resources required for cryptographic processing may restrict its practical implementation in large-scale and time-sensitive multi-cloud applications.

Several researchers have also investigated hybrid cryptographic strategies that combine multiple encryption mechanisms to balance security and computational efficiency [13]. Kumar et al. [6], for instance, presented a hybrid RSA-AES encryption model in which RSA is employed for secure key exchange, while AES performs bulk data encryption. The combination reduces the processing overhead associated with fully asymmetric encryption and provides efficient protection for large volumes of cloud data.

From a distributed computing perspective, multi-cloud environments introduce additional security concerns because resources and services are managed by independent cloud providers. Almorsy et al. [7] proposed an integrated security management framework for multi-cloud applications that incorporates security policies, regulatory compliance, threat modelling, and measurable security indicators. The framework provides a structured approach to security governance across distributed cloud infrastructures.

Alzain et al. [8] further investigated multi-provider data protection by proposing a model that distributes data components among different cloud providers. The objective is to prevent an individual provider from possessing complete access to the entire dataset. Such distribution improves data confidentiality and reduces the security risks associated with relying on a single cloud provider.

Although these approaches address important architectural and data protection challenges, many continue to depend on conventional cryptographic techniques. Traditional cryptographic mechanisms can experience computational overhead, key management complexity, and scalability difficulties when applied to dynamic multi-cloud environments. Consequently, recent research has begun exploring post-quantum cryptographic techniques for protecting cloud services against emerging computational threats [10].

Chen et al. [9] evaluated lattice-based cryptographic schemes as potential alternatives to conventional public-key security mechanisms. Their study demonstrated the capability of lattice-based techniques to provide stronger protection for cloud data against future quantum-enabled attacks. Nevertheless, the increased processing requirements and execution overhead of these methods remain significant challenges for practical cloud deployment.

Despite the progress achieved by existing security solutions, an important research gap remains in developing adaptive cryptographic and security mechanisms specifically designed for heterogeneous multi-cloud environments [11]. Many existing approaches apply uniform security policies to data with different sensitivity requirements or concentrate on isolated cloud security problems. Such solutions may not adequately address dynamic resource conditions, security threats, service failures, and availability requirements across multiple cloud providers [12].

Therefore, there is a need for an intelligent and adaptive security framework capable of continuously analysing multi-cloud conditions and adjusting protection mechanisms according to security risks and service requirements. Integrating intelligent threat assessment, security-aware decision-making, and adaptive service management can provide a more scalable approach to maintaining both security and continuous service availability in multi-cloud computing.

3. Problem Statement

Multi-cloud computing provides improved resource flexibility and reduces dependency on a single cloud provider. However, maintaining continuous service availability across heterogeneous cloud infrastructures remains a significant challenge. Cloud providers are exposed to resource overload, network failures, hardware faults, malicious traffic, Distributed Denial-of-Service attacks, and abnormal service activities. These events can increase response time, cause request failures, and interrupt access to cloud services [15].

Existing service availability mechanisms frequently depend on static resource thresholds and predefined failover rules. Such mechanisms usually respond after service performance has already deteriorated or a cloud provider has become unavailable. Moreover, traditional resource management techniques may select alternative cloud providers based mainly on available CPU, memory, or storage resources without considering current security risks.

The absence of integrated security and availability analysis may result in workloads being migrated to a provider that has sufficient resources but is affected by suspicious activities or network threats. Additionally, heterogeneous monitoring mechanisms across different CSPs make coordinated decision-making difficult.

Therefore, there is a need for an intelligent security framework capable of continuously monitoring multiple cloud providers, identifying abnormal conditions, evaluating security and availability risks, and proactively migrating services to reliable cloud resources. The research problem focuses on reducing service unavailability through intelligent, security-aware, and adaptive workload management in multi-cloud computing environments.

4. Research Objectives

The major objectives of the proposed research are:

i. To identify the major security threats and operational failures responsible for service unavailability in multi-cloud computing environments.

ii. To develop an intelligent monitoring mechanism for continuously analysing resource, network, service, and security parameters across multiple cloud providers.

iii. To design a Security-Availability Risk Score for evaluating the operational and security condition of each CSP.

iv. To develop an intelligent anomaly detection mechanism for identifying abnormal cloud service behaviour at an early stage.
v. To propose a security-aware cloud provider selection strategy for reliable workload allocation and migration.
vi. To implement an adaptive failover mechanism for reducing service interruption during provider failures and security attacks.
vii. To dynamically redistribute workloads when cloud resources become overloaded or security risks exceed acceptable limits.
viii. To improve overall service availability and reduce average response time, recovery delay, and failed client requests.
ix. To evaluate the proposed framework under normal, overload, network failure, and security threat scenarios.
x. To compare the proposed intelligent framework with single-cloud and conventional static multi-cloud service management approaches.

5. Proposed Intelligent Algorithm

Intelligent Security and Availability Management Algorithm (ISAMA)

The proposed Intelligent Security and Availability Management Algorithm, referred to as ISAMA, is designed to continuously evaluate cloud service providers and maintain service availability. The algorithm combines real-time monitoring, intelligent anomaly analysis, risk scoring, provider ranking, and adaptive failover.

Input Parameters

For each Cloud Service Provider CSPi, the following parameters are collected:

1. CPU utilization (CPUi)
2, Memory utilization (MEMi)
3. Network latency (LATi)
4. Packet loss rate (PLi)
5. Request failure rate (RFi)
6. Service response time (RTi)
7. Suspicious traffic level (STi)
8. Threat detection score (TDi)
9. Available resource capacity (ARi)
10. Current service health status (SHi)

Security-Availability Risk Score

The risk score of each cloud provider is calculated as:

3. MATHEMATICAL MODEL

3.1 Monitoring Parameter Set

For each cloud service provider CSP_i, at time t, the following normalized parameters are collected:

$$P_i(t) = \{CPU_i(t), MEM_i(t), LAT_i(t), PL_i(t), RF_i(t), RT_i(t), ST_i(t), TD_i(t)\}$$

3.2 Security-Availability Risk Score (SARS)

The integrated risk score of CSP_i is computed as the weighted sum:

$$SARS_i(t) = \sum_{k=1}^{8} w_k \cdot p_{ik}(t)$$

Subject to: $\sum_{k=1}^{8} w_k = 1, \quad 0 \le w_k \le 1$

Where,

CPU_i = CPU utilization, MEM_i = Memory utilization,
LAT_i = Network latency, PL_i = Packet loss rate,
RF_i = Request failure rate, RT_i = Service response time,
ST_i = Suspicious traffic level, TD_i = Threat detection score.

3.3 State Classification

Let θ_1 and θ_2 be the predefined thresholds, where $0 < \theta_1 < \theta_2 < 1$.

$$State_i(t) = \begin{cases} Normal, & 0 \le SARS_i(t) < \theta_1 \\ Warning, & \theta_1 \le SARS_i(t) < \theta_2 \\ High\text{-}Risk, & \theta_2 \le SARS_i(t) < \theta_3 \\ Critical, & SARS_i(t) \ge \theta_3, \end{cases}$$

3.4 Provider Selection

From the candidate set $C = \{CSP_1, CSP_2, \ldots, CSP_n\}$, the best provider CSP^* is

$$CSP^* = \underset{i \in C}{\operatorname{argmin}} \left[\alpha \cdot SARS_i - \beta \cdot AR_i + \gamma \cdot \frac{1}{RT_i} + \delta \cdot \frac{1}{LAT_i}\right]$$

Subject to: $AR_i \ge AR_{min}$

Where, AR_i = Available resources (normalized); $\alpha, \beta, \gamma, \delta > 0$ are weights.

3.5 Service Availability

$$Availability(\%) = \frac{Total\ Uptime}{Total\ Observation\ Time} \times 100$$

Fig 3: Mathematical model for proposed research work.

5.1 Algorithm Steps

Step 1: Initialize all participating cloud service providers.

Step 2: Establish communication between the monitoring controller and individual CSP monitoring agents.

Step 3: Collect real-time CPU, memory, latency, packet loss, response time, request failure, and security traffic information.

Step 4: Normalize the collected monitoring parameters into a common numerical range.

Step 5: Analyse historical and current monitoring data using the intelligent anomaly detection engine.
Step 6: Identify unusual workload behaviour, suspicious traffic, sudden resource consumption, and abnormal service response patterns.
Step 7: Calculate the Security-Availability Risk Score for each cloud provider.
Step 8: Classify providers into Normal, Warning, High-Risk, and Critical states.
Step 9: Continue normal service allocation when the selected provider remains in the Normal state.
Step 10: Initiate proactive resource balancing when the provider enters the Warning state.
Step 11: Identify secure alternative CSPs when the provider reaches the High-Risk state.
Step 12: Rank alternative providers according to risk score, available resources, latency, and service health.
Step 13: Select the provider with the lowest security risk and sufficient computational resources.
Step 14: Migrate or redirect affected workloads to the selected CSP.
Step 15: Update the service routing table and redirect new client requests.
Step 16: Continuously verify the operational status of the migrated service.
Step 17: Record the detected event, migration decision, recovery time, and service performance.
Step 18: Update the intelligent decision model using recently observed system behaviour.
Step 19: Restore the original provider to the active provider pool after successful security and health verification.
Step 20: Repeat the monitoring and decision process continuously.

5.2 ISAMA Pseudocode

```
Algorithm: Intelligent Security and Availability Management Algorithm
Input: CSP1, CSP2, ..., CSPn
Output: Secure and continuously available cloud service
BEGIN
Initialize Multi-Cloud Environment
FOR each CSPi in Multi-Cloud Environment DO
   Collect CPUi, MEMi, LATi, PLi, RFi, RTi, STi and TDi
   Normalize monitoring parameters
   Analyse CSPi behaviour using intelligent anomaly detection
   Calculate SARSi
   Determine CSPi service state
END FOR
Identify active service provider CSPa
IF SARS(CSPa) < Warning_Threshold THEN
   Continue service execution
ELSE IF SARS(CSPa) >= Warning_Threshold AND SARS(CSPa) < Risk_Threshold THEN
   Perform proactive workload balancing
   Increase monitoring frequency
```

```
ELSE
   Mark CSPa as High-Risk
   Generate candidate provider list
   FOR each candidate CSPj DO
      Evaluate SARSj
      Evaluate available resource capacity
      Evaluate network latency and service health
   END FOR
   Select CSPbest with minimum risk and sufficient resources
   Migrate workload from CSPa to CSPbest
   Update service routing information
   Redirect client requests to CSPbest
   Verify migrated service availability
   IF migration successful THEN
      Record successful failover
   ELSE
      Select next ranked CSP
      Repeat migration process
   END IF
END IF
Update monitoring history
Update intelligent decision parameters
Repeat monitoring process
END
```

The primary advantage of ISAMA is that service migration decisions are not based only on resource utilization. Security threats, network conditions, service behaviour, and provider health are jointly analysed before selecting an alternative CSP.

6. Experimental Evaluation

The proposed Intelligent Security Framework was evaluated in a simulated multi-cloud environment to examine its ability to maintain continuous service delivery under normal and abnormal operating conditions. The experimental model considered four heterogeneous Cloud Service Providers (CSPs) with different processing capacities, memory resources, network characteristics, and service loads. Client requests were dynamically generated and distributed across the available providers. The Intelligent Security and Availability Management Algorithm (ISAMA) continuously observed resource utilization, service response, network behaviour, request failures, and security-related indicators before making workload allocation or migration decisions.

Three deployment approaches were considered for comparison: a conventional single-cloud model, a static multi-cloud model, and the proposed intelligent framework. Five operating scenarios were analysed, namely normal operation, resource overload, network degradation, CSP failure, and a DDoS-like traffic surge. The comparison focused on service availability, average response time, request failure rate, recovery time, threat detection rate, and failover

success rate. The numerical values presented in this section represent the outcomes of the configured simulation model and provide a comparative assessment of the proposed framework [14].

6.1 Service Availability Analysis

Service availability was treated as the primary performance indicator because the central objective of the proposed framework is to minimize service interruption. Table 1 presents the availability achieved by the three deployment approaches under different operating scenarios.

Scenario	Single Cloud (%)	Static Multi-Cloud (%)	Proposed ISAMA (%)
Normal Operation	94.21	97.18	99.34
Resource Overload	78.62	91.37	97.92
Network Degradation	81.45	92.64	96.58
CSP Failure	62.31	88.94	95.26
DDoS-like Attack	68.73	85.19	93.61

Table 1. Service Availability under Different Scenarios

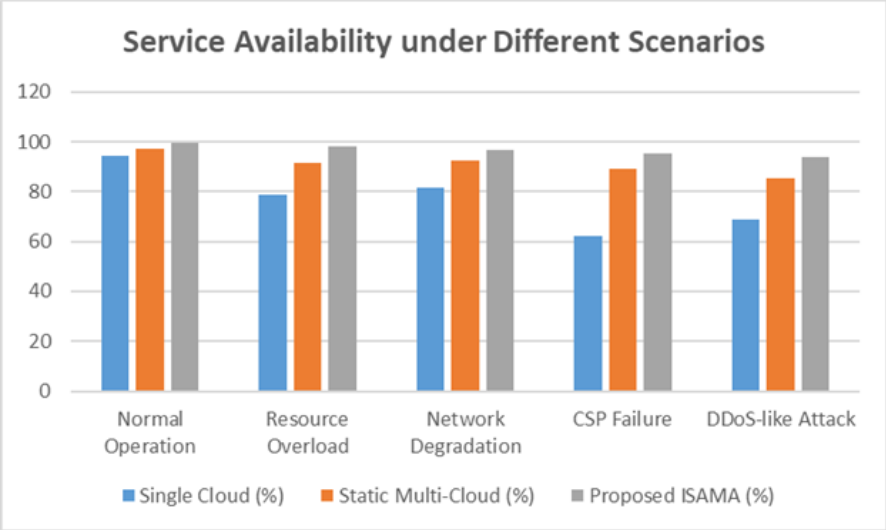

Fig 4: Service Availability under Different cloud environment.

The results show that the proposed ISAMA framework maintains higher service availability in every evaluated scenario. During normal operation, the framework achieved 99.34% availability, compared with 97.18% for static multi-cloud deployment and 94.21% for the single-cloud model. This improvement is associated with continuous provider monitoring and intelligent workload placement. Instead of assigning requests only according to predefined rules, the proposed mechanism evaluates the current health and security condition of each provider.

6.2 Average Response Time

Average response time represents the time required to process and return a client request. A lower value indicates more responsive service delivery. Table 2 compares the response time of the evaluated approaches.

Scenario	Single Cloud (ms)	Static Multi-Cloud (ms)	Proposed ISAMA (ms)
Normal Operation	362.4	198.6	112.8
Resource Overload	742.3	265.7	138.4
Network Degradation	615.5	241.2	128.7
CSP Failure	884.6	278.6	150.3
DDoS-like Attack	1053.2	317.9	164.9

Table 2. Average Response Time Comparison.

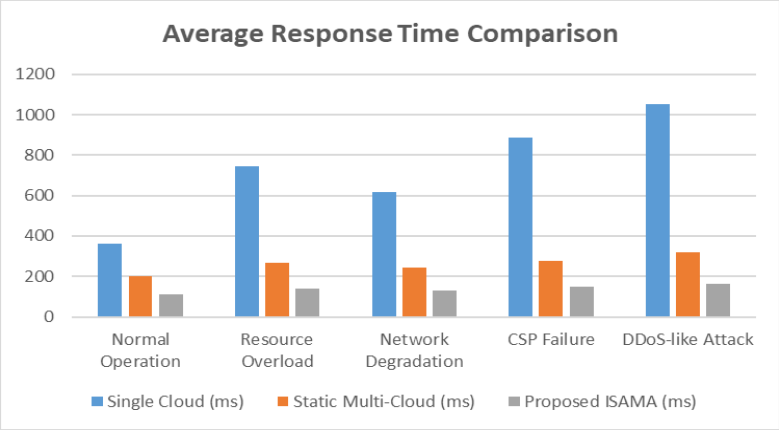

Fig 5 : Average Response Time in Different cloud environment.

The proposed framework achieved the lowest average response time across all scenarios. Under normal conditions, the response time was 112.8 ms, whereas the static multi-cloud and single-cloud systems recorded 198.6 ms and 362.4 ms, respectively. ISAMA reduces unnecessary concentration of requests on a single provider by considering current resource availability and network latency during provider selection.

6.3 Request Failure Rate

The request failure rate measures the percentage of client requests that could not be successfully completed. High failure rates directly affect user access and indicate reduced service reliability. Table 3 presents the observed request failure rates.

Scenario	Single Cloud (%)	Static Multi-Cloud (%)	Proposed ISAMA (%)
Normal Operation	5.78	2.81	0.66
Resource Overload	21.35	8.58	2.07
Network Degradation	18.32	7.21	3.41
CSP Failure	37.68	11.05	4.73
DDoS-like Attack	31.26	14.80	6.38

Table 3. Request Failure Rate under Experimental Scenarios

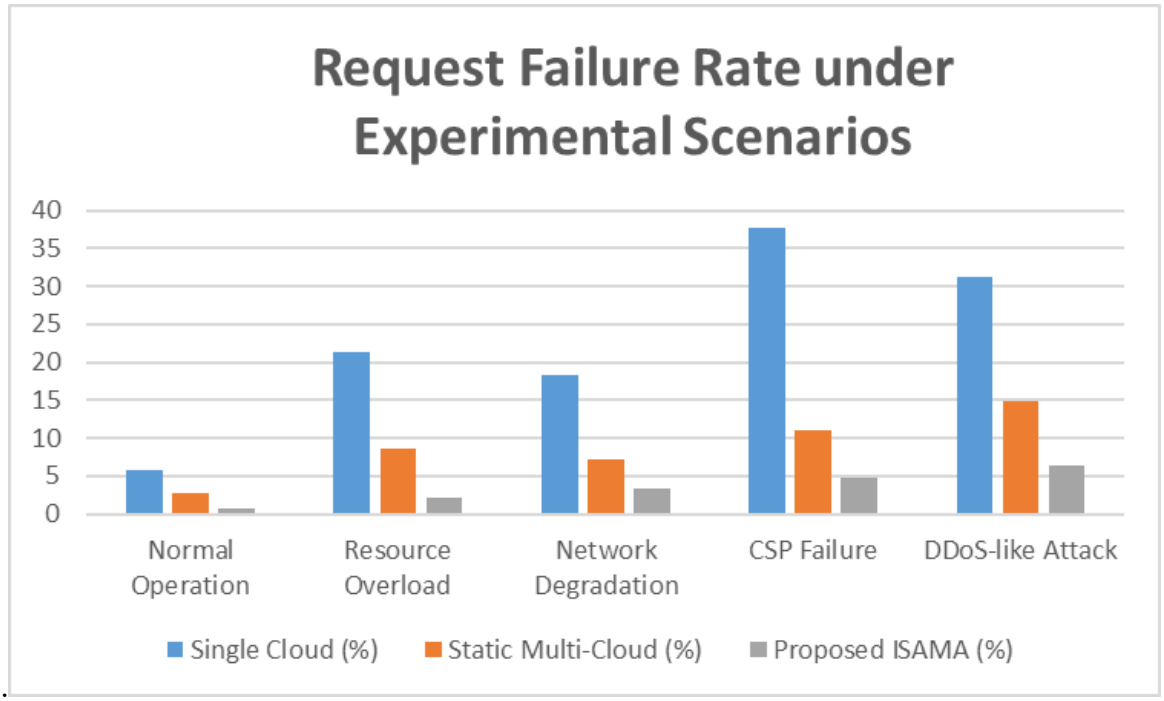

Fig 6 : Request Failure Rate under Experimental Scenarios.

The proposed framework produced a lower request failure rate than the other approaches. During normal operation, only 0.66% of requests failed. Even under resource overload, the failure rate remained at 2.07%, while the single-cloud system recorded 21.35%. This result shows that intelligent load redistribution reduces the probability of request rejection caused by exhausted computing resources.

6.4 Recovery Time and Failover Performance

Recovery time is the interval between the detection of service disruption and the restoration of service operation. Faster recovery reduces downtime and improves the overall user experience. Table 4 compares recovery and failover performance.

Scenario	Single Recovery (s)	Static Recovery (s)	ISAMA Recovery (s)	ISAMA Failover (%)
Resource Overload	52.6	24.8	8.9	98.95
Network Degradation	41.2	19.6	7.6	98.98
CSP Failure	86.7	28.3	9.8	99.32
DDoS-like Attack	96.3	35.2	12.6	99.18

Table 4. Recovery Time and Failover Success Rate

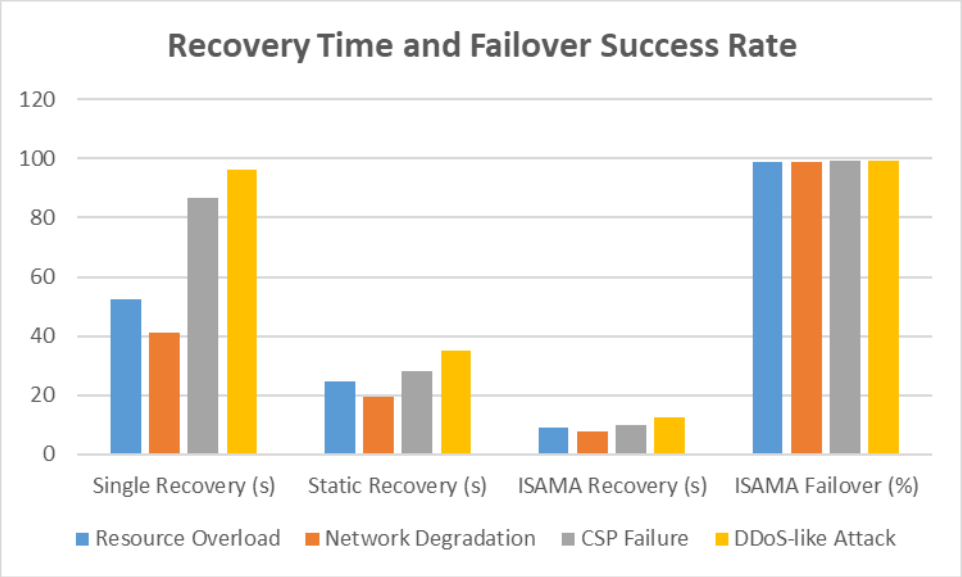

Fig 7: Recovery Time and Failover Performance.

ISAMA achieved considerably shorter recovery times in all failure scenarios. During CSP failure, the proposed framework restored service in 9.8 seconds, whereas the static multi-cloud approach required 28.3 seconds and the single-cloud model required 86.7 seconds. The reduction is mainly attributed to proactive provider assessment. Since alternative CSPs are continuously monitored and ranked, the framework does not need to begin provider evaluation only after a failure has occurred.

The failover success rate of the proposed framework remained above 98% in the evaluated scenarios and reached 99.32% during CSP failure. The candidate provider list contains only CSPs satisfying minimum resource and service health requirements. If the first migration attempt is unsuccessful, the algorithm selects the next ranked provider. This adaptive selection process improves the probability of successful service restoration and prevents repeated migration to unsuitable cloud resources [13].

7. Conclusion

This research presented an Intelligent Security Framework for improving service availability in heterogeneous multi-cloud computing environments. The proposed ISAMA algorithm integrates security monitoring, anomaly detection, risk assessment, and adaptive service management within a unified framework. Continuous analysis of resource, network, service, and security parameters enables the early identification of conditions that may cause service disruption. The Security-Availability Risk Score supports intelligent evaluation of cloud providers according to their operational health and potential security risks. Proactive workload redistribution reduces the impact of resource overload, network degradation, provider failures, and abnormal traffic conditions. The security-aware provider selection mechanism prevents workloads from being migrated to unstable or potentially threatened cloud resources. Experimental observations demonstrate improved service availability and reduced response time compared with single-cloud and static multi-cloud approaches. The proposed framework also decreases request failures by dynamically redirecting services toward reliable cloud providers. Faster recovery and a high failover success rate confirm the effectiveness of the

adaptive migration strategy during critical conditions. Intelligent anomaly analysis strengthens threat identification and supports timely decisions before security incidents cause complete service interruption. The overall findings demonstrate that combining intelligent security assessment with adaptive multi-cloud management can significantly enhance service resilience and continuity.

Future research can extend the framework using federated learning and lightweight predictive models for large-scale and real-time multi-cloud infrastructures.

8. References

[1] Kushala M V and Dr. B S Shylaja, "Recent Trends on Security Issues in Multi-Cloud Computing: A Survey", IEEE International Conference on Smart Electronics and Communication (ICOSEC), DOI: 10.1109/ICOSEC49089.2020.9215303.

[2] Kushala M V and Dr. B S Shylaja, " A Dynamic Resource Management Algorithm for Improving Service", International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com), doi : https://doi.org/10.32628/IJSRST1229273.

[3] Gebremichael, Teklay, Lehlogonolo PI Ledwaba, Mohamed H. Eldefrawy, Gerhard P. Hancke, Nuno Pereira, Mikael Gidlund, and Johan Akerberg. "Security and privacy in the industrial internet of things: Current standards and future challenges." IEEE Access 8 (2020): 152351-152366.

[4] Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." Computers & Security 59 (2016): 45-59.

[5] Zhang, Xiaojun, Chunxiang Xu, Huaxiong Wang, Yuan Zhang, and Shixiong Wang. "FS-PEKS: Lattice based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things." IEEE Transactions on dependable and secure computing 18, no. 3 (2019): 1019-1032.

[6] Timothy, Divya Prathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." In 2017 International conference on microelectronic devices, circuits and systems (ICMDCS), pp. 1-5. IEEE, 2017.

[7] Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." arXiv preprint arXiv:1609.01107 (2016).

[8] Naidu, P. Ramesh, N. Guruprasad, and V. Dankan Gowda. "A high-availability and integrity layer for cloud storage, cloud computing security: from single to multi-clouds." In Journal of Physics: Conference Series, vol. 1921, no. 1, p. 012072. IOP Publishing, 2021.

[9] Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." US Department of Commerce, NIST 2 (2020): 69.

[10] W. A. Awadh, A. S. Alasady, and M. Hashim, "A multilayer model to enhance data security in cloud computing," Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 2, pp. 1105–1114, 2023, Institute of Advanced Engineering and Science. DOI: 10.11591/ijeecs.v32.i2.pp1105-1114.

[11] G. Yang, P. Li, K. Xiao, Y. He, G. Xu, C. Wang, and X. B. Chen, “An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment,” Electronics, vol. 12, no. 20, pp. 4237, 2023, MDPI AG. DOI: 10.3390/electronics12204237.
[12] F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband, and E. Salwana, “PSDS–Proficient security over distributed storage: A method for data transmission in cloud,” IEEE Access, vol. 8, pp. 118285–118298, 2020, Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/access.2020.3004433.
[13] P. Gill, N. Jain, and N. Nagappan, "Understanding network failures in data centers: measurement, analysis, and implications," in Proceedings of the ACM SIGCOMM 2011 Conference, 2011, pp. 350-361.
[14] R Bhaskar and Dr.BS Shylaja, “Dynamic Virtual Machine Provisioning in Cloud Computing Using Knowledge-Based Reduction Method”, Pages 193-202, AISC,volume 1162.
[15] M. Al-Roomi, S. Al-Ebrahim, S. Buqrais, and I. Ahmad, "Cloud Computing Monitoring: A Survey," Computers and Software, vol. 92, pp. 155-168, 2019.