Magna Scientia Advanced Research and Reviews

eISSN: 2582-9394

Cross Ref DOI: 10.30574/msarr

Journal homepage: https://magnascientiapub.com/journals/msarr/

(REVIEW ARTICLE)

Check for updates

Failure Prevention and Recovery Techniques in Cloud-Based Systems: A Systematic Review

Oluwafemi Oluwagboyega Fabiyi [1,*] and Mary Magdalene Yeboah [2]

[1] *Seattle, USA.*
[2] *Texas, USA.*

Magna Scientia Advanced Research and Reviews, 2026, 17(01), 394-405

Publication history: Received on 15 May 2026; revised on 25 June 2026; accepted on 27 June 2026

Article DOI: https://doi.org/10.30574/msarr.2026.17.1.0114

Abstract

Cloud computing systems help to maintain massive distributed applications as well as data-intensive services in various fields. Nonetheless, the distributed and complex nature of the cloud infrastructures render them susceptible to a number of system failures, such as hardware failures, software failures, network failures, virtualization failures, and ineffective resource allocation. Such failures may have a great impact on the availability of services, the reliability of the system, and the general performance. This paper aims to provide a systematic review on the topic of preventing failures and recovery methods in cloud systems in a systematic way to offer an organized view of the existing methods of promoting network reliability. Based on the systematic search strategy in the ScienceDirect database, the sources related to interventions that were published in the last ten years (2015 to 2025) were searched and filtered according to the pre-established inclusion and exclusion criteria, which have led to the identification of a final dataset of 68 studies. The review evaluates proactive failure prevention methods including predictive monitoring, machine learning-based anomaly detection, redundancy plan, load balancing plan and intelligent resource scheduling. Moreover, recovery strategies such as checkpointing, replication, failover systems, container migration and disaster recovery systems are discussed. The authors find that proactive monitoring strategies in combination with effective recovery strategies are highly effective in enhancing the resilience and operational continuity of distributed cloud infrastructures. The paper also finds significant research issues associated with scalability, security risk, real-time monitoring, and multi-cloud reliability. Such results indicate that there is a necessity of coherent resilience frameworks which integrate intelligent monitoring, intelligent fault-tolerance schemes, and automatic recovery systems. The paper offers an organized insight into the approaches of preventing failures and recovery mechanisms of cloud computing infrastructure and the fact that smart and adaptable resilience models are necessary.

Keywords: Cloud computing; Failure prevention; Fault tolerance; Failure recovery; Predictive monitoring

1. Introduction

Cloud computing is now a paradigm of current technology that allows organizations to access and deploy scalable computing resources, storage system and distributed processes platforms using the internet. The blistering growth of cloud infrastructures in the last ten years has very tangibly changed the way contemporary applications are implemented and managed in all sectors, including healthcare, transportation, smart energy systems, and digital governance (Abdi et al., 2024; Ahmed et al., 2025; Abdullayeva, 2023). Combining cloud computing with the new technologies such as Internet of Things (IoT), artificial intelligence, and edge computing has further enhanced the functionalities of distributed computing systems allowing one to conduct real-time analytics, massive data processing, and smart automation (Pentyala, 2024; Ahmed et al., 2025; Ibitoye, 2018). Besides, recent research has become keen on the increasing relevance of cloud-enabled architectures to the support of large-scale digital ecosystems and intricate

* Corresponding author: Oluwafemi Oluwagboyega Fabiyi.

cyber-physical systems (Panful et al., 2025; Shandilya et al., 2024). Notwithstanding these benefits, there are also major challenges of cloud platform reliability, scalability, and operational resilience with the growing dependency on cloud platforms.

With the continuous evolution of the cloud infrastructures, the complexity of the infrastructures grows because of the interplay of various distributed components such as the virtual machines, containers, microservices, storage systems, and network infrastructures. These types of architectures can introduce additional risks of system failures, which can occur due to the failure of hardware, bugs in software, resources allocation error, or network outages. In cloud-based applications, failures may cause a major effect on the performance of the system, the data integrity and its availability (Garraghan et al., 2018; Achary, 2021). Furthermore, current cloud systems become increasingly based on multi-cloud implementations and containerized architectures that demand complex orchestration and monitoring systems to ensure the stability and reliability (Gupta, 2024; Torres Ponce, 2025). It has also been found that the growing involvement of IoT systems and distributed edge infrastructures enhances the reliability problem since the numbers of heterogeneous computing environments and dynamic workloads continue to rise (Lampropoulos et al., 2024; Ibitoye, 2018; Pentyala, 2024). This has made the provision of dependable and fault-tolerant cloud systems one of the key studies in the field of distributed systems engineering.

In order to deal with these issues, scholars have recommended so many strategies that would enhance the reliability and durability of cloud computing environments. Overall, these strategies may be divided into failure prevention strategies and failure recovery models. The prevention of failures strategies inculcates the proactive identification of possible system anomalies and the prevention of risks that may result in failures. Such methods usually entail prediction-based monitoring, intelligent resource management, anomaly detection, and automated system control systems, aimed at enhancing the stability of a system (Pentyala, 2024; Ahmed et al., 2025). The further companies have introduced intelligent monitoring systems that can identify an abnormal behavior of the system and avoid failures in distributed computing infrastructures (Ofili et al., 2024; Ahmed et al., 2025). Also, there are new architectures like edge computing, distributed intelligence systems which are helping in enhancing responsiveness of the system and the operational risks when using large-scale clouds (Gupta, 2024; Andreyev, 2025).

Even though prevention methods can be effective, failure of big-scale distributed systems cannot be avoided. Hence, there must be efficient failure recovery systems that will restore the functionality of the system and the delivery of the service. The common way to recover involved checkpointing, replication, failover, container migration, and disaster recovery framework strategies that aim to minimize the service disruption and provide data access in the event of a system failure (Rana & Giri, 2026; Thumala, 2020). Some articles have already highlighted the significance of using both proactive and reactive strategies to improve distributed computing environments resilience (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018). Nevertheless, the current studies tend to concentrate on technologies or areas of application, including IoT security, blockchain, or distributed architecture instead of offering an overview of failure prevention and recovery methods in the cloud-based systems (Abdi et al., 2024; Sahar Saeed et al., 2025). Therefore, the study of the literature that is structured and systematic to organize the available knowledge, classify the existing techniques, and define the new research questions in the field has not been carried out yet. Thus, the paper is a systematic literature review to analyze the available literature on preventing failure and recovering methods in cloud-based systems, typify the extant methods, and establish gaps and research thrusts in the future that can enhance the reliability and resilience of the modern cloud systems infrastructure.

2. Systematic Review Methodology

A systematic literature review (SLR) is a clear and organized procedure of finding, choosing, and evaluating pertinent literature investigations in a particular area. As a contrast to classic literature reviews, SLRs use well-defined search strategies, screening processes, and data-generating patterns to reduce bias and guarantee the replicability of their findings. Such a methodological approach allows researchers to systematize the current knowledge base and determine the trends and gaps in the research, as well as new prospects in the field of research (Welsh & Benkhelifa, 2020; Abdi et al., 2024). Systematic reviews have been extensively applied in the study of technological advances, reliability issues, and the introduction of new architectural models in the distributed computing environment in the context of cloud computing research (Ahmed et al., 2025; Mukwevho & Celik, 2018).

In this work, the systematic review approach will be used to examine the current literature on the topic of failure prevention and recovery approaches in cloud-based systems. A review process is based on the structured workflow which has four primary steps: literature search, study selection, data extraction, and analysis. The methodological process was developed in a manner that would provide transparency, reproducibility and at the same time provide a comprehensive coverage of the relevant studies published during the specified search period. The review process is in

line with the well-established practices of systematic review that are generally used in computing and information systems research (Welsh & Benkhelifa, 2020; Garraghan et al., 2018).

2.1. Search Strategy

The database that was used in the literature search is the ScienceDirect database that offers access to a sizable number of peer-reviewed journals. The choice of science direct was since the journal covers much of the high-quality research articles concerning cloud computing, distributed systems and fault tolerance mechanisms. In order to retrieve pertinent literature, it was decided to create a structured search query based on the association of keywords and Boolean operators associated with cloud computing failures, prevention mechanisms, and recovery techniques. The terms were tailored to find research dealing with failure management, fault toleration schemes and reliability in cloud-based systems.

The search was conducted on March 10, 2026 in the ScienceDirect database using the following search string:

("cloud computing" OR "cloud-based systems") AND ("failure") AND ("prevention" OR "mitigation") AND ("fault tolerance") AND ("systematic review")

To address the recent developments and emergent research trends in cloud reliability and fault tolerance mechanisms, the search was restricted to publications published in the period of 2015-2025. Initial results of the search included 306 publications. With the use of a publication year filter (2015-2025), the number of studies decreased to 244. This was followed by the filtering of the articles using article type (review articles and research articles) with 219 studies. Lastly, the restriction of the results to open access and open archive sources resulted in an ultimate narrowing of 68 articles to undergo subsequent screening and analysis.

Table 1 Database Search Strategy

Database	Search String	Initial Results	Filtered Results
ScienceDirect	("cloud computing" OR "cloud-based systems") AND ("failure") AND ("prevention" OR "mitigation") AND ("fault tolerance") AND ("systematic review")	306	68

2.2. Inclusion and Exclusion Criteria

In order to make sure the selected studies were relevant and of a higher quality, inclusion and exclusion criteria were predetermined. The retrieved studies were filtered using these criteria and only publications that directly speak about the failure prevention and recovery mechanisms in cloud computing environments were included. The inclusion criteria were aimed at the selection of peer-reviewed studies that examine fault tolerance, reliability strategies, failure management techniques, or resilience mechanisms in the cloud-based infrastructures. Only papers that were published within the year 2015-2025 were considered to capture the current developments in research. The papers that were not directly connected to cloud computing reliability or fault tolerance mechanisms were not included in the studies. Besides this, during the screening, duplicate records, non-peer-reviewed articles, and publications that did not have full-text content were filtered out.

Table 2 Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Studies related to cloud failure prevention	Studies unrelated to cloud computing systems
Papers discussing fault tolerance or recovery mechanisms	Non-peer reviewed publications
Research articles or review papers	Duplicate studies
Published between 2015–2025	Papers without full text availability

2.3. Study Selection Process

The selection of the study used a multi-stage filtration process that was used to narrow down the first set of retrieved studies in a systematic manner. Several steps were used to carry out the screening process so that only the most relevant and high-quality studies should have been incorporated in the final analysis. The initial phase was to apply the search query in the scientific database named ScienceDirect that gave 306 initial results. The second step used a filter based on the year of publication that restricted the search to studies published in 2015 to 2025 and shortened the search results to 244 studies. The third stage involved the use of the article type filters to limit the studies to review articles and research articles, and this narrowed the selection of articles to 219. Lastly, the open access filter was used to make sure that the selected papers were completely accessible, thus, 68 articles were further screened with the help of abstracts and content.

The last selection phase was to go through the abstracts and the full texts of the studies that were retrieved to see whether they were of relevance to the research topic. Only the sources that directly reported on the techniques of failure prevention, recovery or fault tolerance techniques in cloud-based systems were included in the final dataset which was to be analyzed.

Table 3 Paper Screening Process

Stage	Number of Papers
Initial search	306
Year filter	244
Article type filter	219
Open access filter	68
Final selected studies	68

2.4. Data Extraction and Analysis

After the process of selecting the publication, the information that was extracted within each respective publication was relevant and helped in a systematic analysis and comparison. The data extraction procedure was aimed at gathering the most significant peculiarities of each study such as their purpose, methods employed to avoid failures and recover, methods of assessment, and technological environment where the methods were implemented. The data obtained were subsequently examined to determine the recurring research topics, classify the methods that existed and examined the usefulness of various methods employed to promote reliability in cloud computing systems. This systematic review allows identifying prevalent research patterns and what research needs to be done in cloud system resilience.

The next section presents a structured overview of cloud system failures to provide foundational context for the analysis. This overview synthesizes key failure types identified in the reviewed studies without presenting the main findings. Section 4 to 6 present the results and discussion of the failure prevention and recovery techniques with a detailed analysis of the results of the systematic review. Such arrangement guarantees the clear differentiation between the background synthesis and the very outcomes of the review.

Table 4 Data Extraction Framework

Research Category	Number of Studies	Key Techniques Identified	Example Studies	Evaluation Approaches	Key Contribution to Cloud Reliability
Cloud security and privacy mechanisms	16	Blockchain security, encryption frameworks, authentication mechanisms	Abdullayeva (2023); Czuryk (2023); George et al. (2024)	Literature reviews, surveys, comparative analysis	Enhancing cloud security to prevent system vulnerabilities and cyber-attacks
Blockchain-based reliability frameworks	10	Distributed ledger technologies, consensus algorithms, decentralized verification	Abdi et al. (2024); Sahar Saeed et al. (2025); Welsh & Benkhelifa (2020)	Systematic reviews and analytical evaluations	Improving trust, data integrity, and reliability in distributed cloud systems
Edge and distributed computing resilience	12	Edge intelligence, computation offloading, distributed resource allocation	Pentyala (2024); Andreyev (2025); Gupta (2024)	Analytical studies and surveys	Reducing latency and improving fault tolerance in distributed cloud infrastructures
Artificial intelligence and machine learning techniques	9	Federated learning, predictive analytics, AI-driven monitoring	Pentyala (2024); Jha (2025); Ofili et al. (2024)	Systematic reviews and conceptual frameworks	Intelligent fault detection and predictive failure prevention
IoT and cyber-physical system reliability	11	IoT-cloud integration, digital twins, monitoring frameworks	Ibitoye (2018); Lampropoulos et al. (2024);	Systematic mapping and literature synthesis	Enhancing monitoring and predictive maintenance in distributed systems
Cloud monitoring and DevOps management	5	Monitoring tools, microservice observability frameworks	Jha (2025); Torres Ponce (2025); Gupta (2024)	Grey literature reviews and empirical analysis	Early detection of system anomalies in cloud environments

3. Overview of Cloud System Failures

This section provides a descriptive overview of cloud system failures based on the synthesized literature and serves as a foundation for the subsequent analysis. It focuses on identifying and categorizing the major types of failures reported in cloud computing environments without yet evaluating specific techniques. The findings and critical analysis of failure prevention and recovery techniques are presented in Sections 4, 5, and 6, where the results of the systematic review are discussed in detail.

Cloud computing services are systems of distributed data centers, virtualization platforms, and networked resources, which together provide the computing services and digital applications of large scale. These infrastructures assist the organizations with processing huge amounts of data and implementing scalable applications in geographically dispersed settings (Abdi et al., 2024; Ahmed et al., 2025). Nevertheless, the dispersed characteristic of the cloud systems provides numerous possible areas of failure such as hardware errors, software bugs, network outages, and ineffective allocation systems (Garraghan et al., 2018; Achary, 2021). With more technologies, like IoT systems, edge computing structures, and artificial intelligence-based services becoming part of a cloud environment, interactions with a system become highly complex, which makes it more likely that system processes suffer disruption (Ibitoye, 2018; Pentyala, 2024; Lampropoulos et al., 2024). As a result, it is necessary to learn about the causes and consequences of failures in cloud infrastructures that can be used to design efficient prevention and recovery strategies (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018).

One of the most frequent causes of discontinuities in cloud data centers is hardware failures since these infrastructures are based on thousands of servers, storage systems, and networking solutions that are all working at the same time. Software failures can be the result of hardware degradation, overheating, power supply failures, or component failures, and such issues inevitably cause a downturn in the services and slow down performance (Achary, 2021; Nikolovski et al., 2025). Besides hardware problems, software failures are common because of bugs in the programmes, configuration mistakes, and incompatible software updates that apply to the virtualization systems and distributed applications (Torres Ponce, 2025; Szorc, 2023). Since cloud systems are based on microservice architectures and automated deployment pipelines, bugs in the software may spread through several services and result in a series of system failures (Gupta, 2024; Thumala, 2020). That is why a significant number of works highlight the significance of predictive monitoring systems and automated system management software to identify anomalies and prevent the impact of software-related disturbances in a distributed environment (Ahmed et al., 2025; Ofili et al., 2024).

There are also network failures and disruptions related to virtualization that have a great impact on the stability of the cloud-based systems. The operation of cloud infrastructures is based on the stable communication between distributed servers, storage systems, and client applications, which is why the network reliability is one of the key elements of system performance (Herrera & Maennel, 2019; Czuryk, 2023). The bandwidth congestion, the routing errors, the packet loss, or even the cyber-attacks against the communication infrastructures can cause the network failures (George et al., 2024; Panful et al., 2025). In the same vein, the virtual machine (vm) failures can be caused by hypervisor malfunctions, improperly set up virtualization systems, or a lack of computing resources assigned to the virtual workloads (Gupta, 2024; Andreyev, 2025). Such problems have the potential to disrupt cloud services and reduce the performance of distributed applications by a significant margin, especially those running on multi-cloud and containerized environments (Kenna, 2024; Rana & Giri, 2026).

Cloud system failures eventually cause major performance indicators like availability, reliability, and operational efficiency of the system. Service availability is the potential of cloud platforms to make applications and services available in times of need, and reliability is the potential of the system to work in different workloads and environmental settings (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018). In order to overcome these limitations, researchers started to pay more attention to fault tolerance, resilience, and distributed failure management mechanisms of the cloud infrastructures (Abdi et al., 2024; Shandilya et al., 2024). Redundancy, replication, checkpointing, and automated failover systems are fault tolerance methods that enable cloud platforms to perform operations even in case some of the components fail (Thumala, 2020; Rana & Giri, 2026). On the same note, resilience-based models focus on quick recovery of disturbances and of intelligent systems with references to smart monitoring structures and predictive analytics (Sahar Saeed et al., 2025; Ahmed et al., 2025). These systems are needed to ensure stable and reliable cloud services in more sophisticated distributed computing infrastructure (Adjei et al., 2026; Obidiagha & Antwi, 2026).

4. Failure Prevention Techniques in Cloud Systems

The importance of failure prevention techniques in the stability and reliability of cloud computing infrastructures is in the fact that distributed systems are full of interconnected components, which can break down under heavy workloads or due to the complexity of the operations. It will then be necessary to have proactive prevention systems to identify possible errors at an early stage and avoid service failure in distributed clouds (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018). These preventive measures usually entail constant system observation, smart load balancing and predictive analytics to guarantee consistent service provision within the spread-out infrastructures (Ahmed et al., 2025; Pentyala, 2024). It is also found that a combination of monitoring frameworks and adaptive resource management should enhance the resilience and reliability of contemporary cloud systems greatly (Abdi et al., 2024; Shandilya et al., 2024).

Predictive monitoring is one of the most popular prevention methods that continuously examines system performance metrics, including CPU load, memory usage and network response time, to identify any suspicious systems before they fail. Predictive monitoring systems are based on the historical systems logs, telemetry, and performance indicators to detect early warning signs that can signal possible system failures (Ofili et al., 2024; Ahmed et al., 2025). These monitoring tools are usually combined with the DevOps environment to facilitate automated monitoring of systems and detection of anomalies in the distributed microservice classes (Torres Ponce, 2025; Szorc, 2023). Predictive monitoring can enhance the visibility of a system and the early detection of faults, but can be demanding in large scale cloud infrastructure, which entails the use of large datasets and continuous computing resources (Pentyala, 2024; Gupta, 2024).

The other strategy worth considering in terms of prevention is the use of machine learning-based anomaly detection, which performs the analysis of system logs, network traffic, and performance metrics to identify an abnormal pattern

of behavior. Such machine learning approaches as federated learning and AI-based monitoring systems have proven to be useful in detecting sophisticated failure modes in distributed cloud systems (Ahmed et al., 2025; Ofili et al., 2024). Such intelligent detection systems can detect some nuances that conventional rule-based monitoring systems might overlook (Pentyala, 2024; Jha, 2025). Nonetheless, the application of machine learning-enabled monitoring solutions can involve huge volumes of training data and computation resources, which can raise the complexity of implementation in large-scale infrastructures in clouds (Gupta, 2024; Andreyev, 2025).

Besides the monitoring-based methods, there are well-known redundancy mechanisms, load balancing methods, and smart resource scheduling methods that are applied to avoid system breakdown due to resource overload or a malfunctioning component. Redundancy methods duplicate important system parts to ensure that backup resources will be available to substitute failed components immediately to enhance system availability and data integrity (Thumala, 2020; Rana & Giri, 2026). Equally, authors suggest blockchain-based distributed models to amplify the reliability of the system and the integrity of data in decentralized clouds (Abdi et al., 2024; Sahar Saeed et al., 2025). Load balancing systems also assist in spreads the workloads among more than one computing node to ensure that the server is not overloaded and that the system is performed at a stable level (Pentyala, 2024; Gupta, 2024). Also, adaptive resource scheduling models are dynamically used to allocate computing resources according to the workload requirements and enhance efficiency of a system and minimize chances of service failures in the distributed cloud infrastructure (Andreyev, 2025; Nikolovski et al., 2025).

Table 5 Failure Prevention Techniques in Cloud Systems

Study	Technique	Approach Type	Advantages	Limitations
Abdi et al. (2024)	Predictive monitoring	Proactive monitoring	Early detection of system anomalies	Requires continuous monitoring infrastructure
Pentyala (2024)	Machine learning anomaly detection	AI-based prevention	Detects complex failure patterns	Requires large training datasets
Jha (2025)	AI-driven monitoring systems	Predictive analytics	Improves fault prediction accuracy	High computational cost
Welsh & Benkhelifa (2020)	Data replication and redundancy	Fault tolerance strategy	Enhances data reliability	Increased storage overhead
Sahar Saeed et al. (2025)	Blockchain-based security	Distributed prevention	Ensures data integrity	Complex implementation
Gupta (2024)	Load balancing mechanisms	Resource management	Prevents server overload	Requires efficient scheduling algorithms
Andreyev (2025)	Intelligent resource scheduling	Optimization approach	Improves workload distribution	Implementation complexity
Nikolovski et al. (2025)	Edge computing resource allocation	Distributed management	Reduces latency and improves performance	Requires coordination across nodes

5. Failure Recovery Techniques in Cloud Systems

Recovery of failures in cloud computing is essential as failure is always present in the large-scale infrastructures which are distributed. These methods aim at recovering services and reducing down time of the system after the disruption. Cloud systems can fail in terms of hardware, software, and network failure, or resource allocation, which in turn necessitates fast recovery processes to ensure continuity in operations (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018). The studies on cloud reliability also highlight that reactive recovery measures are used to supplement the preventive measures to ensure that services are not disrupted by unforeseen events (Abdi et al., 2024; Shandilya et al., 2024). Consequently, the contemporary cloud architectures combine various recovery frameworks to reinstate system functionalities and service availability in the distributed scenarios (Gupta, 2024; Rana & Giri, 2026).

Checkpointing is one of the recovery methods that are commonly used in cloud infrastructures and it entails the periodic backup of the execution state of applications or virtual machines, such that, in case of a failure, the processes can be restarted using the last saved execution state. This method will help minimize downtime dramatically since the systems

will not require starting a whole process again once the disruptions take place (Rana & Giri, 2026; Thumala, 2020). Checkpointing systems are typically provided by virtual machine snapshots or container checkpoint systems, which store system state(s) at execution (Gupta, 2024; Szorc, 2023). Replication is another significant recovery mechanism, during which critical data and services are replicated on multiple servers or storage systems to be available in the event of unavailability because of a system component failure (Welsh & Benkhelifa, 2020; Achary, 2021). Replication strategies enhance the reliability of the system since the failed components can be immediately replaced by backup nodes but can raise storage and infrastructure costs (Nikolovski et al., 2025; Gupta, 2024).

Along with checkpointing and replication, cloud infrastructures are based on failover systems, container migration approaches, and disaster recovery systems to ensure that they cannot encounter disruptions in service delivery in case of failures. Failover mechanisms automatically direct the workload of failed servers to backup computers so that applications can keep running without causing any major disruption of the service (Andreyev, 2025; Kenna, 2024). In like manner, container migration enables the migration of running applications between computing nodes in case of failures or performance concerns, thus, enabling operational continuity within containerized cloud environments (Gupta, 2024; Torres Ponce, 2025). Disaster recovery systems also facilitate scaling recovery in that they sustain backup systems and recovery procedures to allow cloud platforms to address significant failures including data center failures, data breaches or natural disasters (Ahmed et al., 2025; Filani & Opoku, 2025). All these recovery mechanisms guarantee that cloud systems will be resilient and be able to bring back the services fast in such dynamic distributed computing environments (Mukwevho & Celik, 2018; Adjei et al., 2026; Obidiagha & Antwi, 2026).

Table 6 Recovery Mechanisms in Cloud Systems

Study	Recovery Technique	Implementation	Performance Impact
Rana & Giri (2026)	Checkpointing	Virtual machine snapshot	Fast recovery with minimal downtime
Thumala (2020)	Checkpointing	System state saving during computation	Reduces process restart time
Welsh & Benkhelifa (2020)	Replication	Distributed data duplication	Improved reliability but increased storage cost
Achary (2021)	Replication	Distributed secure data storage	Enhances availability and fault tolerance
Andreyev (2025)	Failover mechanism	Backup server activation	Reduces service interruption
Kenna (2024)	Failover mechanism	Dynamic resource reassignment	Maintains system continuity
Gupta (2024)	Container migration	Container relocation across nodes	Maintains service continuity
Torres Ponce (2025)	Container migration	Cloud-based data exchange framework	Improves workload recovery
Sahar Saeed et al. (2025)	Disaster recovery system	Backup infrastructure and recovery protocols	Enables recovery from large-scale disruptions
Abdi et al. (2024)	Disaster recovery system	Secure distributed healthcare recovery frameworks	Improves system resilience

6. Comparative Analysis of Prevention vs Recovery Techniques

Failure prevention and failure recovery methods are the two complementary approaches to increasing reliability and resilience within the cloud computing environment. Prevention methods are based on the fact of detecting the possible faults of the system in its operation before the event, whereas recovery methods are aimed at restoring the services after the event. The proactive prevention systems that include predictive monitoring, anomaly detection, and smart resource allocation are trying to minimize the disruption chances by continuously examining the system behavior and identifying anomalies at the early stages (Welsh & Benkhelifa, 2020; Mukwevho & Celik, 2018). By contrast, checkpointing, replication, and failover mechanisms are recovery mechanisms that are aimed at reinstating the functionality of the system after failures have taken place, so that services are not affected by the dysfunction of the system (Abdi et al., 2024; Thumala, 2020). With the increased complexity of cloud infrastructures, the two approaches

are being merged to offer a holistic approach to failure management within distributed computing setup (Gupta, 2024; Rana & Giri, 2026).

The first significant disparity between the approaches of prevention and recovery methods is associated with the time of operations and the strategy. The prevention methods are proactive, so they keep track of the system behavior and determine some possible risks before failures have taken place, which would decrease the chances of system disruptions. Machine learning-based anomaly detection and predictive monitoring frameworks are all types of technologies that enable cloud systems to identify abnormal trends in system performance and take action before the faults develop into significant failures (Ahmed et al., 2025; Ofili et al., 2024). Recovery techniques, on the other hand, are reactive in which services are restored after failure has already happened. Checkpointing, container migration, and replication are the mechanisms that allow cloud infrastructures to resume their operations within a short period of time and reduce service outages (Rana & Giri, 2026; Torres Ponce, 2025). The two methods are thus vital because prevention provides the opportunity to minimize the occurrence of failures whereas recovery provides continuity of the system in cases where failures are bound to happen (Mukwevho & Celik, 2018; Adjei et al., 2026).

There are also performance trade-offs that exist between prevention and recovery strategies. The methods of preventive measures usually involve constantly tracking, predictive analysis, and intelligent handling of systems, which can add extra computational load and resource usage (Pentyala, 2024; Jha, 2025). Such monitoring systems have the potential to enhance the reliability of the system, but they can also create more operational complexity in large-scale distributed infrastructures (Abdi et al., 2024; Shandilya et al., 2024). Instead, recovery techniques typically involve extra infrastructure facilities like backup servers, redundant storage systems, and replication strategies to provide the ability to restore the system fast (Achary, 2021; Welsh & Benkhelifa, 2020). Though these mechanisms provide service continuity in case of failures, they can raise the storage demands and the costs of infrastructure in large deployments to the cloud (Nikolovski et al., 2025; Gupta, 2024).

The other factor in the comparison of these approaches is the cost implication and scalability issues. The prevention mechanisms usually involve investment in monitoring infrastructure, AI-driven analytics solutions, and smart coordination systems that constantly examine the performance of the system (Ahmed et al., 2025; Pentyala, 2024). Although these systems enhance the early detection of faults, they might need some advanced computing resources and data management systems to be effective in large-scale settings (Gupta, 2024; Andreyev, 2025). Architectures based on redundancy, backup infrastructures, and disaster recovery mechanisms are, however, required to revive the services in case failures have occurred (Rana & Giri, 2026; Sahar Saeed et al., 2025). Since cloud infrastructures keep growing and adopting new and emerging technologies like IoT and edge computing, it is important to integrate proactive prevention with effective recovery strategies to ensure reliable and resilient cloud computing environments (Ibitoye, 2018; Lampropoulos et al., 2024; Obidiagha & Antwi, 2026) as they grow and become more integrated with new technologies.

Table 7 Comparative Analysis of Prevention vs Recovery Techniques

Aspect	Prevention Techniques	Recovery Techniques
Goal	Avoid system failures through proactive monitoring and anomaly detection	Restore system functionality after failures occur
Time of action	Before failure occurs	After failure occurs
Cost	Monitoring infrastructure and analytics overhead	Backup infrastructure and recovery overhead
Effectiveness	Reduces probability of disruptions	Restores services and minimizes downtime
Resource usage	Continuous monitoring and predictive analysis	Redundant systems and backup resources
Scalability challenge	Managing large monitoring datasets and analytics workloads	Managing replication, redundancy, and disaster recovery infrastructure

7. Research Challenges and Future Directions

Although there have been considerable advancements in the study of cloud reliability, there are still several issues in devising scalable and robust facilities to manage failures. Among these issues, one of the most significant concerns is the scaling of fault-tolerant systems in the large-scale distributed cloud computing system. With the growth of cloud platforms to serve billions of connected things and applications with heavy data requirements, it is further complicated

to ensure consistency in fault tolerance between geographically distributed systems. Redundancy, replication, and checkpointing are fault tolerance mechanisms that need more computing resources, and distributed node coordination, which may add system overhead and complexity of operation. Future studies ought to aim at coming up with scalable fault management systems that can effectively work in highly dynamic cloud and edge computing systems.

The other significant issue is the creation of AI-based predictive systems to detect failures that would be able to detect anomalies in large-scale cloud infrastructures. The techniques of machine learning and artificial intelligence have shown a high possibility of identifying the behaviour of a complex system and anticipating its possible failure before it takes place. Nevertheless, deploying AI-based monitoring systems to a cloud setting comes with some issues in regard to the availability of training data, computational resource demand and model scalability. Also, the more frequent integration of cloud infrastructures and IoT devices and cyber-physical systems further increases predictive monitoring complexity because of the heterogeneous data input and dynamic workloads. Future studies should thus consider more effective machine learning systems and distributed intelligence systems that can be used to detect anomalies in complex cloud systems in real-time.

Another key research problem in modern cloud systems is security vulnerabilities of recovery mechanisms and the problem of multi-cloud reliability. Recovery systems like replication, container migration, and disaster recovery systems frequently depend on distributed data sharing and communication systems among various cloud systems which can subject systems to security vulnerability and information integrity threats. Moreover, the embracement of multi-cloud architecture also poses some new challenges associated with interoperability, workload migration, and coordination of resources in the heterogeneous cloud providers. The other burning issue is the real-time monitoring on the cloud systems that are distributed, in which large amounts of operational data have to be analyzed continuously to trigger anomalies and ensure stability in the system. Subsequent studies should thus be directed towards the development of secure, scalable, and intelligent monitoring schemes that will be able to aid real-time failure detection, to enable adaptive recovery in next generation cloud infrastructures.

8. Conclusion

This literature review was systematic and analyzed failure prevention and recovery strategies to improve the reliability and resiliency of the cloud-based systems. It was seen during the analysis of the chosen research that such failure prevention methods as predictive monitoring, machine learning-based anomaly detection, redundancy mechanisms, load balancing strategies and intelligent resource scheduling are among the most popular methods of preventing failures in cloud infrastructures. These proactive measures will allow identifying anomalies in the system early and will allow mitigating the risk of service disruption in distributed computing systems. Moreover, the review has found the most prevalent recovery methods mentioned as checkpointing, replication, failover mechanism, container migration, and disaster recovery frameworks to recover the services once they have fallen down. These recovery mechanisms guarantee continuity of services as they enable systems to resume normal operation soon after interruptions and at the same time sustain steady operations of big cloud infrastructures.

This review shows that the combination of proactive prevention methods and reactive recovery approaches is relevant in order to obtain robust and resilient cloud architectures. Although the prevention mechanisms can minimize the likelihood of failures by predicting their occurrence by monitoring and maintaining the intelligent systems, recovery techniques offer the necessary backup measures in case of the unavoidable failures that will restore the services. The combination of these methods in integrated resilience systems can go a long way in enhancing system availability, reliability, and performance in distributed cloud systems. These lessons include significant consequences on the design of cloud systems because future systems should be designed with intelligent monitoring, aspects, and adaptable recovery systems to accommodate more complex computing. The analysis gives an organized insight into avoidance and recovery measures of failures in cloud computing systems and points to the necessity of smart and responsive resilience architectures.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abdi, A., Bennouri, H., & Keane, A. (2024, June). Cyber resilience, risk management, and security challenges in enterprise-scale cloud systems: Comprehensive review. In *2024 13th Mediterranean Conference on Embedded Computing (MECO)* (pp. 1-8). IEEE.

[2] Abdullayeva, F. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Results in Control and Optimization*, *12*, 100268.

[3] Achary, R. (2021). Reliability and High Availability Analysis for Cloud Datacenter. In *Cloud Reliability Engineering* (pp. 31-76). CRC Press.

[4] Adjei, G., Obidiagha, C., & Antwi, B. K. (2026). Enhancing supply chain efficiency and sustainability through quality management systems in U.S. logistics operations. *International Journal for Multidisciplinary Research (IJFMR).*

[5] Ahmed, Z., Filani, A., Osifowokan, A. S., & Hutchful, N. (2025). The impact of data breaches in U.S. healthcare: A cost-benefit analysis of prevention vs. recovery.

[6] Ahmed, Z., Suleiman, A. M., Filani, A., Ocansey, I. T., & Donkor, A. A. (2025). The role of advanced machine learning algorithms in detecting and mitigating cybersecurity threats within United States healthcare digital infrastructure: A comprehensive vulnerability analysis. *Journal of Engineering and Computer Sciences*, 4(10), 218–226.

[7] Andreyev, A. (2025). Practices For Planning and Operating Multisite Network Environments Under Crisis Conditions. *Emerging Frontiers Library for The American Journal of Engineering and Technology*, *7*(09), 15-22.

[8] Czuryk, M. (2023). Cybersecurity and protection of critical infrastructure. *Studia Iuridica Lublinensia*, *32*(5), 43-52.

[9] Filani, A., & Opoku, J. A. (2025). Protecting electronic health records (EHRs): Advances and challenges in data security and privacy. *Sarcouncil Journal of Engineering and Computer Sciences*.

[10] Garraghan, P., Yang, R., Wen, Z., Romanovsky, A., Xu, J., Buyya, R., & Ranjan, R. (2018). Emergent failures: Rethinking cloud reliability at scale. *IEEE Cloud Computing*, *5*(5), 12-21.

[11] George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors. *Partners Universal International Innovation Journal*, *2*(1), 51-75.

[12] Gupta, D. (2024). *The Cloud Computing Journey: Design and deploy resilient and secure multi-cloud systems with practical guidance*. Packt Publishing Ltd.

[13] Herrera, L. C., & Maennel, O. (2019). A comprehensive instrument for identifying critical information infrastructure services. *International Journal of Critical Infrastructure Protection*, *25*, 50-61.

[14] Ibitoye, J. S. (2018). Securing smart grid and critical infrastructure through AI-enhanced cloud networking. *International Journal of Computer Applications Technology and Research*, *7*(12), 517-529.

[15] Jha, N. N. (2025). Ethical AI Audits for Observability Systems: Ensuring Equitable Resilience in Cloud Infrastructure. *Journal of Computer Science and Technology Studies*, *7*(4), 573-579.

[16] Kenna, B. (2024). Eliminating single points of failure in cloud computing: A federated multi-cloud solution for financial institutions, US government and corporations storing sensitive data off-site. *US government and corporations storing sensitive data off-site (March 05, 2024)*.

[17] Lampropoulos, G., Larrucea, X., & Colomo-Palacios, R. (2024). Digital twins in critical infrastructure. *Information*, *15*(8), 454.

[18] Mukwevho, M. A., & Celik, T. (2018). Toward a smart cloud: A review of fault-tolerance methods in cloud systems. *IEEE Transactions on Services Computing*, *14*(2), 589-605.

[19] Nikolovski, S., Milenkovski, B., & Petreska, A. (2025, June). Reliability analysis through system dynamics modeling for intellectual capital protection with a cloud services. In *2025 60th International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST)* (pp. 1-4). IEEE.

[20] Obidiagha, C., & Antwi, B. K. (2026). Standardization of supply chain monitoring tools for small and medium manufacturing enterprises. *Sarcouncil Journal of Economics and Business Management*, 5(1), 1–15.

[21] Ofili, B. T., Obasuyi, O. T., & Osaruwenese, E. (2024). Threat intelligence and predictive analytics in USA cloud security: mitigating AI-driven cyber threats. *Int J Eng Technol Res Manag*, *8*(11), 631.

[22] Panful, B., Apaflo, B., & Hutchful, N. (2025). Cyber-physical systems under threat: A case-study review of recent SCADA system attacks in the U.S. utility sector. *Journal of Engineering and Computer Sciences*, 4(12), 104–117.

[23] Pentyala, D. K. (2024). Deep Learning Techniques for Adaptive Resource Allocation and Data Reliability in Cloud Ecosystems. *International Journal of Social Trends*, *2*(3), 25-53.

[24] Rana, M., & Giri, N. (2026). AI in Cloud Disaster Recovery and Business Continuity. In *Revolutionizing the Cloud: Generative AI, Security, and Sustainability* (pp. 301-321). Cham: Springer Nature Switzerland.

[25] Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Advancing security and resilience. In *Digital Resilience: Navigating Disruption and Safeguarding Data Privacy* (pp. 459-529). Cham: Springer Nature Switzerland.

[26] Szorc, C. (2023). *Examining the Procedures of IT Organizations to Improve Fault Tolerance in a Hybrid Cloud* (Doctoral dissertation, Colorado Technical University).

[27] Thumala, S. (2020). Building Highly Resilient Architectures in the Cloud. *Nanotechnology Perceptions*, *16*(2), 264-284.

[28] Torres Ponce, M. E. (2025). Cloud-Native Resilience: DevOps and DORA in Financial Services. *Available at SSRN 5497878*.

[29] Welsh, T., & Benkhelifa, E. (2020). On resilience in cloud computing: A survey of techniques across the cloud domain. *ACM computing surveys (CSUR)*, *53*(3), 1-36.