Journal of Artificial Intelligence in Governance and Public Policy (JAIGPP)
Volume1 | Issue 2 | April-June 2026 | Pages 30-35
DOI: 10.5281/zenodo.21129297

REVIEW ARTICLE OPEN ACCESS Available online: https://jaigpp.org/index.php/j

Survey of Fault Detection Recovery and Security Assurance in Cloud Computing Systems

Dr. Jvalantkumar Kanaiyalal Patel

Assistant Professor, Shri Manilal Kadakia College Of Commerce, Management, Science And Computer Studies, Ankleshwar
jvalant007@gmail.com
Corresponding Author: *Jvalantkumar Kanaiyalal Patel (jvalant007@gmail.com)

Received: 20 April, 2026 | **Revised:** 25 May 2026 | **Accepted:** 15 June 2026

***Abstract*—Cloud computing has become a fundamental computing paradigm that delivers scalable, flexible, and cost-effective services for modern applications. However, the increasing complexity of distributed cloud infrastructures has introduced significant challenges related to fault management, service reliability, and security assurance. This survey presents a comprehensive review of fault detection, recovery, and security assurance techniques employed in cloud computing systems. It examines various cloud fault categories, including crash, Byzantine, transient, permanent, hardware, network, and service-related faults, followed by recent fault detection approaches based on anomaly detection, machine learning, artificial intelligence, log analysis, predictive analytics, and continuous monitoring. The survey further reviews fault recovery and resilience mechanisms such as fault tolerance, replication, disaster recovery, self-healing, and cloud-native orchestration. In addition, it discusses security assurance techniques including access control, authentication, intrusion detection, and AI-driven risk management for protecting cloud environments against evolving cyber threats. A comparative analysis of recent studies highlights current research trends, major contributions, and existing challenges. The survey demonstrates that integrating intelligent fault detection, automated recovery strategies, and comprehensive security assurance significantly improves cloud reliability, availability, resilience, and operational efficiency, while identifying future research opportunities for developing autonomous, secure, and trustworthy cloud computing systems.**

Keywords*—*Cloud Computing, Fault Detection, Fault Recovery, Security Assurance, Anomaly Detection, Threat Detection, Intrusion Detection System (IDS).

I. INTRODUCTION

The increasing demand for scalable, flexible, and efficient computing infrastructure has made cloud computing an essential technology for modern digital services. Cloud computing has emerged as a transformative paradigm that provides scalable, on-demand, and cost-effective computing resources over the Internet. Its rapid adoption across healthcare, finance, education, manufacturing, and business sectors has improved operational efficiency, flexibility, and service delivery [1]. As cloud platforms increasingly host mission-critical applications, ensuring continuous service availability, reliability, and security has become a primary concern for cloud providers and users alike.

Modern cloud environments consist of distributed virtual machines, containers, orchestration frameworks, storage systems, and geographically distributed data centers. The complexity of these infrastructures makes them vulnerable to hardware failures, software defects, network disruptions, configuration errors, security breaches, and environmental incidents [2]. Such failures may lead to service degradation, downtime, data loss, financial losses, and reduced user trust, emphasizing the need for effective fault management mechanisms. Cloud faults can be categorized into crash, Byzantine, transient, intermittent, permanent, hardware, network, and service-related faults. Understanding these fault types is essential for developing appropriate fault detection, tolerance, and recovery strategies that enhance the reliability and resilience of cloud computing systems [3].

Fault detection plays a fundamental role in cloud resilience by identifying abnormal behavior, performance degradation, and potential failures before they cause major service disruptions [4]. Traditional monitoring approaches have evolved into intelligent fault detection systems that employ anomaly detection, predictive analytics, machine learning, application performance monitoring, and real-time observability to enable proactive fault identification and reduce system downtime.

Fault recovery mechanisms are equally important for maintaining business continuity and high service availability [5]. Cloud platforms adopt resilience techniques such as redundancy, replication, checkpointing, failover, workload migration, disaster recovery, and self-healing architectures to automatically isolate failed components and restore normal operations with minimal human intervention, thereby improving fault tolerance and operational reliability.

Security assurance has become another critical aspect of cloud computing due to the increasing volume of sensitive data processed and stored in cloud environments [6]. It ensures that cloud services maintain confidentiality, integrity, availability, privacy, and regulatory compliance through mechanisms such as access control, encryption, intrusion detection, vulnerability assessment, auditing, and incident management. These measures strengthen the trustworthiness and security posture of cloud service providers while mitigating evolving cyber threats.

Journal of Artificial Intelligence in Governance and Public Policy, 1 (2):30-35
DOI: https://doi.org/10.5281/zenodo.21129297

A. *Structure of the paper*

The remainder of this paper is organized as follows: Section II discusses cloud fault types, Section III review's fault detection techniques, Section IV presents recovery and resilience mechanisms, Section V examines security assurance approaches, Section VI summarizes recent literature, and Section VII concludes the survey with future research directions.

II. Faults In Cloud Computing Systems

Cloud computing environments comprise distributed resources, virtual machines, storage systems, networks, and applications that collaboratively deliver services. The complexity and large-scale nature of these infrastructures make them vulnerable to faults that can degrade performance, availability, and reliability. Understanding different fault categories is essential for developing effective fault detection, recovery, and fault-tolerance mechanisms. Based on the surveyed literature, cloud faults are classified according to their behavior, duration, and affected components.

A. *Crash Faults and Byzantine Faults*

Crash faults occur when a system component completely stops functioning due to hardware failures, software crashes, or power outages. In contrast, Byzantine faults allow components to continue operating while producing incorrect or inconsistent results, making them more difficult to detect and significantly affecting system reliability and security.

B. *Faults Based on Duration*

Based on persistence, faults are classified as transient, intermittent, and permanent. Transient faults disappear without intervention, intermittent faults recur unpredictably, and permanent faults remain until the faulty component is repaired or replaced. This classification supports the selection of suitable detection and recovery strategies.

C. *Physical and Hardware Faults*

These faults originate from failures in processors, memory, storage devices, cooling systems, or power supplies within cloud data centers [7]. Such failures may cause service interruptions, performance degradation, and resource unavailability, requiring redundancy and failover mechanisms to maintain system reliability.

D. *Network Faults*

These faults arise from communication failures, including packet loss, link failures, routing errors, bandwidth congestion, and transmission delays. They can disrupt data transfer, reduce service accessibility, and degrade overall system performance, making continuous network monitoring and fault-tolerant communication essential.

E. *Processor and Service Faults*

Processor or node faults result from software defects, resource shortages, inefficient processing, or virtual machine failures. Service-related faults include service expiry and timing faults, where applications exceed execution limits or fail to meet required deadlines, adversely affecting application performance and quality of service.

III. Fault Detection Techniques In Cloud Computing Systems

Fault detection plays a crucial role in maintaining the reliability and availability of cloud computing systems by identifying failures at an early stage. Various detection techniques have been developed to improve fault identification accuracy, enable proactive management, and minimize service disruptions in dynamic cloud environments.

A. *Anomaly Detection Techniques*

These techniques identify abnormal system behavior that may indicate failures, resource degradation, or security threats [8]. Traditional approaches include statistical analysis, rule-based methods [9], and clustering, whereas recent AI-driven models employ machine learning and deep learning to detect complex anomalies in real time. Such methods improve detection accuracy, scalability, adaptability, and reduce false alarms in cloud environments.

B. *Machine Learning and AI-Based Fault Detection Techniques*

Machine learning and artificial intelligence enable intelligent analysis of large-scale cloud data to identify fault patterns and classify anomalies [10]. Supervised, unsupervised, ensemble, and deep learning models, including autoencoders and neural networks, provide high detection accuracy. These techniques also support predictive and self-healing capabilities, improving cloud resilience, adaptability, and fault detection efficiency.

C. *Logging-Based Detection Techniques*

System Log analysis provides valuable operational insights for anomaly detection and fault diagnosis [11]. Techniques such as log parsing, feature extraction, anomaly prediction, and root-cause analysis are often combined with ensemble learning, support vector machines, logistic regression, and principal component analysis to improve detection accuracy and fault localization [12]. These methods are well suited for modern cloud-native environments [13].

D. *Failure Prediction*

Failure prediction focuses on identifying potential faults before they affect cloud services. Predictive models analyze historical system metrics and workload characteristics using artificial intelligence and machine learning to anticipate failures. This proactive approach supports preventive maintenance, minimizes downtime, improves resource utilization, and enhances the reliability of large-scale cloud infrastructures[14].

E. *Monitoring and Diagnostics*

Continuous monitoring collects performance data from cloud resources, virtual machines, applications, and network services to identify abnormal conditions. Diagnostic techniques utilize this information for root-cause analysis, anomaly localization, and reliability assessment [15]. Effective monitoring and diagnostics enable rapid fault identification, improve service continuity, and support efficient cloud management.

IV. Fault Recovery And Resilience Mechanisms

Cloud computing systems require effective recovery and resilience mechanisms to maintain service continuity during hardware failures, software faults, network disruptions, and

Journal of Artificial Intelligence in Governance and Public Policy, 1 (2):30-35
DOI: https://doi.org/10.5281/zenodo.21129297

cyberattacks [16]. These mechanisms combine fault tolerance, redundancy, disaster recovery, and self-healing technologies to minimize downtime, improve availability, and ensure reliable cloud service operation [17]. The major fault recovery and resilience mechanisms discussed in this section include:

A. Fault Tolerance Mechanisms

Fault tolerance enables cloud systems to continue operating despite component failures by preventing service interruptions and maintaining system functionality. Common techniques include checkpointing [18], failover, fault isolation, workload migration, and distributed resource management. Modern cloud-native platforms further enhance fault tolerance through automated orchestration and adaptive recovery, improving reliability and reducing service disruption [19].

B. Replication and Redundancy Strategies

Replication and redundancy improve cloud resilience by maintaining multiple instances of critical services, storage, and computing resources. Backup resources automatically replace failed components [20], ensuring continuous service availability. Modern cloud platforms dynamically manage service replication, container rescheduling, and resource reallocation to achieve reliable recovery while balancing performance, storage efficiency, and operational cost.

C. Disaster Recovery and High Availability

Disaster recovery and high availability ensure business continuity during large-scale failures. High availability minimizes service interruptions through load balancing, failover, redundancy, and continuous health monitoring, whereas disaster recovery restores applications and data using backup, replication, and predefined recovery procedures [21]. These mechanisms reduce Recovery Time Objective (RTO) and Recovery Point Objective (RPO), enabling rapid restoration of cloud services after critical failures [22].

D. Self-Healing and Auto-Recovery Systems

Self-healing systems automatically detect faults, diagnose root causes, and execute recovery actions without human intervention [23]. Using artificial intelligence, machine learning, predictive analytics, and orchestration platforms such as Kubernetes, these systems perform service restarts, workload migration, resource scaling, and automated remediation. Such capabilities reduce Mean Time to Detection (MTTD) and Mean Time to Repair (MTTR), while enhancing cloud resilience, availability, and operational efficiency.

E. Cloud-Native Resilience Mechanisms

Cloud-native resilience mechanisms enhance system reliability by utilizing containerization, orchestration, and automated resource management. Technologies such as Kubernetes enable health monitoring, container restart, workload rescheduling, auto-scaling, and self-healing to maintain uninterrupted service delivery [24]. These mechanisms improve fault recovery, operational flexibility, and resilience in modern distributed cloud environments.

V. Security Assurance Techniques For Cloud Systems

Ensuring secure and trustworthy cloud services is essential for protecting distributed computing environments from evolving cyber threats. Security assurance safeguards the confidentiality, integrity, availability, and reliability of cloud resources through access control, authentication, intrusion detection, and AI-driven security techniques. These mechanisms strengthen security posture, establish user trust, and support regulatory compliance.

A. Cloud Security Threats and Challenges

Cloud computing presents significant security challenges due to its distributed architecture, shared resources, and internet-based service delivery. Common threats include data breaches, unauthorized access, malware, denial-of-service attacks, API vulnerabilities, and misconfigurations. Organizations must also address data privacy, regulatory compliance, and secure resource management through continuous monitoring, risk assessment, and proactive security measures. The major security challenges are summarized as follows:

- **Data Breaches and Data Leakage:** Unauthorized access to sensitive information due to weak security controls or misconfigurations.
- **Misconfigurations and Human Errors:** Incorrect security settings remain one of the leading causes of cloud security incidents.
- **Advanced Persistent Threats (APTs) and Malware:** Sophisticated attacks targeting cloud resources through stealthy and long-term intrusion techniques.
- **Distributed Denial-of-Service (DDoS) Attacks:** Attackers can overwhelm cloud services, causing service disruptions and downtime.

B. Access Control and Authentication Mechanisms

Authorization and authentication ensure secure access to cloud resources by verifying user identities and regulating permissions. Cloud platforms employ Identity and Access Management (IAM), role-based access control (RBAC), multi-factor authentication (MFA), and adaptive authentication to prevent unauthorized access and privilege misuse. These mechanisms strengthen security, improve governance, and support compliance across dynamic and multi-cloud environments [25].

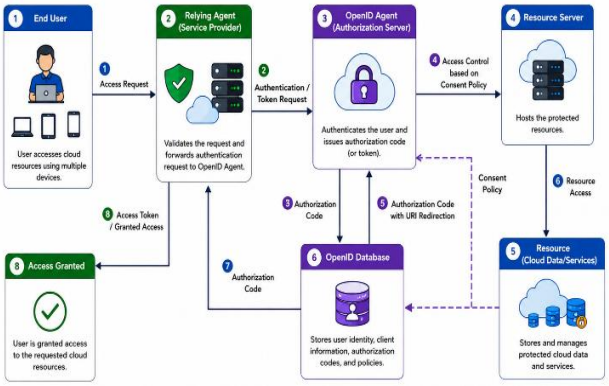

Fig .1. OpenID-Based Security Assurance Framework for Authentication, Authorization, and Secure Access Control in Cloud Computing Systems

C. Intrusion Detection and Prevention Systems

Intrusion prevention and detection systems are essential for identifying and mitigating cyber threats in cloud environments [26]. These systems continuously monitor network traffic, user activities, and system behavior using signature-based, anomaly-based, and behavior-based detection techniques. Their integration with monitoring and

DOI: https://doi.org/10.5281/zenodo.21129297

incident response frameworks enables rapid threat detection, containment, and remediation, thereby enhancing the security and resilience of cloud infrastructures [27][28]. The major prevention mechanisms are as follows: -

- **Signature-Based Prevention:** Blocks known attacks by matching traffic patterns with predefined threat signatures.
- **Real-Time Traffic Monitoring:** Continuously inspects network traffic to detect and stop malicious activities immediately.
- **Automated Threat Containment:** Isolates compromised systems and blocks suspicious IP addresses to prevent attack propagation

D. AI-Driven Security and Risk Management

Artificial intelligence (AI) and machine learning (ML) enhance cloud security by enabling intelligent threat detection and automated risk management [29]. These techniques identify anomalies, predict cyber threats, automate incident response, and support adaptive access control. As a result, they improve security, strengthen resilience, and protect cloud environments from evolving cyber threats.

VI. Literature Review

The literature reviewed in this section highlights recent advancements in fault detection, recovery, and security assurance for cloud computing systems. It examines AI-driven approaches, predictive techniques, self-healing mechanisms, and systematic reviews while identifying existing research gaps and future development opportunities.

Adeel Ali (2026) examines AI-based anomaly detection not as a neutral technical instrument, but as a potent socio-technical influence mechanism that reconfigures organizational judgment, authority, and power. Adopting an interpretive lens grounded in sociotechnical systems theory, sensemaking, and institutional theory, the research investigates how algorithmic outputs shape human interpretation of risk, renegotiate the locus of decision authority, and alter governance structures [30].

Md. Tarek Hasan and Ishtiaque Ahmed (2025) the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework to ensure transparency, replicability, and methodological rigor. A total of 96 peer-reviewed studies published between 2014 and 2024 were systematically analyzed, encompassing empirical, experimental, and theoretical investigations drawn from major academic databases [31].

Hemant Gadde (2024) explores the application of artificial intelligence (AI) techniques in enhancing fault detection and recovery mechanisms within high-availability databases. By leveraging machine learning algorithms and predictive analytics, we propose a novel framework that not only identifies potential faults in real-time but also initiates proactive recovery processes. The proposed AI-powered approach achieves an average fault detection rate of 95% and a recovery time reduction of 40% compared to traditional methods [32].

Rahul Vadisetty et al. (2024) provide a comprehensive review of AI-powered self-healing and fault-tolerant cloud infrastructures, covering their underlying architectures, machine learning techniques, and real-world applications. Finally, we also talk about the issues that AI fault tolerance poses and what future research could be focused on to ensure that cloud computing is more resilient and reliable [33].

Farida Asadova et al. (2023) the basic concepts of the Anytime algorithm in existing works as well as its benefits of usage are analyzed. Various literature is reviewed and combined for possible fault recognition and time deliberation. The paper includes details of anytime processing in fault detection in different subject areas [34].

Wenjin Yu et al. (2022) propose a complete and optimized IoT Big Data ecosystem embedded into a three-layer architecture for predictive maintenance applications. The proposed architecture consists of an edge layer, a cloud layer, and an application layer. The proposed edge infrastructure distributes the tasks effectively between the cloud layer and edge layer. On top of the architecture, different layers are integrated seamlessly to address reliability and scalability issues [35].

Table I summarizes recent studies on fault detection, recovery, and security assurance in cloud computing, highlighting their focus areas, major findings, research gaps, and key contributions to identify current trends and future research directions.

TABLE I. Summery Of The Recent Studies On Fault Detection, Recovery, And Security Assurance In Cloud Computing

Author	Focus Area	Key Findings	Challenges / Research Gap	Key Contributions
Adeel Ali (2026)	AI-based anomaly detection and governance	AI reshapes organizational decision-making and risk assessment.	Limited attention to practical deployment, scalability, and quantitative performance evaluation.	Examines the socio-technical impact of AI-driven anomaly detection in cloud environments.
Md. Tarek Hasan and Ishtiaque Ahmed (2025)	Systematic review of AI-based fault detection	PRISMA-based review summarizes research published between 2014–2024.	Lacks unified benchmarking and standardized evaluation frameworks.	Provides a comprehensive synthesis of AI-driven fault detection research.
Hemant Gadde (2024)	AI-enabled fault detection and recovery	Achieved 95% detection accuracy and 40% faster recovery.	Validation in large-scale heterogeneous cloud environments remains limited.	Proposes an AI-powered framework for real-time fault detection and proactive recovery.
Rahul Vadisetty et al. (2024)	AI-based self-healing cloud infrastructures	Reviews architectures, AI techniques, and practical applications.	Intelligent autonomous recovery and real-world implementation require further investigation.	Presents a comprehensive review of AI-powered self-healing and fault-tolerant systems.
Farida Asadova et al. (2023)	Anytime algorithms for fault detection	Demonstrates the applicability of anytime algorithms across multiple domains.	Limited cloud-specific validation and integration with intelligent recovery mechanisms.	Reviews anytime processing techniques for efficient fault recognition.

Wenjin Yu et al. (2022)	IoT-edge-cloud predictive maintenance	Proposes a three-layer architecture for scalable predictive maintenance.	Security assurance and cloud fault recovery integration remain insufficient.	Develops an optimized edge–cloud architecture to improve reliability and scalability.

VII. Conclusion and Future Work

Cloud computing has become a fundamental platform for delivering scalable, flexible, and reliable computing services across diverse application domains, making effective fault management and security assurance essential for maintaining service continuity. This survey comprehensively reviewed the major fault types, fault detection techniques, recovery and resilience mechanisms, and security assurance approaches adopted in modern cloud computing systems. The study examined intelligent anomaly detection, machine learning and AI-based fault diagnosis, logging and monitoring techniques, predictive failure analysis, fault tolerance, replication, disaster recovery, self-healing architectures, cloud-native resilience, and advanced security mechanisms including authentication, intrusion detection, and AI-driven risk management. Furthermore, a comparative review of recent research highlighted the growing adoption of intelligent and autonomous cloud management while identifying existing challenges related to scalability, heterogeneous environments, standardized evaluation, and integrated security assurance. Overall, the survey demonstrates that combining AI-driven fault detection, automated recovery mechanisms, and comprehensive security assurance significantly enhances the reliability, availability, resilience, and trustworthiness of next-generation cloud computing systems.

Future research should focus on developing unified AI-driven frameworks that integrate fault detection, autonomous recovery, and security assurance within cloud-native and multi-cloud environments. Emphasis should also be placed on explainable AI, Zero Trust security, federated learning, standardized benchmarking, and energy-efficient resilient cloud infrastructures for intelligent and trustworthy cloud service management.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The author declares no conflict of interest.

How to cite this article
J. K. Patel, "Survey of Fault Detection Recovery and Security Assurance in Cloud Computing Systems," *Journal of Artificial Intelligence in Governance and Public Policy*, vol. 1, no. 2, pp. 30–35, Apr.–Jun. 2026.**DOI**, XXXXXXXXX

References

[1] A. Warrier, "iPaaS Solutions for Healthcare Enterprise Integration: Cloud-Native Integration Platforms for Multi-System Orchestration," *Int. J. Lead. Res. Publ.*, vol. 3, no. 1, pp. 1–9, Jan. 2022, doi: 10.70528/IJLRP.v3.i1.1770.

[2] N. B. Okwechime, C. J. Ifechukwu-Jacobs, and O. L. Uzoka, "Cloud Computing System Use and its Effects on Entrepreneurial Venture Performance of Information Technology Firms in Delta State .," *J. Emerg. trends Manag. Sci. Entrep.*, vol. 8, no. 1, pp. 1–18, 2026.

[3] A. U. Rehman, R. L. Aguiar, and J. P. Barraca, "Fault-Tolerance in the Scope of Cloud Computing," in *IEEE Access*, IEEE, 2022, pp. 63422-63441,. doi: 10.1109/ACCESS.2022.3182211.

[4] R. K. Gadiraju, "A Novel Machine Learning Method for Fault Prediction and Reliability in Software Systems," *Int. J. Sci. Res. Sci. Eng. Technol.*, vol. 12, no. 3, pp. 1226–1238, Jun. 2025, doi: 10.32628/IJSRSET2512163.

[5] M. Jain, "Survey Of Resilience Strategies In Cloud Platforms : From Fault Detection To Auto-Recovery," *J. Glob. Res. Math. Arch.*, vol. 12, no. 9, p. 9, 2025.

[6] A. Shukla, B. Katt, and M. Mudassar, "A quantitative framework for security assurance evaluation and selection of cloud services : a case study," *Int. J. Inf. Secur.*, vol. 22, no. 6, pp. 1621--1650, 2023, doi: 10.1007/s10207-023-00709-8.

[7] H. N. Dholariya, "Human-in-the-Loop AI for Cloud Data Engineering: The Collaborative Intelligence Architecture (CIRA) for Regulated Industries," *J. Inf. Syst. Eng. Manag.*, vol. 11, no. 1s, pp. 883–898, Jan, 2026.

[8] A. Gupta, "What Is The Right Security Posture? A Perspective on Cloud Computing Security Threats and Risk Assessment," *Int. J. Emerg. Res. Eng. Technol.*, vol. 4, no. 4, pp. 120–127, December, 2023, doi: 10.63282/3050-922X.IJERET-V4I4P112.

[9] C. Nwachukwu, K. Durodola-Tunde, and C. Akwiwu-Uzoma, "AI-driven anomaly detection in cloud computing environments," *Int. J. Sci. Res. Arch.*, vol. 13, no. 2, pp. 692–710, Nov. 2024, doi: 10.30574/ijsra.2024.13.2.2184.

[10] B. Yahya, "Artificial Intelligence – Driven Fault Detection in Distributed Computer Systems," *World J. Adv. Eng. Technol. Sci.*, vol. 16, no. September, p. 13, 2025.

[11] R. K. Gadiraju, "Machine Learning-Based Anomaly Detection in Enterprise Hardware Telemetry Streams," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 10, no. 9, pp. 262–271, Sep. 2022, doi: 10.17762/ijritcc.v10i9.11948.

[12] B. Wang *et al.*, "Research on anomaly detection and real-time reliability evaluation with the log of cloud platform," *Alexandria Eng. J.*, vol. 61, no. 9, pp. 7183–7193, 2022, doi: 10.1016/j.aej.2021.12.061.

[13] J. B. Mehta, "AI-Driven Test Engineering for Cloud-Native Systems," *Int. J. Data Sci. IoT Manag. Syst.*, vol. 5, no. 1, 2026, doi: 10.64751/ijdim.2026.v5i1.297.

[14] J. H. Abro *et al.*, "Artificial Intelligence Enabled Effective Fault Prediction Techniques in Cloud Computing Environment for Improving Resource Optimization," *Sci. Program.*, vol. 2022, no. 1, p. 7432949, 2022, doi: 10.1155/2022/7432949.

[15] M. Vani, "AI-Based Distributed Systems Observation System : Real-Time Monitoring And Intelligent Anomaly Detection For Cloud Infrastructure," *Power Syst. Prot. Control*, vol. 53, no. 4, pp. 446–457, 2025, doi: 10.46121/pspc.53.4.30.

[16] S. Irfan, "Enhancing Email Security Through Accurate Phishing Detection Using Deep Transformer Models," in *2026 World Conference on Computational Science and Technology (WcCST)*, 2026, pp. 239–244. doi: 10.1109/WcCST67302.2026.11495864.

[17] D. K. Pentyala, "Artificial Intelligence for Fault Detection in Cloud- Optimized Data Engineering Systems," *Int. J. Soc. Trends*, vol. 2, no. 4, pp. 8–44, 2024.

[18] A. Rezaeipanah, M. Mojarad, and A. Fakhari, "Providing a new

approach to increase fault tolerance in cloud computing using fuzzy logic," *Int. J. Comput. Appl.*, vol. 44, no. 2, pp. 139–147, 2022, doi: 10.1080/1206212X.2019.1709288.

[19] W. Survey and F. Directions, "Fault Tolerance Structures in Wireless Sensor Networks (WSNs): Survey, Classification, and Future Directions," *Sensors*, vol. 22, no. 16, p. 6041, 2022.

[20] K. K. Pattan, "Fault Recovery And Resilience In Containerized Distributed Systems," *Int. J. Sci. Technol.*, vol. 14, no. 3, pp. 1–25, 2023.

[21] C. Luca, "High Availability , Fault Tolerance , and Disaster Recovery Strategies," 2025, *ResearchGate*.

[22] V. K. Sharma and A. K. S, "Hierarchical Cloud-IoT Architecture for AI-Powered Intelligent Disaster Response," in *2025 7th International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*, IEEE, Oct. 2025, pp. 603–610. doi: 10.1109/ICIDCA66325.2025.11280408.

[23] M. Sengupta, "The Influence of Self-Healing Infrastructure on Enterprise Service Resilience," 2023, *Research Gate*.

[24] V. Sharma, "Cloud-Native 5G Deployments: Kubernetes and Microservices in Telco Networks," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 10, no. 3, pp. 1–8, May 2022, doi: 10.37082/IJIRMPS.v10.i3.232706.

[25] J. B. Mehta, "Autonomous Workload Right-Sizing for Multi-Cloud Cost Optimization," in *2026 International Conference on Artificial Intelligence, Systems, and Emerging Technologies (ICAISET)*, Cairo, Egypt: IEEE, 2026, pp. 1–11, June. doi: 10.1109/ICAISET66439.2026.11541899.

[26] A. Joon, B. K. R. Janumpally, A. Gogineni, and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," in *2025 5th International Conference on Intelligent Technologies (CONIT)*, 2025, pp. 1–8. doi: 10.1109/CONIT65521.2025.11167760.

[27] J. J. Ang'udi and S. Awour, "Security challenges in cloud computing: A comprehensive analysis," *World J. Adv. Eng. Technol. Sci.*, vol. 10, no. 2, pp. 155–181, Dec. 2023, doi: 10.30574/wjaets.2023.10.2.0304.

[28] B. P. Singh and H. Singh, "Using LLMs for Autonomous Cloud Infrastructure Entitlement Management to Prevent Overprivileged Access," *J. Eng. Comput. Sci.*, vol. 5, no. 4, pp. 1–14, April, 2026, doi: 10.5281/zenodo.19488212.

[29] R. Vadisetty, A. Polamarasetti, and S. K. Rongali, "AI-Driven Threat Detection: Enhancing Cloud Security with Generative Models for Real-Time Anomaly Detection and Risk Mitigation," *J. Comput. Anal. Appl.*, vol. 31, no. 3, pp. 532–543, 2023.

[30] A. Ali, "Decision-Making In Cloud Security Management Using AI-Based Anomaly Detection : A Social Sciences Perspective," *Spectr. Eng. Sci.*, vol. 4, no. 2, pp. 55–69, 2026.

[31] M. T. Hasan and I. Ahmed, "AI-Driven Anomaly Detection for Data Loss Prevention and Security Assurance in Electronic Health Records," *Rev. Appl. Sci. Technol.*, vol. 04, no. 03, pp. 35–67, Sep. 2025, doi: 10.63125/dzyr0648.

[32] H. Gadde, "AI-Powered Fault Detection and Recovery in High-Availability Databases," *Int. J. Mach. Learn. Res. Cybersecurity Artif. Intell.*, vol. 15, no. 1, pp. 500–537, 2024.

[33] R. Vadisetty, A. Polamarasetti, J. B. Butani, S. Prajapati, and V. Raghunath, "AI-Powered Self-Healing and Fault-Tolerant Cloud Infrastructures for Improved Resilience and Reliability," *J. Inf. Syst. Eng. Manag.*, vol. 9, no. 1, p. 10, 2024.

[34] F. Asadova, A. R. Varkonyi-Koczy, G. Kertész, and R. Lovas, "A Survey of Usage of Anytime Algorithm in Fault Detection in Cloud Systems," in *2023 IEEE 21st World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Herl'any, Slovakia: IEEE, 2023, pp. 69-74,January. doi: 10.1109/SAMI58000.2023.10044521.

[35] W. Yu, Y. Liu, T. Dillon, and W. Rahayu, "Edge Computing-Assisted IoT Framework With an Autoencoder for Fault Detection in Manufacturing Predictive Maintenance," *IEEE Trans. Ind. Informatics*, vol. 19, no. 4, pp. 5701–5710, 2022, doi: 10.1109/TII.2022.3178732.