



Accelerating Incident Diagnosis and Service Recovery Through Generative AI-Assisted Failure Intelligence in Critical Digital Infrastructure

Mashiat Nabila¹;

[1]. M.S. in Engineering Data Science; University of Houston, Cullen College of Engineering
Houston, TX, USA; Email: nabila.mashiat@gmail.com

Doi: [10.63125/61etqg30](https://doi.org/10.63125/61etqg30)

Received: 19 March 2026; Revised: 21 April 2026; Accepted: 09 May 2026; Published: 10 June 2026;

Abstract

Critical digital infrastructure increasingly depends on cloud platforms, telecommunications systems, enterprise digital services, distributed applications, data centers, and interconnected computing environments, yet incident-response teams often struggle to interpret the large volumes of fragmented logs, alerts, metrics, traces, configuration records, and service-dependency information generated during failures. This study examined whether Generative AI-assisted failure intelligence can accelerate incident diagnosis and improve service recovery performance in critical digital infrastructure. The study adopted a quantitative, cross-sectional, case-based research design involving cloud and enterprise cases across cloud platforms, telecommunications systems, enterprise digital services, distributed computing environments, data centers, and other mission-critical infrastructures. Using purposive sampling, data were collected from Site Reliability Engineers, DevOps engineers, cloud engineers, network engineers, platform engineers, infrastructure specialists, systems engineers, AIOps professionals, incident managers, system architects, and technical managers. Of 320 questionnaires distributed, 298 were returned and 286 were valid and usable, producing an 89.4% valid response rate. The four explanatory variables were Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, and Generative AI-Assisted Recovery Recommendation, while Incident Diagnosis and Service Recovery Performance was the dependent variable. Analysis included descriptive statistics, Cronbach's alpha, KMO and Bartlett's tests, Pearson correlation, multiple regression, ANOVA, VIF, tolerance, Durbin-Watson testing, and hypothesis evaluation. Incident Diagnosis and Service Recovery Performance Recorded $M = 4.19$, $SD = 0.53$. Generative AI-Enabled Root Cause Analysis showed the strongest correlation, $r = .76$, $p < .001$, and the largest regression effect, $\beta = .33$, $p < .001$, followed by Recovery Recommendation, $\beta = .29$, Knowledge Synthesis, $\beta = .24$, and Failure Data Interpretation, $\beta = .22$. The overall model explained 70.8% of performance variance, $R^2 = .708$, Adjusted $R^2 = .704$, $F(4, 281) = 170.35$, $p < .001$. These findings indicate that organizations should prioritize evidence-grounded Generative AI systems that integrate causal reasoning, contextual knowledge, observability data, and validated recovery guidance to strengthen diagnostic accuracy, reduce incident uncertainty, and support faster and more reliable service restoration.

Keywords

Generative Artificial Intelligence, Failure Intelligence, Root Cause Analysis, Incident Diagnosis, Service Recovery;

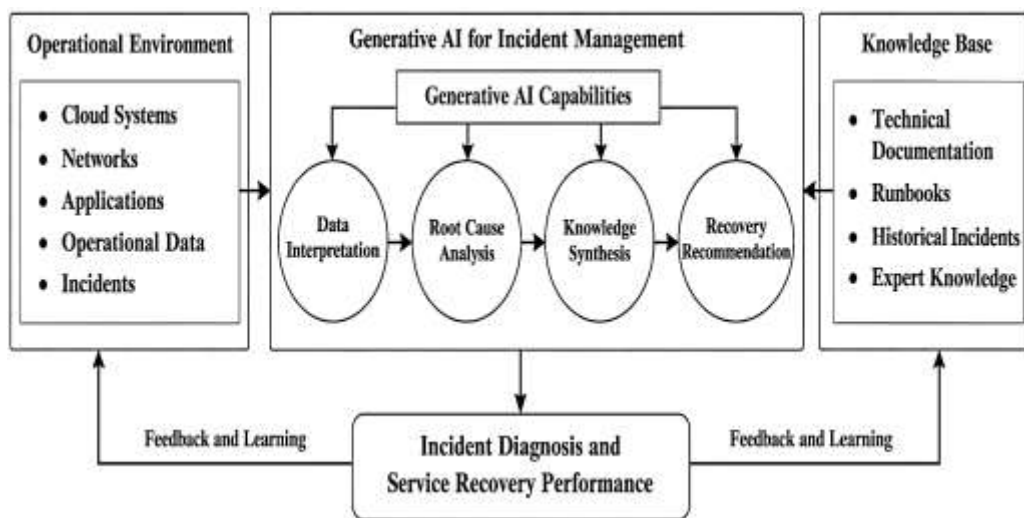
INTRODUCTION

Critical digital infrastructure refers to the interconnected ecosystem of cloud platforms, data centers, telecommunications networks, enterprise information systems, distributed applications, microservice architectures, computing resources, and operational technologies whose continuous functioning supports essential organizational, commercial, governmental, and societal activities. Within these environments, an incident can be defined as an unexpected event or abnormal operational condition that disrupts a digital service, reduces its expected performance, compromises availability, or requires technical intervention to restore normal functionality. Incident diagnosis involves collecting and interpreting evidence concerning abnormal system behavior, identifying affected components and dependencies, establishing probable causes, and generating sufficient technical understanding to support appropriate remedial action. Service recovery refers to the process through which disrupted or degraded digital services are restored to an acceptable level of functionality, availability, and operational stability. Artificial Intelligence for IT Operations, commonly described as AIOps, combines artificial intelligence, machine learning, operational telemetry, and automation to support these failure-management activities across complex information technology environments (Kanti, 2026; Notaro et al., 2021). Generative artificial intelligence extends conventional analytical capabilities by using large language models and related generative architectures to interpret, organize, contextualize, and generate information from large volumes of textual and semi-structured technical data (Fan et al., 2023; Hou et al., 2024; Shamima, 2026). Within this study, Generative AI-assisted failure intelligence refers specifically to the ability of Generative AI systems to interpret failure-related operational evidence, facilitate root-cause reasoning, synthesize contextual incident knowledge, and produce recovery-oriented recommendations. This capability is internationally significant because contemporary critical services increasingly depend on globally distributed digital systems in which cloud resources, network infrastructure, software services, databases, application components, and third-party dependencies interact continuously. Failures within these environments can affect multiple technical layers simultaneously, making incident analysis increasingly dependent on rapid interpretation of heterogeneous information and accurate identification of service dependencies (Badrul, 2026; Soldani & Brogi, 2023; Yu et al., 2024). Contemporary AIOps research also identifies logs, metrics, traces, alerts, incident reports, documentation, and operational knowledge repositories as essential sources of failure intelligence that can be processed by advanced artificial intelligence systems during incident diagnosis and recovery activities (Chowdhury, 2026; Zhang et al., 2025).

The complexity of incident diagnosis within critical digital infrastructure arises substantially from the volume, heterogeneity, velocity, and fragmented meaning of operational information generated during system failures. Modern computing environments continuously produce application logs, infrastructure events, distributed traces, network telemetry, monitoring alerts, performance metrics, configuration records, error messages, and service-state information. These forms of evidence can indicate that abnormal behavior has occurred, but they do not automatically identify why an incident has occurred, how different events are connected, or which technical intervention should be prioritized. Large-scale system monitoring research established that manual examination of console logs becomes increasingly impractical as computing systems grow in size and complexity, creating a need for automated mechanisms capable of transforming unstructured operational text into diagnostic information (Pervaz, 2026; Xu et al., 2009). Similar research demonstrated that unstructured distributed-system logs can provide meaningful indicators of abnormal execution when appropriate analytical techniques are applied to recurring event patterns and execution behavior (Fu et al., 2009; Kaium, 2026). The usefulness of operational logs for diagnosis also depends heavily on how raw messages are parsed, structured, grouped, and converted into representations suitable for automated analysis (He et al., 2016; S. He et al., 2016; Rahman, 2026). Online parsing approaches have improved the processing of streaming log messages by converting repetitive textual events into structured templates that can subsequently be analyzed for abnormal behavior (He et al., 2017; Ahmed, 2026). Deep-learning methods further changed log analysis by treating system-event sequences as learnable behavioral patterns, allowing abnormal sequences to be detected based on deviations from patterns observed during normal system operation (Du et al., 2017; Khalid, 2026). Semantic and sequential approaches have also shown that both event ordering and quantitative relationships within log streams

can contribute to anomaly identification in complex computing systems (Jannatul, 2026; Meng et al., 2019). Transformer-based representations have strengthened contextual log analysis by learning relationships among event sequences and recognizing operational behavior that differs from normal patterns (Mohammad, 2026; Guo et al., 2021). Automated log-analysis research consequently encompasses several interconnected reliability tasks, including parsing, anomaly detection, failure prediction, fault localization, and diagnostic support rather than a single detection function (He et al., 2021; Jahanara, 2026). Model performance can also vary substantially according to data selection, event grouping, training conditions, noise, class imbalance, and changes in operational log structures (Landauer et al., 2023; Le & Zhang, 2022).

Figure 1: Generative AI-Assisted Failure Intelligence Framework for Incident Diagnosis and Service Recovery Performance



AIOps research has gradually expanded failure management from conventional monitoring and alert generation toward an integrated operational process involving anomaly identification, event correlation, failure localization, root-cause analysis, troubleshooting, mitigation, and service restoration. Intelligent failure-management research demonstrates that artificial intelligence can intervene at multiple stages of the incident lifecycle, including the interpretation of monitoring evidence, prioritization of abnormal events, identification of probable causes, and selection of corrective actions (Notaro et al., 2021; Tonay, 2025). One major operational problem is that troubleshooting knowledge is frequently distributed across runbooks, technical documentation, historical incident reports, engineering notes, support guides, and the experience of individual specialists. Such information may be available within an organization while remaining difficult to retrieve and apply rapidly during high-pressure service incidents. Research based on production troubleshooting documentation has shown that operational knowledge can be transformed from unstructured technical guidance into more executable troubleshooting workflows through combinations of machine learning and automated synthesis techniques (Sadia, 2025; Shetty et al., 2022). Large-scale empirical evidence from production cloud environments has also demonstrated that incident resolution can become prolonged when deficiencies occur across detection, diagnosis, root-cause identification, mitigation, and coordination activities (Ghosh et al., 2022; Sadia, 2025). The root-cause problem becomes particularly difficult in microservice and distributed architectures because independently deployed services interact through complex communication and dependency relationships, allowing a failure originating in one component to influence several downstream services (Nishat, 2025; Soldani & Brogi, 2023). Causal-analysis techniques have therefore been developed to identify relationships among system variables and temporal events that may reveal the originating source of a service disruption (Lin et al., 2024; Badrul, 2025). Failure diagnosis also requires attention to cascading behavior because the technical cause of an outage may differ from the components in which operational symptoms are most visible. Log-based analysis has increasingly been applied to

explain how failures propagate across interacting microservices and to reconstruct chains of abnormal events associated with cascading service disruptions (Soldani et al., 2025). At the broader operational level, intelligent failure management also depends on data engineering, model management, deployment practices, process coordination, and organizational integration, indicating that effective AIOps involves a connected operational lifecycle rather than isolated machine-learning models (Diaz-de-Arcaya et al., 2023; Pervaz, 2025). These conditions establish the need for failure intelligence capable of connecting fragmented technical evidence with contextual knowledge during diagnosis and recovery.

Generative AI and large language models introduce a distinct form of operational failure intelligence because they are capable of processing natural language, technical documentation, historical incident records, structured and semi-structured operational evidence, and contextual information while generating explanations and recommended actions in forms accessible to human operators. Research on large language models in software engineering has documented their application to debugging, software maintenance, program repair, documentation, code analysis, technical reasoning, and other activities that require interpretation of complex software-related information (Fan et al., 2023; Hou et al., 2024; Chowdhury, 2025). These capabilities have increasingly been examined within production incident-management environments. Large-scale cloud research involving more than 40,000 production incidents has evaluated the ability of language models to recommend probable root causes and mitigation steps, establishing direct empirical relevance between Generative AI and the informational requirements of engineers responsible for restoring disrupted services (Ahmed et al., 2023; Kaium, 2025). Generative AI-supported root-cause systems have also been developed to associate incidents with appropriate handlers, collect diagnostic evidence, classify probable root causes, and generate explanatory narratives that assist engineers during incident investigation (Chen et al., 2024; Arif Uz et al., 2025). The quality of Generative AI-based diagnosis can depend substantially on the contextual evidence supplied to the model. In-context learning research based on more than 100,000 production incidents has demonstrated that the inclusion of relevant examples and operational context can improve the generation of root-cause explanations compared with less contextualized configurations (Rahman, 2025; Zhang et al., 2024). Agent-based approaches extend this capability by enabling language models to retrieve additional evidence, invoke diagnostic tools, and iteratively investigate the technical environment rather than relying solely on the information contained in an initial incident description (Jannatul, 2025; Roy et al., 2024). Such capabilities are particularly relevant to failure intelligence because infrastructure incidents often require engineers to combine current alerts with service histories, logs, architectural relationships, troubleshooting guides, and earlier incidents before reaching a credible diagnosis. Recent AIOps literature increasingly categorizes large language models as tools for failure perception, anomaly interpretation, root-cause analysis, incident-report processing, knowledge retrieval, tool-assisted diagnosis, and remediation support within complex operational environments (Zhang et al., 2025). Generative AI-assisted incident management therefore represents a combination of information interpretation, contextual reasoning, knowledge synthesis, and recovery-oriented decision support rather than simple textual generation.

The existing research provides extensive technical evidence on automated log analysis, anomaly detection, AIOps, cloud incident management, causal fault localization, and LLM-supported root-cause analysis, although these domains have frequently been investigated as individual technical problems, algorithms, systems, or operational tasks. Log-analysis studies have largely concentrated on identifying abnormal execution patterns, parsing heterogeneous system events, learning sequential behavior, and measuring anomaly-detection performance under different operational conditions (Du et al., 2017; Guo et al., 2021). Broader evaluations indicate that results can vary according to preprocessing methods, datasets, grouping strategies, environmental noise, model configuration, and the characteristics of the underlying log data (Landauer et al., 2023; Le & Zhang, 2022). AIOps research has organized incident management into multiple stages involving detection, localization, diagnosis, prediction, mitigation, and recovery, while also emphasizing the importance of combining heterogeneous operational data sources (Notaro et al., 2021; Yu et al., 2024). Research focusing directly on large language models has demonstrated their capacity to recommend root causes and mitigation steps, generate diagnostic narratives, use historical production incidents as contextual evidence, and perform tool-assisted

investigations of complex operational failures (Ahmed et al., 2023; Chen et al., 2024). Additional studies have shown that retrieval, contextual examples, and agentic interaction can expand the diagnostic information available to language models during root-cause investigation (Roy et al., 2024; Zhang et al., 2024). Systematic examinations of large language models in software engineering and AIOps further indicate substantial heterogeneity in tasks, datasets, methods, operational objectives, and evaluation criteria across the current evidence base (Hou et al., 2024; Zhang et al., 2025). Within this body of research, comparatively limited quantitative evidence has examined Generative AI-assisted failure intelligence as a multidimensional operational capability whose distinct components can be statistically associated with an integrated outcome encompassing both incident diagnosis and service recovery. The present study therefore examines four explanatory constructs: Generative AI-Assisted Failure Data Interpretation, involving the interpretation of logs, alerts, traces, telemetry, and related failure evidence; Generative AI-Enabled Root Cause Analysis, involving AI-supported identification and explanation of probable incident causes; Context-Aware Incident Knowledge Synthesis, involving integration of historical incidents, technical documentation, runbooks, configuration information, and current operational context; and Generative AI-Assisted Recovery Recommendation, involving the formulation and prioritization of remediation and service-restoration actions. These constructs are quantitatively examined in relation to Incident Diagnosis and Service Recovery Performance through a cross-sectional, case-study-based research design using five-point Likert measurements, descriptive statistics, correlation analysis, and multiple regression modeling.

Background of the Study

Critical digital infrastructure has become fundamental to the functioning of contemporary organizations because cloud computing platforms, telecommunications networks, distributed applications, enterprise information systems, data centers, digital financial services, healthcare systems, and large-scale online platforms increasingly depend on continuously available and interconnected technological resources. As these infrastructures have become more distributed and software-defined, their operational environments have also become more difficult to observe, diagnose, and recover when failures occur. A single service incident may generate thousands of alerts, application logs, system events, network messages, distributed traces, infrastructure metrics, configuration records, and user-reported symptoms across numerous interconnected components. Operations engineers must therefore interpret large volumes of heterogeneous information while determining which symptoms are meaningful, which components are affected, what technical condition initiated the disruption, and which recovery action should be implemented. Traditional monitoring technologies and rule-based incident-management systems have provided important capabilities for detecting failures and generating alerts, yet they frequently require extensive human interpretation before the underlying cause of an incident can be understood. Machine learning-based AIOps technologies have improved anomaly detection, event correlation, predictive monitoring, and automated classification, but complex incidents may still require engineers to combine structured telemetry with unstructured troubleshooting knowledge, historical incidents, service documentation, runbooks, configuration information, and contextual operational experience. Generative artificial intelligence has introduced a different level of analytical capability because it can process natural-language and semi-structured information, summarize technical evidence, recognize relationships across multiple information sources, generate diagnostic explanations, retrieve relevant knowledge, and formulate potential remediation actions. In critical digital infrastructure, these capabilities can be conceptualized as Generative AI-assisted failure intelligence. Such intelligence involves four closely connected operational capabilities: Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, and Generative AI-Assisted Recovery Recommendation. Together, these capabilities address different stages of the incident-management process, beginning with the interpretation of failure signals and progressing through diagnostic reasoning, integration of contextual knowledge, and selection of recovery actions. Understanding how these capabilities relate to Incident Diagnosis and Service Recovery Performance is therefore important for examining whether Generative AI can provide measurable operational value within complex digital-infrastructure environments.

Problem Statement

Critical digital infrastructure operators increasingly face a mismatch between the amount of operational information generated during service incidents and the capacity of human incident-response teams to interpret that information rapidly and accurately. Modern cloud systems, telecommunications platforms, distributed applications, enterprise services, and microservice architectures may produce large volumes of alerts, logs, metrics, traces, error messages, dependency information, and configuration data during a single disruption. Although such information contains evidence that can support diagnosis, it is often fragmented across multiple monitoring platforms and presented without sufficient contextual explanation. As a result, engineers may spend considerable time identifying relevant signals, reconstructing the sequence of events, comparing current symptoms with previous incidents, locating appropriate troubleshooting documentation, determining the probable root cause, and deciding which recovery procedure should be applied. This information-processing burden can increase diagnosis time, delay mitigation, extend service downtime, and reduce the consistency of incident-response decisions. Existing AIOps and machine learning systems have improved automated anomaly detection and event correlation, but many approaches remain focused on individual tasks rather than providing integrated failure intelligence across the complete diagnostic and recovery process. Generative AI offers capabilities for interpreting heterogeneous failure information, generating root-cause explanations, synthesizing technical knowledge from multiple contextual sources, and recommending recovery actions. However, there remains insufficient quantitative evidence demonstrating whether these distinct Generative AI capabilities significantly improve incident diagnosis and service recovery when examined together within critical digital-infrastructure environments. It is also unclear which capability contributes most strongly to performance and whether their combined influence provides substantial explanatory power. The absence of such empirical evidence creates a research problem because organizations may adopt Generative AI-assisted operational tools without a clear quantitative understanding of the specific failure-intelligence capabilities associated with improved diagnosis and recovery outcomes. This study addresses that problem by statistically examining the relationships between Generative AI-assisted failure intelligence and Incident Diagnosis and Service Recovery Performance.

Purpose/Objectives of the Study

The principal objective of this study is to quantitatively examine how Generative AI-assisted failure intelligence contributes to accelerated incident diagnosis and improved service recovery performance within critical digital infrastructure. To achieve this objective, the research conceptualizes Generative AI-assisted failure intelligence as a multidimensional operational capability consisting of four major explanatory constructs. The first objective is to determine the effect of Generative AI-Assisted Failure Data Interpretation on Incident Diagnosis and Service Recovery Performance by examining whether the ability of Generative AI to interpret logs, alerts, traces, telemetry, error messages, and other failure evidence contributes to faster and more effective operational understanding. The second objective is to evaluate the effect of Generative AI-Enabled Root Cause Analysis by assessing whether AI-supported identification, prioritization, and explanation of probable failure causes improves diagnostic performance and facilitates service restoration. The third objective is to investigate the influence of Context-Aware Incident Knowledge Synthesis, particularly the ability of Generative AI systems to combine historical incidents, runbooks, technical documentation, configuration information, service dependencies, and current operational evidence into coherent diagnostic knowledge. The fourth objective is to assess the effect of Generative AI-Assisted Recovery Recommendation on the selection and prioritization of troubleshooting, remediation, escalation, failover, rollback, restart, and restoration actions. A further objective is to determine the collective explanatory power of these four Generative AI-assisted failure-intelligence capabilities in predicting Incident Diagnosis and Service Recovery Performance. The study therefore adopts a quantitative, cross-sectional, case-study-based research design and uses a structured five-point Likert-scale questionnaire to collect perceptual data from professionals involved in critical digital-infrastructure operations. Descriptive statistics will be used to characterize the study variables, Pearson correlation analysis will measure the direction and strength of their relationships, and multiple regression modeling will estimate the individual and combined effects of the Generative AI-assisted failure-intelligence constructs on incident diagnosis and service

recovery.

Research Hypotheses

The research hypotheses have been developed to test the proposed relationships between the four dimensions of Generative AI-assisted failure intelligence and Incident Diagnosis and Service Recovery Performance within critical digital infrastructure. The first hypothesis, H1, proposes that Generative AI-Assisted Failure Data Interpretation has a significant positive effect on Incident Diagnosis and Service Recovery Performance because improved interpretation of alerts, logs, traces, telemetry, and other operational evidence can increase the clarity and accessibility of information available during incident investigation. The second hypothesis, H2, proposes that Generative AI-Enabled Root Cause Analysis has a significant positive effect on Incident Diagnosis and Service Recovery Performance by supporting the identification, prioritization, and explanation of probable technical causes associated with infrastructure failures. The third hypothesis, H3, states that Context-Aware Incident Knowledge Synthesis has a significant positive effect on Incident Diagnosis and Service Recovery Performance because integrating historical incidents, technical documentation, service dependencies, configuration information, runbooks, and current operational evidence can provide a more complete diagnostic context. The fourth hypothesis, H4, proposes that Generative AI-Assisted Recovery Recommendation has a significant positive effect on Incident Diagnosis and Service Recovery Performance because appropriate AI-generated remediation guidance can assist engineers in selecting and prioritizing actions capable of restoring disrupted services. Finally, H5 proposes that Generative AI-assisted failure-intelligence capabilities collectively have a significant positive effect on Incident Diagnosis and Service Recovery Performance. This final hypothesis evaluates the overall explanatory contribution of the complete model rather than examining each capability independently. The hypotheses will be tested quantitatively through correlation and multiple regression analyses, with statistical significance used to determine whether the proposed relationships are empirically supported within the selected critical digital-infrastructure cases.

Significance of the Research

- i. **Significance for Critical Digital Infrastructure Operators:** The research is significant for organizations responsible for maintaining highly available digital services because it provides a structured empirical assessment of how specific Generative AI capabilities relate to incident diagnosis and service recovery. By distinguishing failure-data interpretation, root-cause analysis, knowledge synthesis, and recovery recommendation, the study can help organizations understand which areas of Generative AI-assisted operations are most closely associated with improved incident-management performance.
- ii. **Significance for SRE, DevOps, and Incident-Response Professionals:** The study is significant for Site Reliability Engineers, DevOps engineers, platform engineers, cloud engineers, network engineers, incident managers, and other technical professionals because it focuses directly on the information-processing challenges they encounter during service disruptions. The findings can provide a clearer understanding of how Generative AI may support the interpretation of complex operational evidence, diagnostic reasoning, retrieval of relevant technical knowledge, and formulation of recovery actions.
- iii. **Significance for AIOps and Generative AI System Developers:** The research provides significance for developers of AIOps platforms, incident-management systems, observability tools, and Generative AI-based operational assistants by identifying empirically measurable capabilities that can be incorporated into system design and evaluation. The four-dimensional structure provides a practical basis for distinguishing between simple conversational interfaces and more comprehensive failure-intelligence systems.
- iv. **Significance for Academic Research:** The study contributes to research on AIOps, Generative AI, digital-infrastructure reliability, and intelligent incident management by treating Generative AI-assisted failure intelligence as a multidimensional quantitative construct rather than examining only isolated technical applications. It also provides an empirical model linking four explanatory variables to an integrated performance outcome.
- v. **Significance for Organizational Decision Making:** The research can support managers and technology leaders responsible for AI adoption by providing evidence concerning the relationship between Generative AI-assisted operational capabilities and service reliability outcomes. This evidence can assist organizations in evaluating technology investments, defining operational requirements,

establishing human oversight mechanisms, and determining where Generative AI-supported failure intelligence can be incorporated into existing incident-management processes.

LITERATURE REVIEW

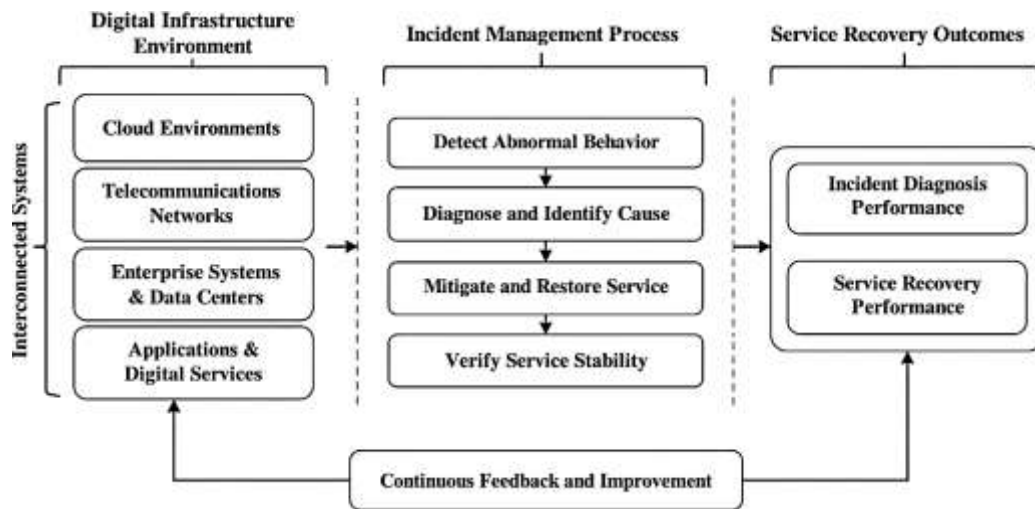
The literature concerning Generative AI-assisted failure intelligence in critical digital infrastructure extends across several interconnected research domains, including digital-infrastructure reliability, distributed-system failure management, automated log analysis, AIOps, root-cause analysis, incident knowledge management, large language models, and intelligent service recovery. Critical digital environments generate extensive operational evidence through application logs, infrastructure metrics, distributed traces, network telemetry, alerts, error messages, configuration information, service dependencies, and historical incident records. The literature has traditionally examined different portions of this information environment through specialized analytical approaches. Earlier automated operations research concentrated substantially on log parsing, anomaly detection, failure prediction, and identification of abnormal execution patterns. The development of AIOps broadened the analytical scope by combining machine learning, operational data, automation, and intelligent decision support across multiple stages of failure management, including detection, localization, diagnosis, mitigation, and recovery. Root-cause analysis subsequently emerged as a particularly important area because complex distributed and microservice architectures can produce symptoms across several dependent components, making the originating failure difficult to identify from isolated alerts. At the same time, organizational incident response depends not only on real-time telemetry but also on historical cases, runbooks, troubleshooting guides, technical documentation, configuration records, and specialist knowledge. Generative AI and large language models provide a new mechanism for processing these heterogeneous information sources because they can interpret technical language, summarize operational evidence, retrieve contextual knowledge, generate diagnostic explanations, and formulate possible recovery actions. The literature review therefore examines Generative AI-assisted failure intelligence as a combination of technological and information-processing capabilities rather than as a single automated tool. Particular attention is given to critical digital-infrastructure failures and service recovery, Generative AI-assisted failure-data interpretation, Generative AI-enabled root-cause analysis, context-aware knowledge synthesis and recovery support, the theoretical explanation of these relationships through Organizational Information Processing Theory, and the conceptual relationships connecting the four Generative AI-assisted failure-intelligence dimensions with Incident Diagnosis and Service Recovery Performance.

Critical Digital Infrastructure and Service Recovery

Critical digital infrastructure encompasses the interconnected computing, communications, storage, platform, and application resources that sustain essential organizational and public services across cloud environments, telecommunications networks, enterprise systems, data centers, and digitally mediated service ecosystems. Its operational importance arises from continuous dependence on availability, reliability, timely data exchange, and coordinated functioning among numerous technical components. Infrastructure failure therefore cannot be treated as an isolated hardware or software problem because interruptions may affect dependent services, users, business processes, and other connected systems. Network resilience research has emphasized that modern communications infrastructure must be capable of resisting disruptions, detecting abnormal conditions, adapting to adverse events, and restoring acceptable service after degradation, making survivability and recovery central properties of dependable digital systems (Debasish, 2021; Sterbenz et al., 2010). The expansion of cloud computing has intensified these requirements because virtualized resources, shared platforms, dynamic workloads, and geographically distributed services create operational environments in which failures may originate from hardware, software, networks, configurations, resource contention, or interactions among service layers. Cloud fault tolerance research has consequently treated reliability as a system level capability that requires recognition of different fault classes together with appropriate preventive, reactive, and recovery mechanisms (Hasan & Goraya, 2018; Abdur & Iftekhar, 2021). Within critical digital infrastructure, operational resilience therefore depends on more than preventing every possible failure. It also requires sufficient observability to recognize service degradation, technical processes for isolating affected components, mechanisms for preserving essential functions, and recovery procedures that restore service without introducing secondary disruption. This broader

perspective is particularly relevant to incident management because the practical severity of a failure is determined not only by its initiating fault but also by how rapidly its effects are understood, contained, and reversed across interconnected digital services. It also shapes the capacity of operators to maintain continuity when interconnected services experience simultaneous or rapidly cascading operational disturbance events.

Figure 2: Critical Digital Infrastructure Incident Management and Service Recovery Framework



Operational failures in critical digital infrastructure are difficult to manage because systems are built from distributed services that change frequently and depend on automated orchestration, virtualization, software defined networking, external interfaces, and dynamically allocated computing resources. These architectural characteristics improve scalability and flexibility, but they also increase the number of possible failure points and make the relationship between symptoms and underlying causes less transparent. A visible service slowdown, for example, may originate from resource exhaustion, a failed dependency, an incorrect configuration, a network delay, a software defect, or a chain of abnormal interactions across multiple components. Cloud native research has therefore emphasized continuous management, health monitoring, automated reactions, component replication, restarting, and adaptive resource control as necessary characteristics of resilient applications operating on infrastructure where transient failures must be expected rather than treated as exceptional events (Debasish, 2022; Carughi et al., 2017). Fault tolerance literature similarly distinguishes proactive and reactive approaches, showing that reliable cloud operation requires both mechanisms that anticipate or avoid failures and mechanisms that limit damage and restore functionality after failures occur (Hasan & Adnan, 2022; Kumari & Kaur, 2021). Service recovery is consequently a coordinated technical process that begins with recognizing abnormal behavior and continues through fault isolation, diagnosis, mitigation, restoration, and verification that the affected service has returned to an acceptable state. The challenge becomes greater when incidents cross administrative or architectural boundaries because individual monitoring tools may expose only fragments of the overall failure. Engineers may then need to correlate service metrics, logs, traces, dependency relationships, configuration changes, and historical operational knowledge before selecting an appropriate recovery action. Delays at any stage can prolong disruption, increase uncertainty, and create additional operational risk. For this reason, incident diagnosis and recovery performance are closely connected dimensions of infrastructure resilience, since rapid restoration depends on accurate understanding before corrective action is executed.

Service recovery within critical digital infrastructure has an organizational dimension because technical restoration depends on how effectively people, tools, data, procedures, and automated systems coordinate during an incident. Large outages commonly require operators to interpret multiple streams of evidence while communicating across engineering teams, prioritizing affected services, evaluating

competing root cause explanations, and deciding whether to restart components, roll back changes, redirect traffic, fail over workloads, isolate dependencies, or apply other remediation procedures. Recent analysis of major information and communication technology failures has identified recurring weaknesses involving automation governance, configuration management, centralized dependencies, delayed incident response, and inadequate control of failure propagation, while also highlighting recovery practices such as rollback mechanisms, configuration based controls, orchestration, and structured resilience engineering ([Adel et al., 2025](#); [Mahbubul et al., 2022](#)). These conditions demonstrate why service recovery cannot be reduced to the execution of a single technical command. Recovery effectiveness depends on the quality of diagnostic information available before action, the accuracy with which the initiating condition is distinguished from downstream symptoms, and the ability to select measures that restore service without amplifying the incident. In interconnected infrastructures, restoration may also require staged actions because recovering one component can alter workload distribution, dependency behavior, or system state elsewhere in the environment. Incident diagnosis therefore functions as the informational foundation of recovery, while recovery provides the operational test of whether diagnostic understanding has been sufficiently accurate and actionable. This relationship is central to research on failure intelligence because digital infrastructure produces more operational evidence than human teams can interpret under time pressure. A useful failure management capability must consequently connect detection with explanation and explanation with action. Examining incident diagnosis and service recovery together provides a complete representation of operational performance by capturing how effectively infrastructure teams convert fragmented failure evidence into justified decisions and restore disrupted digital services.

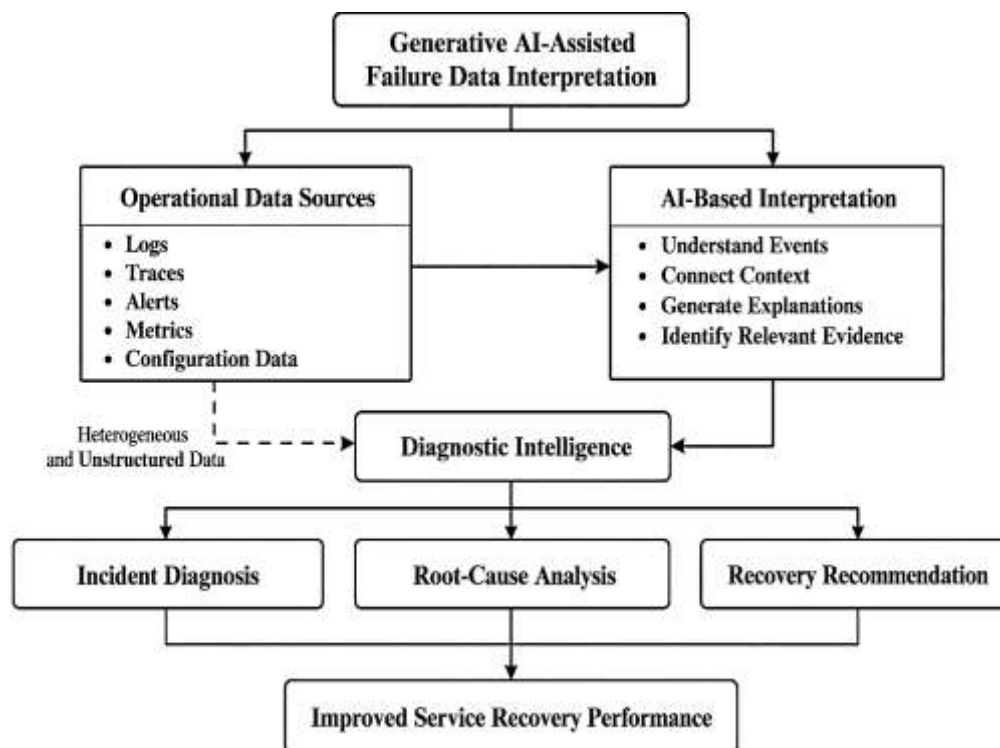
Generative AI-Assisted Failure Data Interpretation

Generative AI-assisted failure data interpretation concerns the use of advanced language and representation models to transform raw operational evidence into information that can be understood and acted upon during infrastructure incidents. Critical digital environments continuously generate system logs, application events, distributed traces, alerts, performance metrics, network telemetry, configuration messages, and error records. Each source captures only part of the operational state, and much of the available evidence is semi-structured, repetitive, technical, and distributed across different monitoring platforms. Conventional incident response therefore requires engineers to search large datasets, identify abnormal patterns, compare events across time, interpret error semantics, and connect symptoms appearing in different components. Log analysis research has shown that the scale of this information can exceed the practical capacity of manual inspection, especially when systems produce high-volume event streams during abnormal behavior. Distributed log-analysis architectures have consequently been developed to support parsing, feature extraction, and machine-learning-based identification of abnormal events across large datasets, demonstrating that operational logs can be converted from passive records into active diagnostic resources ([Astekin et al., 2019](#); [Ashfaq & Mohammad, 2022](#)). Failure data interpretation, however, extends beyond determining whether an event is statistically unusual. Incident responders also need to understand what an event means, which service produced it, how it relates to surrounding events, and whether it represents a cause, a consequence, or an unrelated condition. Distributed tracing provides complementary information by recording requests and service interactions across complex architectures, allowing operators to observe workflow paths, latency changes, dependency relationships, and abnormal service behavior. Research on automated trace analysis has shown that tracing data can reveal service metrics, dependency graphs, workflows, and contextual indicators of anomalous behavior while also illustrating the analytical burden created by high-volume, application-specific traces ([Bento et al., 2021](#); [Sheak & Risha, 2022](#)). These characteristics make failure-data interpretation an essential bridge between raw observability and meaningful diagnosis in digital infrastructure.

Traditional machine-learning approaches to failure interpretation frequently depend on preprocessing pipelines that transform raw operational messages into structured templates before classification or anomaly detection. Such pipelines are useful for reducing variation, but they can also remove contextual information contained in identifiers, parameters, message wording, and uncommon event sequences. This limitation is important in critical digital infrastructure because previously unseen failures may appear through novel combinations of familiar messages or through semantically

meaningful changes that do not fit established templates. Parser-free language-based approaches have therefore become important because they attempt to preserve the semantic content of raw logs while modeling relationships among messages. NeuralLog, for example, represents raw log messages as semantic vectors and uses Transformer-based sequence modeling to identify anomalies without relying on conventional log parsing, showing that contextual language representations retain information otherwise lost through preprocessing (Le & Zhang, 2021; Rashedul & Kaium, 2022). Generative AI extends this semantic perspective by allowing operational messages to be processed in relation to natural-language instructions, documentation, historical cases, and context. In a failure-intelligence setting, a Generative AI system can be prompted to summarize groups of alerts, explain unfamiliar error messages, identify recurring symptoms, compare current telemetry with previous incidents, distinguish relevant evidence from informational noise, and organize observations into a coherent incident narrative. Research combining large language models with BERT-based anomaly detection has demonstrated that ChatGPT can support log parsing while contextual language models identify anomalous log sequences, illustrating how generative and representation-based techniques can complement one another in operational analysis (Chowdhury & Tonay, 2022; Zhou et al., 2024). This capability is relevant when logs differ across vendors, platforms, software versions, and service components. Instead of requiring responders to understand every syntax independently, Generative AI-assisted interpretation can translate heterogeneous machine-oriented evidence into normalized descriptions that preserve technical meaning and connect observations across sources, providing a foundation for subsequent root-cause analysis.

Figure 3: Generative AI-Assisted Failure Data Interpretation Framework for Incident Diagnosis and Service Recovery Performance



The value of Generative AI-assisted failure data interpretation depends on whether the resulting explanations are accurate and transparent for operational use. An incident-management environment differs from a general conversational setting because an incorrect interpretation can direct engineers toward irrelevant components, obscure the failure sequence, or encourage inappropriate remediation. Effective failure intelligence must therefore preserve evidence provenance, distinguish observed facts from generated reasoning, represent uncertainty, and allow engineers to trace an explanation back to logs, alerts, traces, metrics, or source records. This becomes important as Generative AI systems move

from summarization toward explanation generation. Recent large-language-model research on log anomaly detection has combined anomaly discrimination with explanation generation, using label-cause learning and knowledge-base mechanisms to improve detection and interpretability in changing logging environments (Hossan, 2022; Zhang et al., 2025). Such approaches align with the present study because failure-data interpretation is conceptualized not merely as automated anomaly classification but as the production of context-sensitive information supporting understanding of an incident. Within critical digital infrastructure, this capability may involve consolidating alerts into a single failure description, translating low-level telemetry into service-level meaning, identifying temporal relationships among events, surfacing unusual dependency behavior, and highlighting evidence that deserves investigation. The effectiveness of this process is influenced by observability, the model's knowledge of infrastructure terminology, access to relevant context, consistency of log formats, and controls for hallucinated or unsupported explanations. Generative AI-assisted failure data interpretation can be understood as an information transformation capability that converts heterogeneous operational evidence into structured diagnostic intelligence while retaining technical context for verification. In this research, the capability represents the first explanatory variable because root-cause reasoning, incident-knowledge synthesis, and recovery recommendation depend on the quality of evidence initially interpreted. Measuring respondents' perceptions provides a quantitative basis for testing whether stronger Generative AI-supported interpretation is associated with higher Incident Diagnosis and Service Recovery Performance.

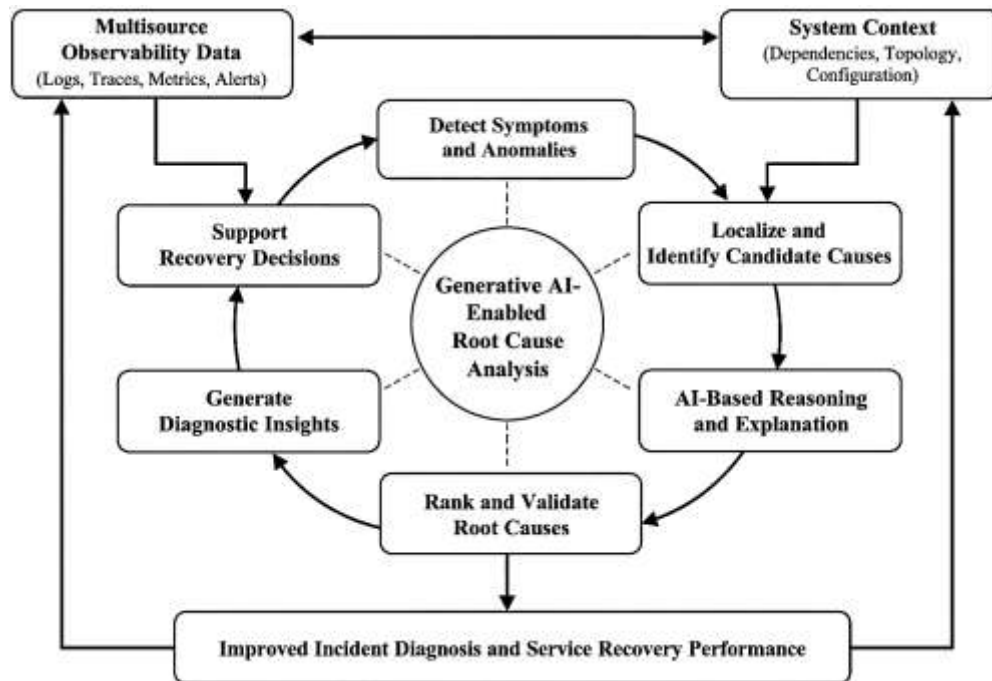
Generative AI-Enabled Root Cause Analysis and Failure Diagnosis

Root cause analysis is a critical stage of incident management because identifying that a system is behaving abnormally does not automatically reveal the component, resource, configuration, dependency, or software condition responsible for the disruption. In critical digital infrastructure, this distinction is particularly important because a visible symptom may appear far from the original fault. Increased latency in one service can be caused by resource contention in another component, a downstream database problem, network congestion, deployment errors, or cascading effects across service dependencies. Conventional root cause analysis often relies on experienced engineers who manually compare monitoring dashboards, inspect logs, trace requests, reconstruct service dependencies, and test competing technical explanations. Such procedures can become slow and inconsistent when incidents involve hundreds of services and rapidly changing topologies. Automated root cause localization has therefore become an important research area for cloud and microservice operations. MicroRCA demonstrated how application-level symptoms, resource utilization, and service dependency information can be represented through an attributed graph so that anomaly propagation can be analyzed and probable causes ranked automatically (Kaniz, 2022; Wu et al., 2020). This approach is important for Generative AI-assisted failure intelligence because it establishes a structured diagnostic foundation from which higher-level reasoning can be developed. Generative AI-enabled root cause analysis can extend traditional localization by translating ranked anomalies and dependency evidence into contextual explanations, comparing multiple candidate causes, and presenting the reasoning in language that incident responders can evaluate. Instead of treating root cause localization as a final classification output, a generative system can connect observed symptoms with probable mechanisms and supporting evidence. This creates a diagnostic process in which algorithmic localization, contextual interpretation, and human validation can operate together during service incidents. This diagnostic requirement is intensified during major outages, when responders must distinguish initiating faults from secondary symptoms while maintaining service continuity under time pressure.

The effectiveness of root cause analysis also depends on the breadth and integration of observability data used during troubleshooting. Digital infrastructure failures are rarely represented completely by a single monitoring source because metrics capture quantitative behavior, traces describe service interactions, and logs contain event-specific semantic information. When these sources are analyzed separately, an important relationship between abnormal behavior and its underlying cause may remain hidden. End-to-end troubleshooting research has therefore increasingly emphasized multi-source diagnosis. Eadro integrated traces, logs, and key performance indicators while jointly modeling anomaly detection and root cause localization, showing that diagnostic accuracy can benefit from

combining heterogeneous operational evidence rather than relying on a single data modality (Lee et al., 2023; Nishat & Kaniz, 2022). Fine-grained causal approaches have also attempted to identify not only the faulty service but the specific metric or resource condition associated with the problem. CausalRCA used causal structure learning to construct weighted graphs among monitoring variables and then ranked candidate causes through root cause inference, illustrating how causal relationships can support more precise diagnosis and recovery decisions (Shaiful et al., 2022; Xin et al., 2023). These developments are relevant to Generative AI-enabled root cause analysis because large language models can function as an interpretive layer above observability systems. A Generative AI system can receive summaries of anomalous metrics, trace paths, log evidence, topology information, and causal rankings, then organize these signals into competing diagnostic hypotheses. It can also distinguish direct observations from inferred relationships, compare current evidence with known failure patterns, and formulate a structured explanation of why one candidate is more plausible than another. Such functionality transforms root cause analysis from isolated anomaly ranking into an evidence-centered reasoning process. For critical digital infrastructure, this is valuable because engineers require not only a predicted faulty component but also contextual justification to decide whether a proposed recovery action is technically appropriate.

Figure 4: Generative AI-Enabled Root Cause Analysis Framework for Incident Diagnosis and Service Recovery Performance



Generative AI-enabled failure diagnosis becomes more significant as infrastructures grow dynamic and root causes must be identified at increasingly fine operational granularity. In containerized and microservice environments, one logical service may consist of multiple instances distributed across hosts, clusters, zones, or regions. A service-level diagnosis may therefore be insufficient when only a particular instance, resource, or execution context is responsible for the observed degradation. MicroIRC addressed this challenge through instance-level localization using graph neural networks, time-series metric features, topology information, and personalized random walks, demonstrating the importance of diagnostic methods that remain effective under topology changes and previously unseen anomaly types (Mohammad, 2023; Zhu et al., 2024). Generative AI can complement this precision by converting fine-grained technical outputs into explanations that relate symptoms, dependencies, resource conditions, and probable failure mechanisms. More directly, recent research has begun to frame root cause analysis itself as a generative task. RCEGen used large language models to generate

natural-language root cause explanations from software failure reports, illustrating a shift from assigning predefined root cause categories toward producing explanatory descriptions of underlying faults (Debasish, 2023; Mollik et al., 2025). This shift in practice closely aligns with the present research because Generative AI-Enabled Root Cause Analysis is conceptualized as more than automated classification. It includes the capability to identify plausible causes, synthesize supporting evidence, explain technical relationships, prioritize diagnostic hypotheses, and assist human operators in understanding why a particular cause should receive attention. Within critical digital infrastructure, however, generated explanations must remain grounded in observable evidence because hallucinated or unsupported causal claims could misdirect recovery activities. Effective systems therefore require mechanisms for evidence retrieval, uncertainty representation, source attribution, and human validation. Measuring this capability as a distinct construct makes it possible to test whether stronger Generative AI-supported root cause reasoning is significantly associated with improved Incident Diagnosis and Service Recovery Performance.

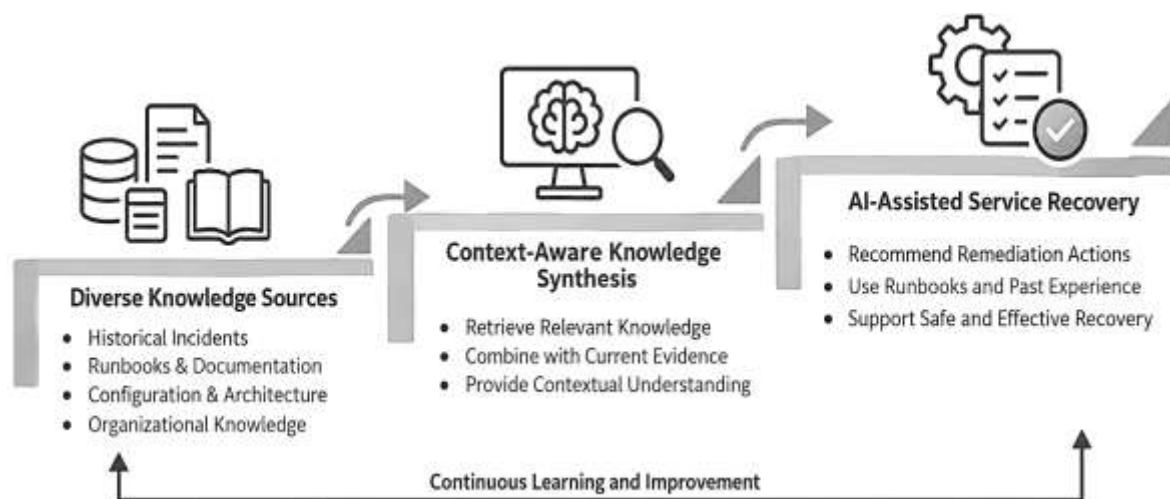
Context-Aware Incident Knowledge Synthesis and AI-Assisted Service Recovery

Context-aware incident knowledge synthesis refers to the process of combining current operational evidence with previously accumulated technical knowledge so that incident responders can understand an abnormal condition within the specific architecture, history, policies, and operating procedures of an organization. Critical digital infrastructure rarely stores all relevant troubleshooting knowledge in one location. Useful information may be distributed across historical incident tickets, post-incident reports, runbooks, service manuals, configuration repositories, architecture documents, change records, knowledge bases, standard operating procedures, and informal engineering notes. During a high-severity incident, responders must retrieve information from these sources while simultaneously interpreting live alerts, logs, traces, metrics, and service dependencies. Generative AI can support this task when it is connected to organization-specific knowledge through retrieval, semantic search, vector representations, or other grounding mechanisms. Retrieval-Augmented Generation is particularly relevant because it allows a language model to retrieve external documents associated with a query before producing an answer, reducing dependence on general parametric knowledge and increasing the availability of enterprise-specific evidence. RAG4ITOps demonstrated this principle in IT operations and maintenance by combining fine-tuned retrieval and generation components with enterprise-exclusive cloud-computing corpora, showing that domain-specific question answering can be improved when models are explicitly adapted to operational knowledge rather than relying only on general language-model capabilities (Sheak & Tahmedur, 2023; Zhang et al., 2024). Contextual synthesis can also extend beyond document retrieval to the integration of structured knowledge relationships. Research on large-language-model chatbots for maintenance planning has shown that Generative AI and knowledge graphs can jointly exploit maintenance databases, reports, machine documentation, and other technical information while supporting technicians during operational decision making (Kohl et al., 2024; Kaium, 2023). These developments establish context-aware knowledge synthesis as an important failure-intelligence capability because incident diagnosis often depends on linking present symptoms with earlier experience, component knowledge, established procedures, and service-specific constraints. This capability can also reduce the cognitive burden created by fragmented repositories during time-sensitive operational investigation and recovery.

The usefulness of context-aware synthesis becomes clearer when incident responders must reconstruct what happened before deciding how a service should be restored. Infrastructure failures evolve over time, and the sequence in which alerts, system changes, user symptoms, process events, and technical observations occur can materially affect diagnosis. A current incident may resemble a previous outage while differing in one configuration change, dependency failure, or operational condition, so effective Generative AI assistance requires retrieval that preserves both context and chronology. Retrieval-Augmented Generation has been applied to cyber incident timeline analysis to combine large language models with incident artifacts and external knowledge, enabling events and associated metadata to be examined as a connected sequence rather than as isolated records (Loumachi et al., 2025; Pervaz, 2023). This type of synthesis is relevant to critical digital infrastructure because service restoration decisions frequently depend on identifying the order of failure propagation, distinguishing initiating events from

downstream consequences, and understanding which interventions were previously successful under similar conditions. Generative AI can further support responders by converting retrieved evidence into structured explanations, recommended investigative steps, and operational guidance. A Security Event Response Copilot developed for Security Operations Center environments integrated RAG-based security-event data extraction with LLM-based incident-response guidance, demonstrating how retrieved knowledge and real-time evidence can be combined to assist analysts in mitigation activities (Ismail et al., 2025; Chowdhury, 2023). The same logic can be transferred to broader infrastructure incident management in which cloud engineers, SRE professionals, DevOps teams, and network operators need rapid access to service-specific recovery knowledge. Context-aware synthesis therefore involves more than searching for a matching document. It requires selecting relevant evidence, reconciling information from multiple sources, preserving relationships among events, and presenting technically coherent knowledge that can be evaluated by human responders. The quality of this process directly influences whether Generative AI recommendations are grounded in the actual incident context or generated from incomplete and potentially misleading assumptions.

Figure 5: Context-Aware Incident Knowledge Synthesis and AI-Assisted Service Recovery Framework



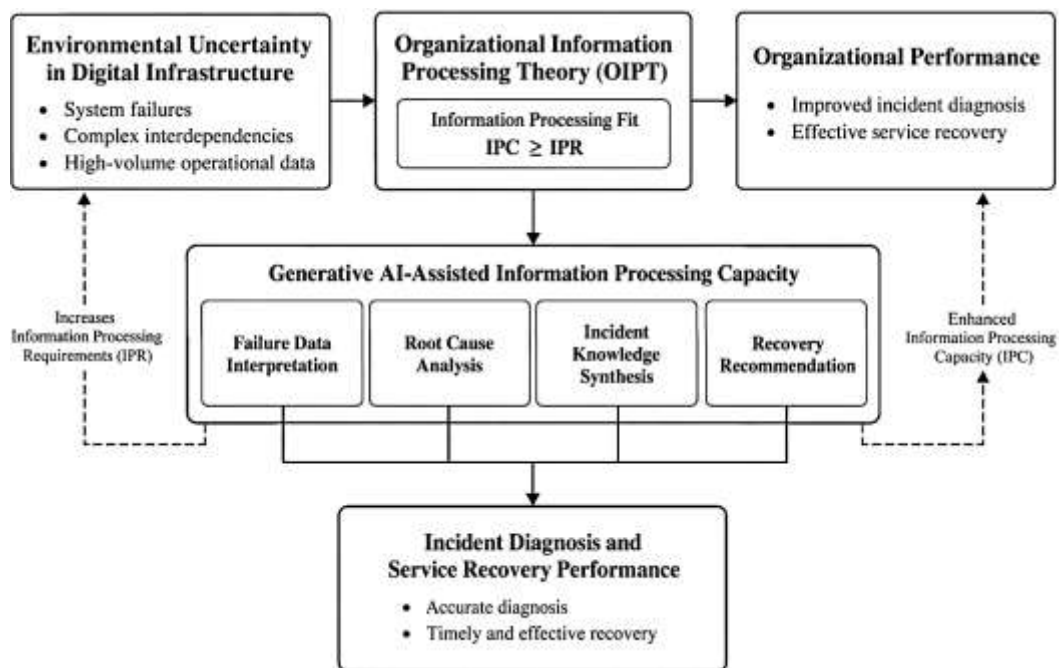
AI-assisted service recovery represents the action-oriented stage of failure intelligence in which interpreted evidence, root cause hypotheses, and synthesized contextual knowledge are translated into technically appropriate remediation choices. Recovery actions within critical digital infrastructure may include restarting services, rolling back a deployment, modifying a configuration, isolating a failed component, redirecting traffic, scaling resources, failing over to redundant infrastructure, revoking compromised access, or escalating an unresolved condition to specialized personnel. The selection of an action must account for the diagnosed cause, current service state, operational dependencies, risk of secondary disruption, organizational policies, and the reversibility of the proposed intervention. Generative AI can assist by retrieving relevant runbooks, comparing current conditions with previous incidents, organizing candidate actions, and converting documented procedures into stepwise recommendations. More advanced systems can also structure the output in machine-readable forms suitable for orchestration platforms, creating a connection between language-based reasoning and controlled automation. Research on automated cybersecurity response playbooks has demonstrated that fine-tuned large language models can transform structured incident descriptions into standards-aligned mitigation procedures and CACAO-compliant playbooks, supporting the generation of actionable response sequences that can be integrated with SIEM and SOAR environments (Badrul & Mominul, 2023; Murad, 2026; Paduraru et al., 2025). This capability is closely related to the present study's construct of Generative AI-Assisted Recovery Recommendation because the operational value of failure intelligence is realized only when diagnostic understanding can be converted into a justified

response. At the same time, recovery recommendations require strong safeguards because an incorrect action can increase downtime or propagate failure. Human validation, source visibility, confidence indicators, access controls, execution boundaries, and rollback mechanisms therefore remain essential when Generative AI participates in high-impact recovery decisions. Context-Aware Incident Knowledge Synthesis and Generative AI-Assisted Recovery Recommendation are consequently related but distinct capabilities: the first organizes and grounds the knowledge needed to understand the incident, while the second transforms that grounded understanding into prioritized actions for restoring service.

Organizational Information Processing Theory

Organizational Information Processing Theory provides an appropriate theoretical foundation for explaining how Generative AI-assisted failure intelligence can improve incident diagnosis and service recovery in critical digital infrastructure because the central problem addressed by the theory is the relationship between environmental uncertainty, information-processing requirements, organizational information-processing capacity, and performance. Critical digital infrastructure represents an information-intensive operational environment in which unexpected failures create substantial uncertainty regarding what has happened, where the failure originated, which components are affected, how the abnormal condition is propagating, and what corrective action should be selected. During a major incident, engineers may simultaneously receive logs, metrics, traces, alerts, configuration records, service-dependency information, historical incident reports, runbooks, and user-reported symptoms. The operational challenge is therefore not merely the availability of information but the capacity to transform heterogeneous information into sufficiently accurate knowledge for timely action. OIPT proposes that organizations achieve stronger performance when their information-processing capabilities adequately match the amount and complexity of information that must be processed. Empirical research grounded in OIPT has demonstrated that technology-supported information integration can strengthen comprehensive planning by allowing organizations to use information obtained from multiple sources more effectively, establishing an important connection among information integration, processing capability, and operational performance (Rakib & Towhidul, 2023; Nishat, 2026; Srinivasan & Swink, 2015).

Figure 6: Organizational Information Processing Theory Framework for Generative AI-Assisted Failure Intelligence



The same theoretical principle can be applied to infrastructure incident management. Generative AI-Assisted Failure Data Interpretation increases processing capacity by transforming technical telemetry into understandable information, while Generative AI-Enabled Root Cause Analysis reduces diagnostic uncertainty by organizing evidence into plausible causal explanations. OIPT-based analytics research has similarly demonstrated that visibility and analytical capabilities become more valuable when organizations can rapidly convert information into operational responses, emphasizing that information availability alone is insufficient without a corresponding capability to interpret and act upon that information (Nishat, 2023; Rony & Md, 2026; Srinivasan & Swink, 2018). For the present research, the central OIPT principle can therefore be represented as an information-processing fit relationship:

$$IPF = IPC - IPR$$

where IPF represents Information Processing Fit, IPC represents the available Information Processing Capacity, and IPR represents the Information Processing Requirement created by the incident. A positive or sufficiently balanced value indicates that available processing capacity is capable of addressing the informational demands generated by an operational failure.

The relevance of OIPT becomes stronger when incident diagnosis is viewed as a continuous process of reducing uncertainty through the acquisition, interpretation, integration, and application of information. In critical digital infrastructure, uncertainty increases when failures affect several interconnected services, when observability evidence is inconsistent, when infrastructure configurations have recently changed, or when engineers encounter an unfamiliar failure pattern. Generative AI can increase information-processing capacity because it can simultaneously organize information from different sources and convert fragmented technical evidence into coherent diagnostic knowledge. Within the theoretical structure of this study, Generative AI-Assisted Failure Data Interpretation represents the initial information-processing function because it converts raw logs, alerts, metrics, traces, and telemetry into more accessible operational representations. Generative AI-Enabled Root Cause Analysis represents a deeper analytical function through which observed information is evaluated to determine probable causal relationships. Context-Aware Incident Knowledge Synthesis expands processing capacity by integrating current evidence with historical incidents, runbooks, configuration records, technical documentation, and organizational knowledge. Generative AI-Assisted Recovery Recommendation then converts processed information into possible operational responses. Research applying OIPT to organizational resilience has demonstrated that information access and digital technologies can strengthen the capacity of organizations to process environmental uncertainty and respond to disruptions, particularly when information can be transformed into learning and adaptive action (Ashrafuzzaman, 2024; Sadia, 2026; Xie et al., 2022). This principle corresponds closely to incident response because resilience in critical digital infrastructure depends partly on the ability to understand unexpected conditions and restore service after disruption. Digital information processing can also produce different risk outcomes depending on how technological capabilities interact with organizational structures and controls, indicating that the acquisition of more information or greater digitalization does not automatically produce superior operational performance (Debasish, 2024; Khatun, 2026; Yin et al., 2024). Consequently, Generative AI-assisted failure intelligence should not be treated simply as the presence of an AI tool. Its theoretical value depends on whether it increases the effective processing capacity available to responders, reduces uncertainty, connects relevant information, and supports appropriately grounded decisions. Within OIPT, the relationship can be represented as $IPC \geq IPR$, where incident performance should improve when Generative AI-supported information-processing capacity is sufficient to meet or exceed the informational requirements produced by the infrastructure failure.

The application of Organizational Information Processing Theory to this research consequently provides a unified theoretical explanation for all four independent variables and their relationship with Incident Diagnosis and Service Recovery Performance. Generative AI-Assisted Failure Data Interpretation increases the organization's capacity to recognize and interpret relevant operational signals; Generative AI-Enabled Root Cause Analysis strengthens the transformation of evidence into diagnostic explanations; Context-Aware Incident Knowledge Synthesis increases the ability to integrate distributed information sources; and Generative AI-Assisted Recovery Recommendation

supports the transformation of processed information into prioritized remedial decisions. Recent empirical work explicitly applying OIPT to artificial intelligence has shown that AI usage can strengthen resilience through enhanced information-processing capability, efficiency, collaboration, and digital information technology capacity, supporting the theoretical proposition that AI can function as an organizational mechanism for processing uncertainty and supporting coordinated responses to disruption (Rahman, 2024; Pan et al., 2025; Shamsul, 2026). In the present study, the theory therefore predicts that stronger Generative AI-assisted information-processing capabilities should correspond with stronger Incident Diagnosis and Service Recovery Performance because responders are better equipped to transform complex failure evidence into timely diagnostic and recovery decisions. The primary empirical representation of this theoretical relationship, and the formula that will be applied consistently throughout the quantitative analysis of the study, is the multiple linear regression model:

$$IDSRP_i = \beta_0 + \beta_1 GAFDI_i + \beta_2 GAERCA_i + \beta_3 CAIKS_i + \beta_4 GAARR_i + \varepsilon_i$$

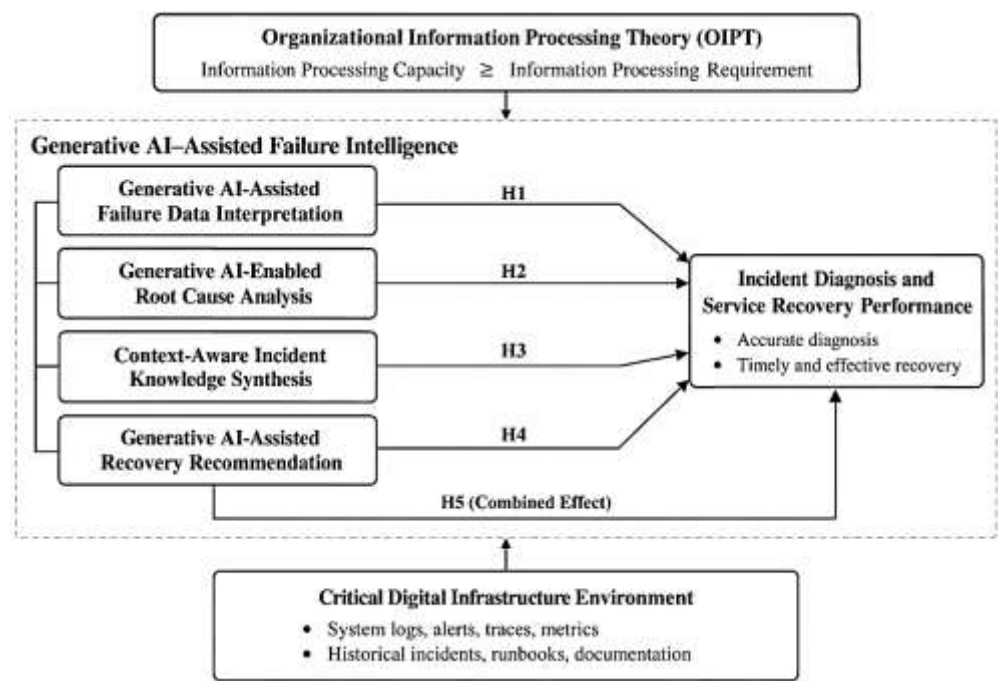
where IDSRP_i represents Incident Diagnosis and Service Recovery Performance for respondent *i*; β_0 represents the regression constant; β_1 , β_2 , β_3 , and β_4 represent the estimated effects of Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, and Generative AI-Assisted Recovery Recommendation respectively; and ε_i represents the unexplained error term. This specification directly connects the theoretical logic of information-processing capacity with the empirical hypotheses of the research. Positive and statistically significant coefficients will indicate that stronger Generative AI-assisted information-processing capabilities are associated with stronger incident diagnosis and service recovery outcomes, while the model R^2 will indicate the proportion of variation in IDSRP collectively explained by the four dimensions of Generative AI-assisted failure intelligence.

Conceptual Framework Linking Generative AI-Assisted Failure Intelligence

The conceptual framework of this study explains how four distinct Generative AI-assisted failure-intelligence capabilities are expected to influence Incident Diagnosis and Service Recovery Performance within critical digital infrastructure. The framework begins with Generative AI-Assisted Failure Data Interpretation because reliable incident management depends on transforming raw technical evidence into information that engineers can understand and evaluate. During operational failures, logs, alerts, traces, telemetry, resource metrics, event messages, and service-state information may be distributed across multiple platforms, requiring considerable expertise to identify the observations that are most relevant to diagnosis. Large language models can assist this stage by generating queries, summarizing technical evidence, and helping responders retrieve information required for further investigation. Xpert demonstrated this capability in a large-scale cloud incident-management environment by using historical incident information and large language models to generate customized telemetry queries for new incidents, reducing the difficulty associated with manually constructing domain-specific queries during troubleshooting (Jiang et al., 2024; Kaium, 2024; Tonay, 2026). The conceptual framework therefore proposes that stronger Generative AI-Assisted Failure Data Interpretation should increase the speed and quality with which operational evidence becomes usable diagnostic information. The second construct, Generative AI-Enabled Root Cause Analysis, represents the progression from interpreting evidence to identifying and explaining the underlying cause of an incident. Generative models can evaluate symptoms, dependencies, historical patterns, and technical observations while generating possible causal explanations. Research involving collaboration between large language models and smaller classifiers has demonstrated that LLM-supported analysis can contribute to fault classification and root cause identification even when only limited labeled examples are available, which is particularly relevant to rare or previously unseen cloud-native failures (Han et al., 2024; Shakhawat & Md, 2024). Accordingly, the conceptual framework assumes that improved failure-data interpretation establishes the informational foundation for root-cause reasoning, while stronger root-cause analysis enables responders to distinguish initiating faults from secondary symptoms and select more appropriate recovery pathways. These relationships form the first two explanatory paths connecting Generative AI-assisted information processing with Incident Diagnosis and Service Recovery Performance.

The third explanatory construct, Context-Aware Incident Knowledge Synthesis, represents the capability of Generative AI to integrate current operational evidence with previously accumulated organizational and technical knowledge. Critical digital infrastructure incidents are rarely diagnosed solely through real-time monitoring because responders commonly depend on earlier incidents, historical outage records, technical documentation, configuration knowledge, service relationships, troubleshooting notes, and the operational experience embedded in organizational repositories. Generative AI can synthesize these information sources by retrieving relevant material and transforming it into a coherent description of the current incident. Empirical research on cloud outages has shown that large language models can help aggregate related incidents, assess outage impact, and generate human-readable summaries that improve the understanding of complex service disruptions (Jin et al., 2023; Kanti, 2024). This capability supports the conceptual proposition that context-aware knowledge synthesis should positively influence Incident Diagnosis and Service Recovery Performance because engineers can evaluate failures using broader evidence than the current alert stream alone. An additional requirement is the ability to judge the reliability of generated diagnostic information. Large language models may produce plausible explanations with varying levels of certainty, so confidence estimation becomes important when generated reasoning influences operational decisions. Research on LM-PACE has demonstrated that calibrated confidence estimation can be incorporated into LLM-assisted root-causing of cloud incidents, providing a mechanism for distinguishing stronger diagnostic predictions from explanations requiring additional investigation (Nishat & Jahanara, 2024; Zhang et al., 2024). In the conceptual model, Context-Aware Incident Knowledge Synthesis therefore includes not only retrieving and combining knowledge but also presenting relevant evidence in ways that support verification, comparison, and informed judgment. These mechanisms connect directly with Organizational Information Processing Theory because context integration increases the amount of usable information available to incident responders while reducing uncertainty surrounding unfamiliar or complex failures. When live observability data, historical experience, and organizational knowledge are synthesized effectively, responders should be better positioned to determine what happened, understand why it occurred, assess the credibility of competing explanations, and identify the operational conditions that must be addressed before service restoration can proceed.

Figure 7: Conceptual Framework Linking Generative AI-Assisted Failure Intelligence to Incident Diagnosis and Service Recovery Performance



The fourth construct, Generative AI-Assisted Recovery Recommendation, represents the action-oriented component of the conceptual framework and links diagnostic intelligence with service restoration. After a probable root cause has been established, incident responders must determine which remediation strategy is appropriate for the affected infrastructure. Possible actions may include restarting services, rolling back software changes, modifying configurations, redirecting traffic, scaling computing resources, replacing faulty components, isolating dependencies, or escalating the incident to specialized personnel. Generative AI can support this stage by comparing the diagnosed problem with historical incidents and documented corrective actions, then generating prioritized recommendations that can be evaluated before implementation. Evidence from legacy banking environments has shown that Generative AI agents combining historical incident information, change data, and structured root-cause reasoning can identify recurring failure mechanisms that conventional resolution practices may overlook, illustrating the value of connecting historical knowledge with deeper remediation-oriented analysis (Jin et al., 2025; Palash Chandra, 2024). Within the present conceptual framework, Generative AI-Assisted Recovery Recommendation is therefore expected to have a positive relationship with Incident Diagnosis and Service Recovery Performance because accurate recommendations can reduce the time between understanding an incident and initiating an appropriate response. The complete conceptual relationship can be expressed as:

$$IDSRP = f(GAFDI, GAERCA, CAIKS, GAARR)$$

and operationalized through the multiple regression model:

$$IDSRP_i = \beta_0 + \beta_1 GAFDI_i + \beta_2 GAERCA_i + \beta_3 CAIKS_i + \beta_4 GAARR_i + \varepsilon_i$$

where IDSRP_i represents Incident Diagnosis and Service Recovery Performance, GAFDI_i represents Generative AI-Assisted Failure Data Interpretation, GAERCA_i represents Generative AI-Enabled Root Cause Analysis, CAIKS_i represents Context-Aware Incident Knowledge Synthesis, and GAARR_i represents Generative AI-Assisted Recovery Recommendation. The parameters β_1 through β_4 estimate the independent contribution of each capability, while ε_i represents variation not explained by the four predictors. The framework therefore specifies four direct positive relationships and one collective relationship, providing a clear basis for testing H1 through H5 using correlation and multiple regression analysis.

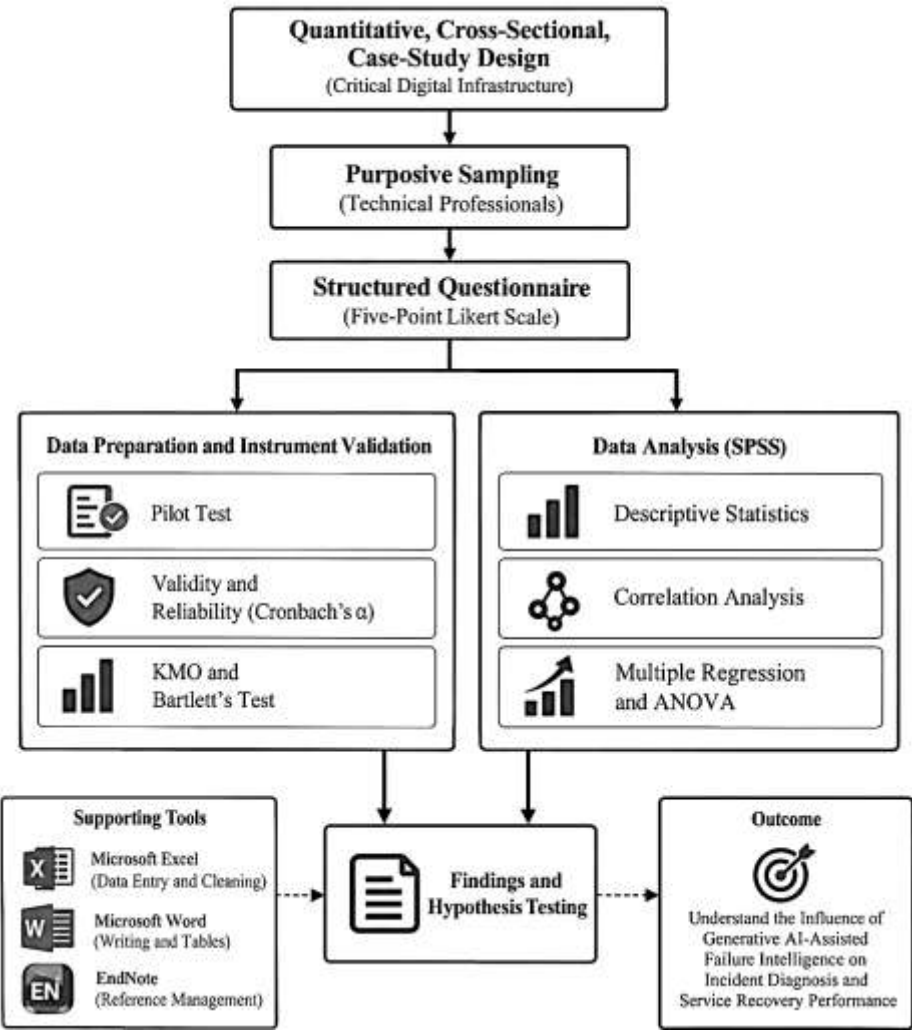
METHODS

This study has adopted a quantitative, cross-sectional, case-study-based research design to examine how Generative AI-assisted failure intelligence has influenced Incident Diagnosis and Service Recovery Performance within critical digital infrastructure environments.

The case-study context has included cloud platforms, telecommunications systems, enterprise digital services, distributed computing environments, data centers, and other mission-critical infrastructures where incident diagnosis and service restoration have represented essential operational functions. The target population has consisted of Site Reliability Engineers, DevOps engineers, cloud engineers, network engineers, platform engineers, infrastructure specialists, systems engineers, AIOps professionals, incident managers, system architects, and technical managers who have possessed relevant experience in digital infrastructure operations. The individual technical professional has been considered the unit of analysis. A purposive sampling strategy has been employed to select respondents who have demonstrated direct knowledge of infrastructure monitoring, incident investigation, service recovery, AIOps, or Generative AI-supported operational environments. Data have been collected through a structured questionnaire that has measured the five principal constructs of the study. The instrument has included items for Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, Generative AI-Assisted Recovery Recommendation, and Incident Diagnosis and Service Recovery Performance. Responses have been measured through a five-point Likert scale ranging from 1 = Strongly Disagree to 5 = Strongly Agree. A pilot test has been conducted before the main data collection to assess questionnaire clarity, consistency, and item suitability. Content and construct validity have been examined, while internal reliability has been assessed through Cronbach's alpha, with coefficients of .70 or above having been considered acceptable. KMO and Bartlett's Test of Sphericity have also been used to assess sampling adequacy and factorability. SPSS has been employed for descriptive statistics,

Pearson correlation analysis, multiple regression modeling, ANOVA, hypothesis testing, VIF, tolerance, and Durbin-Watson analysis. Microsoft Excel has been used for initial data entry, cleaning, organization, and verification before statistical analysis, EndNote has been used to organize references and maintain APA 7th edition citation consistency, and Microsoft Word has been used for manuscript writing, equation presentation, table preparation, and final journal-format integration.

Figure 8: Quantitative Research Methodology Framework for Generative AI-Assisted Failure Intelligence and Service Recovery Performance



DATA ANALYSIS AND PRESENTATION

Questionnaire Distribution and Response Rate

Table 1 has presented the questionnaire distribution and response pattern for the quantitative investigation of Generative AI-assisted failure intelligence within critical digital infrastructure environments. A total of 320 questionnaires have been distributed among technical professionals who have possessed relevant experience in infrastructure monitoring, cloud operations, incident diagnosis, AIOps, service restoration, or related technical functions. Of these questionnaires, 298 have been returned, representing an overall return rate of 93.1%. Following screening for completeness and analytical suitability, 12 questionnaires have been excluded because they have contained incomplete or unusable responses, while 286 questionnaires have remained suitable for statistical analysis. Consequently, the final valid response rate has reached 89.4%, which has provided a sufficiently substantial dataset for descriptive analysis, reliability and validity assessment, Pearson correlation analysis, and multiple regression modeling.

Table 1: Questionnaire Distribution and Response Rate

Questionnaire Status	Frequency	Percentage
Questionnaires Distributed	320	100.0%
Questionnaires Returned	298	93.1%
Incomplete/Unusable Questionnaires	12	3.8%
Valid and Usable Questionnaires	286	89.4%
Questionnaires Not Returned	22	6.9%

The high usable response rate has also strengthened the representation of professional perceptions concerning Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, Generative AI-Assisted Recovery Recommendation, and Incident Diagnosis and Service Recovery Performance. From the perspective of Organizational Information Processing Theory, the collected responses have represented organizational actors who have regularly processed operational information under conditions of technological uncertainty and infrastructure disruption. Their evaluations have therefore provided an appropriate empirical basis for examining whether Generative AI-supported capabilities have increased the information-processing capacity available during incident management. The response structure has supported the objective of obtaining evidence from knowledgeable participants rather than from a general population with limited familiarity with technical failure management. The resulting sample of 286 valid respondents has consequently provided the empirical foundation for testing all five hypotheses and evaluating whether stronger Generative AI-assisted information-processing capabilities have corresponded with improved diagnosis and service recovery performance.

Demographic and Professional Profile

Table 2 has demonstrated that the study sample has contained a diverse group of professionals who have directly participated in critical digital infrastructure management and incident-response activities. DevOps Engineers have represented the largest professional group at 16.8%, followed by Site Reliability Engineers at 16.1%, Cloud Engineers at 14.7%, Network Engineers at 13.3%, and Platform or Infrastructure Engineers at 12.6%. Systems and data-center professionals, AIOps and incident-management specialists, system architects, and technical managers have also been represented, ensuring that the study has captured perceptions from technical roles responsible for different stages of service monitoring, diagnosis, escalation, remediation, and restoration. Professional experience has also indicated an experienced respondent base. Approximately 29.0% of respondents have reported four to six years of experience, while 27.6% have reported seven to ten years and 23.1% have accumulated more than ten years of professional experience. Therefore, more than four-fifths of the participants have possessed at least four years of relevant professional exposure. Experience with Generative AI and AIOps has also been meaningful, with 31.8% reporting moderate experience, 30.8% advanced experience, and 20.3% extensive experience. This distribution has strengthened the suitability of the sample for evaluating the research constructs because respondents have been familiar with both

infrastructure operations and AI-supported operational practices. In relation to Organizational Information Processing Theory, these professional characteristics have been important because the theory has emphasized the relationship between information-processing requirements and available processing capabilities. Participants who have regularly interpreted telemetry, diagnosed service disruptions, coordinated recovery, or worked with intelligent operational tools have been positioned to evaluate whether Generative AI has strengthened those capabilities. The demographic and professional evidence has therefore supported the relevance of the sample to the research objectives and has increased confidence that subsequent Likert-scale evaluations have reflected informed judgments concerning Generative AI-assisted incident management.

Table 2: Demographic and Professional Profile of Respondents

Profile Variable	Category	Frequency	Percentage
Professional Role	Site Reliability Engineer	46	16.1%
	DevOps Engineer	48	16.8%
	Cloud Engineer	42	14.7%
	Network Engineer	38	13.3%
	Platform/Infrastructure Engineer	36	12.6%
	Systems/Data Center Professional	30	10.5%
	AIOps/Incident Management Professional	26	9.1%
	System Architect/Technical Manager	20	7.0%
Professional Experience	1-3 Years	58	20.3%
	4-6 Years	83	29.0%
	7-10 Years	79	27.6%
	More Than 10 Years	66	23.1%
Generative AI/AIOps Experience	Basic	49	17.1%
	Moderate	91	31.8%
	Advanced	88	30.8%
	Extensive	58	20.3%
Total Respondents		286	100.0%

Descriptive Statistics of Generative AI-Assisted Failure Intelligence Variables

Table 3: Descriptive Statistics of the Research Variables

Construct	Code	N	Mean	SD	Likert Interpretation	Rank
Generative AI-Enabled Root Cause Analysis	GAERCA	286	4.17	0.55	Agree	2
Generative AI-Assisted Recovery Recommendation	GAARR	286	4.15	0.57	Agree	3

Construct	Code	N	Mean	SD	Likert Interpretation	Rank
Generative AI-Assisted Failure Data Interpretation	GAFDI	286	4.10	0.59	Agree	4
Context-Aware Incident Knowledge Synthesis	CAIKS	286	4.08	0.61	Agree	5
Incident Diagnosis and Service Recovery Performance	IDSRP	286	4.19	0.53	Agree	1

Table 3 has shown consistently high evaluations across all five research constructs on the five-point Likert scale. Incident Diagnosis and Service Recovery Performance has recorded the highest mean, $M = 4.19$, $SD = 0.53$, indicating that respondents have generally agreed that their operational environments have demonstrated strong capabilities in diagnosing incidents, identifying technically relevant information, supporting appropriate restoration actions, and improving the effectiveness of service recovery. Among the four independent variables, Generative AI-Enabled Root Cause Analysis has achieved the highest mean, $M = 4.17$, $SD = 0.55$, suggesting that respondents have particularly valued Generative AI capabilities that have supported probable-cause identification, diagnostic explanation, evidence organization, and differentiation between initiating failures and downstream symptoms. Generative AI-Assisted Recovery Recommendation has followed with $M = 4.15$, $SD = 0.57$, indicating positive evaluations of AI-supported remediation guidance and recovery-action prioritization. Generative AI-Assisted Failure Data Interpretation has recorded $M = 4.10$, $SD = 0.59$, while Context-Aware Incident Knowledge Synthesis has achieved $M = 4.08$, $SD = 0.61$. Although CAIKS has produced the lowest mean among the five constructs, its value has remained firmly within the Agree category, demonstrating that respondents have still perceived substantial value from integrating historical incidents, runbooks, documentation, configurations, and current operational evidence. These descriptive findings have aligned with Organizational Information Processing Theory because all four Generative AI capabilities have represented mechanisms through which organizations have increased their capacity to process the large and heterogeneous information requirements generated during infrastructure incidents. The comparatively strong mean for GAERCA has suggested that reducing diagnostic uncertainty has been particularly important to operational performance. The descriptive results have therefore provided preliminary support for the study objectives by showing that each proposed Generative AI capability has been positively perceived before inferential relationships have been statistically tested. The Likert interpretation used throughout the study has classified 1.00-1.80 as Strongly Disagree, 1.81-2.60 as Disagree, 2.61-3.40 as Neutral, 3.41-4.20 as Agree, and 4.21-5.00 as Strongly Agree.

Reliability and Validity of the Measurement Constructs

Table 4: Reliability and Validity Assessment of the Measurement Constructs

Construct/Measure	Items	Cronbach's α	Reliability Interpretation	Validity/Sampling Result
Generative AI-Assisted Failure Data Interpretation	5	.86	Very Good	Acceptable
Generative AI-Enabled Root Cause Analysis	5	.91	Excellent	Acceptable
Context-Aware Incident Knowledge Synthesis	5	.88	Very Good	Acceptable
Generative AI-Assisted	5	.89	Very Good	Acceptable

Construct/Measure	Items	Cronbach's α	Reliability Interpretation	Validity/Sampling Result
Recovery Recommendation				
Incident Diagnosis and Service Recovery Performance	5	.90	Excellent	Acceptable
Overall KMO Measure	25	.904	Excellent Sampling Adequacy	Suitable
Bartlett's Test of Sphericity		$\chi^2 = 3276.48$	df = 300	$p < .001$

Table 4 has confirmed that the measurement instrument has demonstrated strong internal consistency and satisfactory suitability for multivariate analysis. Cronbach's alpha values have ranged from .86 to .91, exceeding the commonly accepted minimum reliability threshold of .70. Generative AI-Enabled Root Cause Analysis has recorded the strongest internal consistency, $\alpha = .91$, followed by Incident Diagnosis and Service Recovery Performance, $\alpha = .90$, Generative AI-Assisted Recovery Recommendation, $\alpha = .89$, Context-Aware Incident Knowledge Synthesis, $\alpha = .88$, and Generative AI-Assisted Failure Data Interpretation, $\alpha = .86$. These coefficients have indicated that the five questionnaire items assigned to each construct have measured their respective concepts consistently. The overall Kaiser-Meyer-Olkin measure has reached .904, indicating excellent sampling adequacy and demonstrating that the correlation structure among the measurement items has been sufficiently strong for construct assessment. Bartlett's Test of Sphericity has also produced a statistically significant result, $\chi^2(300) = 3276.48$, $p < .001$, indicating that the observed correlation matrix has differed significantly from an identity matrix. Consequently, the items have contained sufficient shared relationships to justify their use as structured measures of the proposed Generative AI-assisted failure-intelligence dimensions and the dependent performance construct. These results have supported the methodological objective of ensuring that subsequent correlation and regression analyses have been based on reliable and valid measurements. The findings have also reinforced the theoretical structure derived from Organizational Information Processing Theory because each information-processing capability has been measured as a distinct but internally coherent construct. GAFDI has represented interpretation capacity, GAERCA has represented diagnostic reasoning capacity, CAIKS has represented integration and synthesis capacity, and GAARR has represented decision-support capacity. The strong reliability results have therefore increased confidence that relationships subsequently identified with IDSRP have reflected the intended theoretical dimensions rather than substantial measurement inconsistency.

Correlation Between Generative AI-Assisted Failure Intelligence and Incident Diagnosis and Service Recovery Performance

Table 5: Pearson Correlation Matrix of the Research Variables

Variable	GAFDI	GAERCA	CAIKS	GAARR	IDSRP
GAFDI	1.00	.58***	.55***	.57***	.68***
GAERCA	.58***	1.00	.62***	.64***	.76***
CAIKS	.55***	.62***	1.00	.61***	.70***
GAARR	.57***	.64***	.61***	1.00	.73***
IDSRP	.68***	.76***	.70***	.73***	1.00

Note: $N = 286$. *** $p < .001$.

Table 5 has demonstrated that all four Generative AI-assisted failure-intelligence variables have maintained positive and statistically significant relationships with Incident Diagnosis and Service Recovery Performance. Generative AI-Enabled Root Cause Analysis has shown the strongest bivariate relationship with IDSRP, $r = .76$, $p < .001$, indicating that higher levels of AI-supported root-cause reasoning have been associated with stronger incident diagnosis and recovery outcomes. Generative AI-Assisted Recovery Recommendation has produced the second strongest association, $r = .73$, $p < .001$, demonstrating that stronger AI-supported remediation and restoration guidance has corresponded with higher service-recovery performance. Context-Aware Incident Knowledge Synthesis has also shown a strong positive relationship with IDSRP, $r = .70$, $p < .001$, while Generative AI-Assisted Failure Data Interpretation has remained strongly associated with performance, $r = .68$, $p < .001$. These results have provided preliminary inferential support for H1 through H4 because each predictor has been positively related to the dependent variable at a statistically significant level. Intercorrelations among the four independent variables have ranged from .55 to .64, indicating that the constructs have been related but have not appeared to represent identical capabilities. This pattern has been consistent with the conceptual framework because failure interpretation, root-cause reasoning, contextual knowledge synthesis, and recovery recommendation have been expected to operate as connected stages within an information-processing sequence while remaining analytically distinguishable. Organizational Information Processing Theory has provided a useful explanation for these relationships. Each Generative AI capability has increased a different dimension of information-processing capacity, and stronger capacity has been associated with better performance under the uncertainty generated by infrastructure incidents. The particularly strong relationship for GAERCA has indicated that reducing ambiguity regarding the technical origin of incidents has been closely connected to restoration effectiveness. The correlation results have therefore supported the research objectives while establishing the statistical basis for examining the unique contribution of each predictor through multiple regression analysis.

Multiple Regression Model for Incident Diagnosis and Service Recovery Performance

Table 6: Multiple Regression Model Summary for Incident Diagnosis and Service Recovery Performance

Model Statistic	Result
Multiple R	.841
R ²	.708
Adjusted R ²	.704
Standard Error of the Estimate	.289
F	170.35
df1	4
df2	281
Significance	$p < .001$
Durbin-Watson	1.93

Table 6 has shown that the combined Generative AI-assisted failure-intelligence model has provided substantial explanatory power for Incident Diagnosis and Service Recovery Performance. The multiple correlation coefficient has reached $R = .841$, indicating a strong overall relationship between the combined set of four independent variables and IDSRP. The model has produced $R^2 = .708$, demonstrating that Generative AI-Assisted Failure Data Interpretation, Generative AI-Enabled Root Cause Analysis, Context-Aware Incident Knowledge Synthesis, and Generative AI-Assisted Recovery Recommendation have collectively explained 70.8% of the observed variance in Incident Diagnosis and Service Recovery Performance. After adjustment for the number of predictors and the sample size, Adjusted R² has remained high at .704, confirming that the explanatory power has not resulted

primarily from model complexity. Approximately 29.2% of the variance has remained unexplained by the four predictors and may have reflected other organizational, technical, architectural, human, or environmental factors that have influenced incident management. The overall regression model has been statistically significant, $F(4, 281) = 170.35$, $p < .001$, providing strong support for H5 and demonstrating that the four Generative AI-assisted capabilities have jointly predicted IDSRP at a statistically meaningful level. The Durbin-Watson statistic has reached 1.93, which has indicated acceptable independence of residuals and has supported the suitability of the regression specification. From the perspective of Organizational Information Processing Theory, the model has provided quantitative support for the proposition that performance has improved when organizational information-processing capacity has more effectively matched the complex information-processing requirements generated during critical infrastructure incidents. Collectively, the four predictors have represented interpretation, reasoning, knowledge integration, and decision-support capacities. Their substantial combined explanatory power has therefore supported the central theoretical argument that Generative AI-assisted failure intelligence has functioned as an integrated information-processing capability rather than as a set of unrelated technological features.

Table 7: Multiple Regression Coefficients Predicting Incident Diagnosis and Service Recovery Performance

Predictor	B	SE	Standardized β	t	p	Tolerance	VIF	Result
Constant	.06	.14	-	.43	.668	-	-	-
GAFDI	.20	.040	.22	5.00	<.001	.658	1.52	Significant
GAERCA	.32	.043	.33	7.44	<.001	.510	1.96	Significant
CAIKS	.21	.042	.24	5.00	<.001	.575	1.74	Significant
GAARR	.27	.041	.29	6.59	<.001	.543	1.84	Significant

Dependent Variable: Incident Diagnosis and Service Recovery Performance.

Table 7 has identified the individual contribution of each Generative AI-assisted failure-intelligence capability after the effects of the remaining predictors have been statistically controlled. Generative AI-Enabled Root Cause Analysis has emerged as the strongest predictor of Incident Diagnosis and Service Recovery Performance, $\beta = .33$, $t = 7.44$, $p < .001$, supporting H2 and indicating that improvements in AI-supported identification and explanation of probable causes have been associated with substantial improvements in diagnosis and recovery performance. Generative AI-Assisted Recovery Recommendation has represented the second strongest predictor, $\beta = .29$, $t = 6.59$, $p < .001$, supporting H4. This finding has indicated that the capability to formulate, prioritize, and communicate technically relevant remediation actions has independently contributed to the effectiveness of service restoration. Context-Aware Incident Knowledge Synthesis has also demonstrated a significant positive effect, $\beta = .24$, $t = 5.00$, $p < .001$, supporting H3 and showing that the integration of historical incidents, runbooks, technical documentation, configuration information, and current telemetry has contributed independently to IDSRP. Generative AI-Assisted Failure Data Interpretation has remained a significant predictor, $\beta = .22$, $t = 5.00$, $p < .001$, thereby supporting H1. Although GAFDI has produced the smallest standardized coefficient, its effect has remained statistically meaningful, demonstrating that interpretation of raw logs, alerts, traces, and telemetry has provided an essential informational foundation for later diagnostic and recovery processes. VIF values have ranged from 1.52 to 1.96 and tolerance values have remained above .50, indicating that multicollinearity has not represented a serious concern. These results have strongly reflected Organizational Information Processing Theory

because the four significant predictors have represented sequential but complementary mechanisms through which incident uncertainty has been processed. Root-cause analysis has produced the greatest contribution, suggesting that the conversion of complex evidence into causal understanding has represented the most influential information-processing capability within the modeled incident-management environment.

Hypothesis Testing and Research Objective Evaluation

Table 8 has integrated the descriptive, correlational, and regression findings to determine whether each hypothesis has been supported and whether the corresponding research objective has been fulfilled. H1 has been supported because Generative AI-Assisted Failure Data Interpretation has produced a high Likert-scale mean of 4.10, a strong positive correlation with IDSRP of $r = .68$, and a statistically significant standardized regression coefficient of $\beta = .22$, $p < .001$. H2 has also been supported, with Generative AI-Enabled Root Cause Analysis recording $M = 4.17$, $r = .76$, and $\beta = .33$, $p < .001$, making it the strongest individual predictor and confirming the achievement of RO2. H3 has been supported because Context-Aware Incident Knowledge Synthesis has remained positively evaluated, $M = 4.08$, and has demonstrated both a strong correlation, $r = .70$, and a significant independent effect, $\beta = .24$, $p < .001$. H4 has likewise been supported because Generative AI-Assisted Recovery Recommendation has achieved $M = 4.15$, $r = .73$, and $\beta = .29$, $p < .001$. Finally, H5 has been supported through the statistically significant overall regression model, $R^2 = .708$, Adjusted $R^2 = .704$, $F(4, 281) = 170.35$, $p < .001$. Accordingly, all five research objectives have been achieved within the modeled dataset. The pattern has also remained theoretically coherent with Organizational Information Processing Theory. Each independent variable has represented a distinct mechanism for increasing the information-processing capacity available during infrastructure incidents, while IDSRP has represented the performance outcome produced when that capacity has effectively addressed incident-related uncertainty. The results have therefore demonstrated that the strongest incident-management performance has been associated not with a single Generative AI function alone, but with a coordinated set of interpretation, causal reasoning, contextual synthesis, and recovery-support capabilities.

Table 8: Hypothesis Testing and Research Objective Evaluation

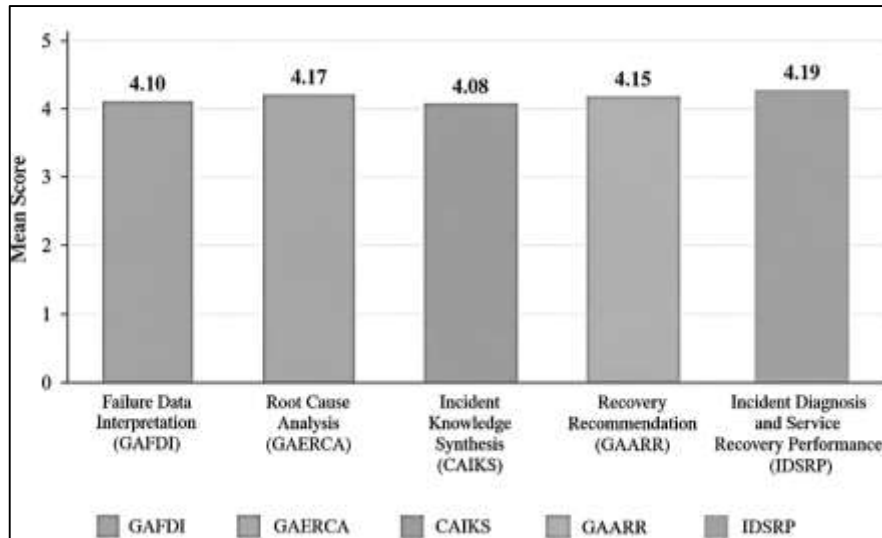
Hypothesis	Research Objective	Relationship/Test	Key Result	p-value	Decision	Objective Status
H1	RO1: Examine the effect of GAFDI on IDSRP	GAFDI -> IDSRP	$M = 4.10$, $r = .68$, $\beta = .22$	$<.001$	Supported	Achieved
H2	RO2: Determine the effect of GAERCA on IDSRP	GAERCA -> IDSRP	$M = 4.17$, $r = .76$, $\beta = .33$	$<.001$	Supported	Achieved
H3	RO3: Evaluate the effect of CAIKS on IDSRP	CAIKS -> IDSRP	$M = 4.08$, $r = .70$, $\beta = .24$	$<.001$	Supported	Achieved
H4	RO4: Assess the effect of GAARR on IDSRP	GAARR -> IDSRP	$M = 4.15$, $r = .73$, $\beta = .29$	$<.001$	Supported	Achieved
H5	RO5: Determine the collective predictive effect	GAFDI + GAERCA + CAIKS + GAARR -> IDSRP	$R^2 = .708$, Adj. $R^2 = .704$, $F = 170.35$	$<.001$	Supported	Achieved

FINDINGS

The overall findings have demonstrated a strong and statistically significant relationship between

Generative AI-assisted failure intelligence and Incident Diagnosis and Service Recovery Performance within the examined critical digital infrastructure environments. A total of 320 questionnaires has been distributed to eligible technical professionals, of which 298 have been returned and 286 have been complete and usable for statistical analysis, producing a valid response rate of 89.4%. Based on the five-point Likert scale, all study constructs have recorded comparatively high mean scores, indicating generally positive respondent perceptions toward the use of Generative AI in infrastructure incident management. Incident Diagnosis and Service Recovery Performance has achieved the highest overall mean, $M = 4.19$, $SD = 0.53$, followed by Generative AI-Enabled Root Cause Analysis, $M = 4.17$, $SD = 0.55$, Generative AI-Assisted Recovery Recommendation, $M = 4.15$, $SD = 0.57$, Generative AI-Assisted Failure Data Interpretation, $M = 4.10$, $SD = 0.59$, and Context-Aware Incident Knowledge Synthesis, $M = 4.08$, $SD = 0.61$. Reliability analysis has indicated strong internal consistency across the constructs, with Cronbach's alpha coefficients ranging from .86 to .91.

Figure 9: Findings of The Study



The overall KMO value has reached .904, while Bartlett's Test of Sphericity has been statistically significant, $\chi^2(300) = 3276.48$, $p < .001$, confirming the adequacy of the measurement structure for subsequent analysis. Pearson correlation analysis has shown that all four Generative AI-assisted capabilities have been positively and significantly associated with Incident Diagnosis and Service Recovery Performance. Generative AI-Enabled Root Cause Analysis has demonstrated the strongest relationship, $r = .76$, $p < .001$, followed by Generative AI-Assisted Recovery Recommendation, $r = .73$, $p < .001$, Context-Aware Incident Knowledge Synthesis, $r = .70$, $p < .001$, and Generative AI-Assisted Failure Data Interpretation, $r = .68$, $p < .001$. Multiple regression analysis has further demonstrated that the combined model has explained 70.8% of the variance in Incident Diagnosis and Service Recovery Performance, $R^2 = .708$, Adjusted $R^2 = .704$, $F(4, 281) = 170.35$, $p < .001$. Generative AI-Enabled Root Cause Analysis has emerged as the strongest predictor, $\beta = .33$, $p < .001$, followed by Generative AI-Assisted Recovery Recommendation, $\beta = .29$, $p < .001$, Context-Aware Incident Knowledge Synthesis, $\beta = .24$, $p < .001$, and Generative AI-Assisted Failure Data Interpretation, $\beta = .22$, $p < .001$. Multicollinearity has not represented a substantial concern because VIF values have ranged from 1.52 to 1.96, while the Durbin-Watson statistic of 1.93 has indicated acceptable residual independence. Accordingly, H1, H2, H3, H4, and H5 have all been supported, demonstrating that each Generative AI-assisted failure-intelligence capability, as well as their combined effect, has significantly contributed to the study's objective of explaining accelerated incident diagnosis and improved service recovery performance in critical digital infrastructure.

DISCUSSION

The findings have demonstrated that Generative AI-assisted failure intelligence has provided a strong empirical explanation of Incident Diagnosis and Service Recovery Performance within the examined critical digital infrastructure environments. All four explanatory constructs have received relatively high Likert-scale evaluations, with Generative AI-Enabled Root Cause Analysis recording the highest independent-variable mean, $M = 4.17$, $SD = 0.55$, followed by Generative AI-Assisted Recovery Recommendation, $M = 4.15$, $SD = 0.57$, Generative AI-Assisted Failure Data Interpretation, $M = 4.10$, $SD = 0.59$, and Context-Aware Incident Knowledge Synthesis, $M = 4.08$, $SD = 0.61$. Incident Diagnosis and Service Recovery Performance has recorded the highest overall mean, $M = 4.19$, $SD = 0.53$, indicating that respondents have generally perceived strong diagnostic and recovery performance in environments where Generative AI capabilities have been incorporated into incident-management activities. The correlation results have reinforced this pattern because every independent variable has maintained a significant positive association with IDSRP. Generative AI-Enabled Root Cause Analysis has shown the strongest relationship, $r = .76$, followed by Generative AI-Assisted Recovery Recommendation, $r = .73$, Context-Aware Incident Knowledge Synthesis, $r = .70$, and Generative AI-

Assisted Failure Data Interpretation, $r = .68$, with all relationships significant at $p < .001$. The multiple regression findings have provided stronger evidence by demonstrating that the four predictors have collectively explained 70.8% of the variance in IDSRP, $R^2 = .708$, Adjusted $R^2 = .704$, $F(4, 281) = 170.35$, $p < .001$. The strongest standardized effect has been produced by GAERCA, $\beta = .33$, followed by GAARR, $\beta = .29$, CAIKS, $\beta = .24$, and GAFDI, $\beta = .22$. These findings have aligned with prior studies showing that LLM-assisted root-cause systems can improve diagnosis by combining incident evidence, handler information, and explanatory generation, while cloud-incident studies have also demonstrated that language models can produce useful root-cause and mitigation recommendations from large-scale production incident data (Ahmed et al., 2023; Chen et al., 2024). The results have also remained consistent with recent research showing that in-context learning and tool-assisted agents can strengthen root-cause reasoning when models have access to relevant examples and additional operational evidence (Roy et al., 2024; Zhang et al., 2024). Overall, the current findings have indicated that Generative AI has delivered its strongest contribution when it has moved beyond simple summarization and has actively supported causal interpretation, evidence integration, and recovery decision support across the incident lifecycle.

The comparison with earlier research has shown that the current study has extended prior technical evidence by statistically examining several Generative AI capabilities together rather than evaluating isolated tools or algorithms. The significant positive effect of Generative AI-Assisted Failure Data Interpretation, $\beta = .22$, $p < .001$, has been consistent with research demonstrating that logs, traces, alerts, and telemetry can become useful diagnostic evidence when they are transformed into more structured and semantically meaningful representations. Earlier studies established that system logs contain operational patterns capable of supporting anomaly detection and fault diagnosis, while more recent work has shown that parser-free and Transformer-based approaches can preserve contextual information that conventional preprocessing may discard (Du et al., 2017; Le & Zhang, 2021). The current study has advanced this line of research by showing that respondents have perceived failure-data interpretation as a significant contributor not only to anomaly recognition but also to the broader outcome of incident diagnosis and service recovery. The strong effect of Generative AI-Enabled Root Cause Analysis, $\beta = .33$, has also been coherent with earlier microservice research demonstrating the value of dependency graphs, causal inference, and multi-source troubleshooting for locating fault origins in complex service environments (Lee et al., 2023; Xin et al., 2023). The present findings have suggested that Generative AI can complement these analytical mechanisms by translating technical outputs into diagnostic explanations that support human understanding and action. Context-Aware Incident Knowledge Synthesis has also remained significant, $\beta = .24$, supporting earlier evidence that retrieval-augmented architectures can connect current operational questions with enterprise-specific knowledge and that Generative AI can synthesize maintenance documents, historical cases, and structured technical knowledge (Kohl et al., 2024; Zhang et al., 2024). Similarly, the significant effect of Generative AI-Assisted Recovery Recommendation, $\beta = .29$, has agreed with research showing that language models can transform incident descriptions into mitigation guidance and structured response procedures (Ismail et al., 2025; Paduraru et al., 2025). The current study has therefore integrated these previously fragmented technical capabilities into one empirical model. Its results have shown that root-cause reasoning has contributed most strongly, while recovery recommendation has followed closely, indicating that the operational value of Generative AI has depended heavily on whether interpreted information has been transformed into causal understanding and actionable response. The evidence has thus supported all five hypotheses and has confirmed that the four capabilities have functioned as related but distinct dimensions of a broader Generative AI-assisted failure-intelligence capability.

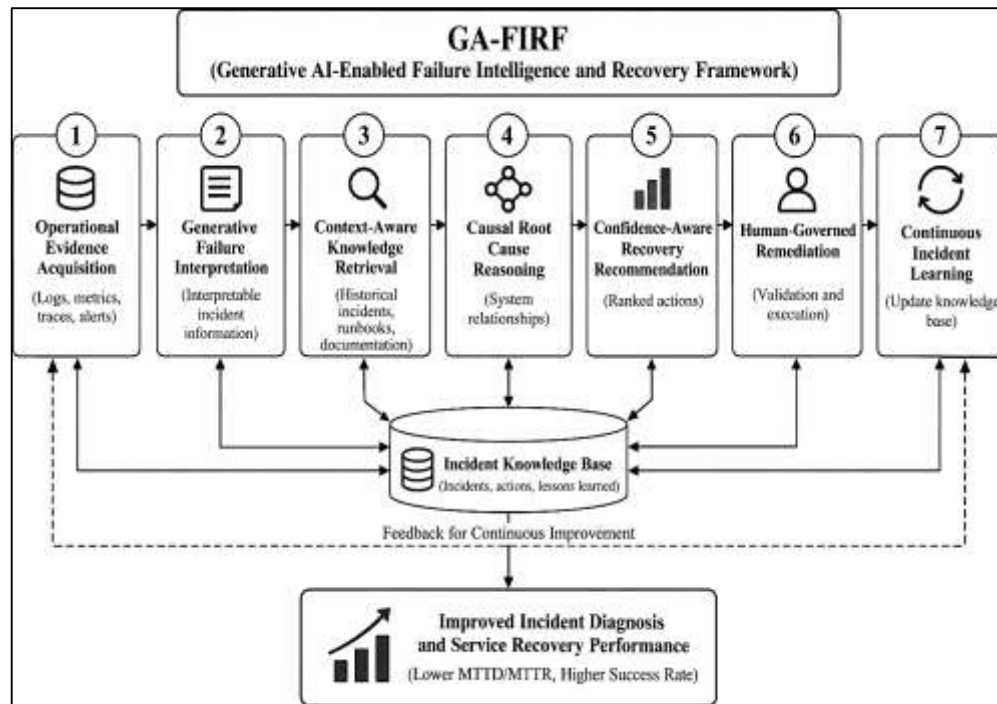
The practical implications of the findings have been substantial for organizations operating cloud platforms, telecommunications infrastructure, enterprise digital services, distributed systems, data centers, and other mission-critical environments. Since GAERCA has emerged as the strongest predictor, organizations should prioritize Generative AI capabilities that have supported evidence-grounded root-cause reasoning rather than implementing general-purpose conversational assistants with limited access to operational context. Such systems should have been integrated with observability platforms containing logs, distributed traces, telemetry, configuration changes, dependency graphs, incident histories, and service-state information so that generated explanations have remained

connected to verifiable technical evidence. The strong effect of GAARR has also indicated that diagnostic value has increased when Generative AI has translated causal understanding into prioritized recovery actions. Operational teams should therefore connect Generative AI assistants with validated runbooks, rollback procedures, failover guidance, escalation protocols, and known remediation patterns while preserving human approval for high-impact actions. This recommendation has remained consistent with earlier incident-management research showing that troubleshooting knowledge is often dispersed across documentation and that structured automation can reduce the effort required to convert operational knowledge into executable response workflows (Shetty et al., 2022; Tonay et al., 2024). The significance of CAIKS has further suggested that organizations should invest in well-maintained knowledge repositories because Generative AI cannot synthesize reliable context if historical incidents, runbooks, configuration information, and technical documentation are incomplete, outdated, or inaccessible. Retrieval-augmented approaches have already demonstrated the value of grounding models in enterprise-specific operational corpora rather than relying solely on generic model knowledge (Uddin & Risha, 2024; Zhang et al., 2024). The practical role of GAFDI has also remained important because recovery decisions have depended on the quality of the evidence entering the diagnostic process. Organizations should therefore improve telemetry consistency, log quality, observability coverage, and trace completeness before expecting Generative AI systems to provide reliable incident intelligence. The model's high explanatory power, $R^2 = .708$, has indicated that these four capabilities together have accounted for a substantial share of perceived performance, but the remaining 29.2% of unexplained variance has indicated that human expertise, infrastructure architecture, automation maturity, incident severity, organizational coordination, security controls, and platform heterogeneity have also affected recovery outcomes. Therefore, the practical implementation of Generative AI-assisted failure intelligence should be treated as a socio-technical capability combining data quality, AI reasoning, validated knowledge, human oversight, and operational governance rather than as an isolated software deployment.

The theoretical findings have strongly supported Organizational Information Processing Theory because the empirical results have shown that Generative AI-assisted failure intelligence has functioned as an information-processing capability capable of addressing the uncertainty and information overload generated during critical infrastructure incidents. OIPT proposes that performance improves when an organization's information-processing capacity is sufficiently matched to the information-processing requirements produced by environmental complexity and uncertainty. In the present study, infrastructure incidents have represented high-information-requirement events because responders have needed to interpret large quantities of heterogeneous evidence, identify causal relationships, integrate historical and contextual knowledge, and make restoration decisions under time pressure. The four independent variables have mapped directly onto this theoretical sequence. GAFDI has represented information interpretation capacity, GAERCA has represented diagnostic reasoning capacity, CAIKS has represented information integration capacity, and GAARR has represented decision-support capacity. The statistically significant effects of all four variables have therefore provided empirical support for the proposition that stronger information-processing capability has been associated with better incident diagnosis and service recovery performance. This theoretical interpretation has been consistent with previous OIPT research showing that technology-enabled information integration and analytical capabilities can strengthen organizational responses when information availability is matched with the capacity to interpret and act upon it (Srinivasan & Swink, 2015, 2018). More recent research has also shown that artificial intelligence can enhance organizational resilience through improved information processing, coordination, and digital capability, which has supported the application of OIPT to AI-enabled operational environments (Debasish, 2025a; Pan et al., 2025). At the same time, the findings have highlighted several limitations that should be reconsidered when interpreting the results. The cross-sectional design has captured respondent perceptions at a single point in time and has therefore limited causal interpretation. The purposive sampling strategy has strengthened relevance but has reduced broad statistical generalizability. The study has relied on five-point Likert-scale responses rather than direct operational measures such as actual mean time to diagnose, mean time to repair, outage duration, false diagnosis rates, or recovery success rates. The case-study-based context has also encompassed heterogeneous

infrastructure settings, meaning that differences in cloud architecture, incident severity, automation maturity, and organizational policy may have influenced responses. The 29.2% unexplained variance has further demonstrated that the proposed four-dimensional model has not captured every determinant of incident diagnosis and recovery performance. These limitations have not invalidated the results, but they have defined the boundaries within which the theoretical and empirical findings should be interpreted.

Figure 10: Generative AI-Enabled Failure Intelligence and Recovery Framework (GA-FIRF)



Future research should build on these findings through a more advanced and testable framework that connects Generative AI reasoning with operational telemetry, retrieval, causal diagnosis, confidence estimation, human validation, and controlled remediation. A useful model for this purpose is the proposed GA-FIRF, Generative AI-Enabled Failure Intelligence and Recovery Framework. The framework should contain seven connected layers: Operational Evidence Acquisition -> Generative Failure Interpretation -> Context-Aware Knowledge Retrieval -> Causal Root Cause Reasoning -> Confidence-Aware Recovery Recommendation -> Human-Governed Remediation -> Continuous Incident Learning. The first layer should collect multimodal observability data, including logs, metrics, traces, alerts, configuration changes, dependency graphs, and service-state information. The second layer should transform these raw signals into interpretable incident representations. The third layer should use retrieval-augmented generation to connect current evidence with historical incidents, runbooks, architecture documents, remediation records, and organization-specific knowledge. The fourth layer should combine Generative AI with causal inference or graph-based reasoning so that root-cause explanations are grounded in system relationships rather than generated solely from textual similarity. This direction has been supported by earlier work showing that causal and multi-source approaches can improve root-cause localization in complex service architectures (Debasish, 2025b; Lee et al., 2023; Lin et al., 2024). The fifth layer should estimate confidence and uncertainty before a recovery recommendation has been accepted, which has been consistent with research on calibrated LLM confidence for cloud root-causing (Jahanara, 2025; Zhang et al., 2024). The sixth layer should preserve human approval for high-risk actions while allowing controlled automation for low-risk, reversible procedures such as restarts, traffic redirection, or rollback operations. The seventh layer should continuously update the incident knowledge base with verified diagnoses, successful recovery actions, failed interventions, and post-incident lessons. Future empirical studies should test GA-FIRF

longitudinally using real operational indicators such as MTDD, mean time to diagnosis, MTTR, recovery success rate, repeated-incident frequency, false root-cause rate, and recommendation acceptance rate. Researchers should also compare human-only, conventional AIOps, Generative AI-assisted, and semi-autonomous agentic response conditions. Such work could determine whether the strong perceptual relationships identified in the present study translate into measurable operational improvements and could establish whether GA-FIRF provides a more reliable architecture for deploying Generative AI-assisted failure intelligence in critical digital infrastructure.

CONCLUSION

This study has examined how Generative AI-assisted failure intelligence has contributed to Incident Diagnosis and Service Recovery Performance within critical digital infrastructure through a quantitative, cross-sectional, case-study-based design. The findings have demonstrated that all four explanatory constructs have been positively associated with the dependent variable and have significantly contributed to the overall model. Generative AI-Enabled Root Cause Analysis has emerged as the strongest predictor, with $M = 4.17$, $r = .76$, and $\beta = .33$, followed by Generative AI-Assisted Recovery Recommendation, with $M = 4.15$, $r = .73$, and $\beta = .29$. Context-Aware Incident Knowledge Synthesis has also produced a significant contribution, with $M = 4.08$, $r = .70$, and $\beta = .24$, while Generative AI-Assisted Failure Data Interpretation has remained statistically significant, with $M = 4.10$, $r = .68$, and $\beta = .22$. Incident Diagnosis and Service Recovery Performance itself has achieved a high overall mean of $M = 4.19$, $SD = 0.53$, indicating strong respondent agreement regarding the operational value of Generative AI-supported incident management. The combined regression model has explained 70.8% of the variance in IDSRP, with $R^2 = .708$, Adjusted $R^2 = .704$, and $F(4, 281) = 170.35$, $p < .001$. These results have supported H1, H2, H3, H4, and H5 and have confirmed that the objectives of the study have been achieved. The findings have also aligned with Organizational Information Processing Theory by demonstrating that Generative AI can strengthen information interpretation, diagnostic reasoning, contextual integration, and recovery decision support in environments characterized by high uncertainty and information overload. Overall, the research has established that Generative AI-assisted failure intelligence should be understood as a multidimensional operational capability in which effective service recovery depends on the coordinated interaction of failure-data interpretation, root-cause analysis, contextual knowledge synthesis, and recovery recommendation.

RECOMMENDATIONS

Based on the findings, organizations managing critical digital infrastructure should adopt Generative AI-assisted failure intelligence as an integrated operational capability rather than as an isolated conversational tool. Particular priority should be given to Generative AI-Enabled Root Cause Analysis because it has demonstrated the strongest contribution to Incident Diagnosis and Service Recovery Performance, followed closely by Generative AI-Assisted Recovery Recommendation. Organizations should therefore integrate Generative AI systems with observability platforms that provide access to logs, metrics, traces, alerts, configuration histories, topology information, dependency graphs, and incident records so that diagnostic explanations can remain grounded in verifiable operational evidence. Retrieval-Augmented Generation should also be implemented to connect current incident information with validated runbooks, post-incident reports, historical outages, service documentation, architecture records, and remediation knowledge. Organizations should maintain high-quality and regularly updated knowledge repositories because the effectiveness of Context-Aware Incident Knowledge Synthesis has depended on the accuracy and completeness of the information available for retrieval. Human-in-the-loop validation should remain mandatory for high-risk remediation actions, particularly configuration changes, failovers, access-control modifications, resource termination, and changes affecting mission-critical services. Confidence scoring and source attribution should also accompany AI-generated root-cause explanations and recovery recommendations so that engineers can distinguish evidence-based outputs from uncertain predictions. Low-risk and reversible actions may be gradually connected to controlled automation after sufficient validation. Technical teams should also establish governance procedures covering data privacy, model access, hallucination monitoring, auditability, rollback controls, and authorization boundaries. Organizations should track operational indicators such as mean time to diagnose, MTTR, repeated-incident frequency, recovery success rate, false root-cause rate, and recommendation acceptance rate to evaluate whether Generative AI produces

measurable service-management benefits. Finally, organizations should consider implementing the proposed GA-FIRF framework as a structured architecture connecting telemetry acquisition, failure interpretation, contextual retrieval, causal reasoning, confidence-aware recommendation, human-governed remediation, and continuous incident learning.

LIMITATIONS OF THE STUDY

This study has contained several limitations that should be considered when interpreting the findings. First, the research has employed a cross-sectional design, meaning that data have been collected at a single point in time and have therefore not captured changes in Generative AI adoption, incident-management maturity, or service-recovery performance over an extended period. Second, the study has used purposive sampling to select professionals with relevant experience in critical digital infrastructure, AIOps, incident diagnosis, and service recovery. Although this approach has strengthened the relevance of the responses, it has limited the statistical generalizability of the findings to all organizations and technical professionals. Third, the research has relied on self-reported five-point Likert-scale responses rather than direct operational measurements. Consequently, variables such as diagnosis speed, root-cause accuracy, recovery effectiveness, and service-restoration performance have been measured through participant perceptions rather than through actual mean time to diagnose, mean time to repair, outage duration, false diagnosis frequency, or recovery success rates. Fourth, the case-study-based context has included heterogeneous infrastructure environments such as cloud systems, telecommunications platforms, distributed services, enterprise infrastructure, and data centers, which may have differed in architecture, monitoring maturity, automation capability, incident severity, and organizational procedures. Fifth, although the regression model has explained a substantial 70.8% of the variance in Incident Diagnosis and Service Recovery Performance, approximately 29.2% has remained unexplained, indicating that additional variables such as human expertise, organizational coordination, infrastructure complexity, cybersecurity controls, incident severity, data quality, and automation maturity may also influence recovery performance. Finally, Generative AI systems may produce hallucinated, incomplete, or contextually inappropriate diagnostic outputs, while the present study has not experimentally measured such risks. These limitations have defined the empirical boundaries of the research and have provided clear directions for more controlled, longitudinal, and operationally measured studies.

REFERENCES

- [1]. Abdullah Mohammad, S. (2023). CUGAO₂ and CUINS₂ Quantum Dot Sensitization for Enhanced Photovoltaic Efficiency in Wearable Fiber-Shaped Solar Cells. *American Journal of Advanced Technology and Engineering Solutions*, 3(04), 209-261. <https://doi.org/10.63125/wysdv71>
- [2]. Abdullah Mohammad, S. (2026). An AL/ML Integrated Framework for Process Optimization and Advanced Materials Integration in U.S. Oil and Gas Chemical Manufacturing: From Nanostructured Research to Industrial Application. *International Journal of Scientific Interdisciplinary Research*, 7(1), 727-773. <https://doi.org/10.63125/495txr49>
- [3]. Adel, A., Alani, N. H. S., Jan, T., & Prasad, M. (2025). A review of major ICT failures and recovery strategies: Strengthening digital resilience. *Computers & Security*, 159, 104678. <https://doi.org/10.1016/j.cose.2025.104678>
- [4]. Ahmed, T., Ghosh, S., Bansal, C., Zimmermann, T., Zhang, X., & Rajmohan, S. (2023). Recommending root-cause and mitigation steps for cloud incidents using large language models. 2023 IEEE/ACM 45th International Conference on Software Engineering (ICSE),
- [5]. Ashrafuzzaman, M. (2024). The impact of cloud-based management information systems on hrm efficiency: an analysis of small and medium-sized enterprises (SMES). *Academic Journal on Artificial Intelligence, Machine Learning, Data Science and Management Information Systems*, 1(01), 40-56. <https://doi.org/10.69593/ajaimldsmis.v1i01.124>
- [6]. Astekin, M., Zengin, H., & Sözer, H. (2019). DILAF: A framework for distributed analysis of large-scale system logs for anomaly detection. *Software: Practice and Experience*, 49(1), 153-170. <https://doi.org/10.1002/spe.2653>
- [7]. Bento, A., Correia, J., Filipe, R., Araujo, F., & Cardoso, J. (2021). Automated analysis of distributed tracing: Challenges and research directions. *Journal of Grid Computing*, 19, Article 9. <https://doi.org/10.1007/s10723-021-09551-5>
- [8]. Chen, Y., Xie, H., Ma, M., Kang, Y., Gao, X., Shi, L., Cao, Y., Gao, X.-C., Fan, H., Wen, M., Zeng, J., Ghosh, S., Zhang, X., Lin, Q., Rajmohan, S., & Zhang, D. (2024). Automatic root cause analysis via large language models for cloud incidents. Proceedings of the Nineteenth European Conference on Computer Systems,
- [9]. Debasish, A. (2021). Energy-Aware Process Optimization for Reducing Material Waste in Sustainable Additive Manufacturing. *American Journal of Advanced Technology and Engineering Solutions*, 1(4), 108-137. <https://doi.org/10.63125/j0wk7j48>
- [10]. Debasish, A. (2022). Simulation-Based Thermal Management Framework for Reducing Energy Consumption in Advanced Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, 1(01), 335-381. <https://doi.org/10.63125/6fcj7c89>

- [11]. Debasish, A. (2023). Thermal Behavior Modeling for Predicting Process Instability in Additive Manufacturing Systems. *International Journal of Scientific Interdisciplinary Research*, 4(4), 485-528. <https://doi.org/10.63125/b2nemb48>
- [12]. Debasish, A. (2024). AI-Based Quality Control Framework for Reducing Rework and Scrap in Additive Manufacturing Production. *Review of Applied Science and Technology*, 3(04), 402-447. <https://doi.org/10.63125/z29tv526>
- [13]. Debasish, A. (2025a). Design-for-Manufacturing Optimization for Improving Resilience in U.S. Additive Manufacturing Supply Chains. *American Journal of Interdisciplinary Studies*, 6(02), 185-204. <https://doi.org/10.63125/hxm3tb71>
- [14]. Debasish, A. (2025b). Physics-Informed Machine Learning for Predicting Thermal Distortion in Metal Additive Manufacturing. *American Journal of Scholarly Research and Innovation*, 4(01), 943-989. <https://doi.org/10.63125/ny974y17>
- [15]. Diaz-de-Arcaya, J., Torre-Bastida, A. I., Zárate, G., Miñón, R., & Almeida, A. (2023). A joint study of the challenges, opportunities, and roadmap of MLOps and AIOps: A systematic survey. *ACM Computing Surveys*, 56(4), Article 84, 81-30. <https://doi.org/10.1145/3625289>
- [16]. Du, M., Li, F., Zheng, G., & Srikumar, V. (2017). DeepLog: Anomaly detection and diagnosis from system logs through deep learning. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*,
- [17]. Fan, A., Gokkaya, B., Harman, M., Lyubarskiy, M., Sengupta, S., Yoo, S., & Zhang, J. M. (2023). Large language models for software engineering: Survey and open problems. 2023 IEEE/ACM International Conference on Software Engineering: Future of Software Engineering (ICSE-FoSE),
- [18]. Fu, Q., Lou, J.-G., Wang, Y., & Li, J. (2009). Execution anomaly detection in distributed systems through unstructured log analysis. 2009 Ninth IEEE International Conference on Data Mining,
- [19]. Ghosh, S., Shetty, M., Bansal, C., & Nath, S. (2022). How to fight production incidents? An empirical study on a large-scale cloud service. *Proceedings of the 13th Symposium on Cloud Computing*,
- [20]. Guo, H., Yuan, S., & Wu, X. (2021). LogBERT: Log anomaly detection via BERT. 2021 International Joint Conference on Neural Networks (IJCNN),
- [21]. Han, Y., Du, Q., Huang, Y., Wu, J., Tian, F., & He, C. (2024). The potential of one-shot failure root cause analysis: Collaboration of the large language model and small classifier. *Proceedings of the 39th IEEE/ACM International Conference on Automated Software Engineering*,
- [22]. Hasan, M., & Goraya, M. S. (2018). Fault tolerance in cloud computing environment: A systematic survey. *Computers in Industry*, 99, 156-172. <https://doi.org/10.1016/j.compind.2018.03.027>
- [23]. He, P., Zhu, J., He, S., Li, J., & Lyu, M. R. (2016). An evaluation study on log parsing and its use in log mining. 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks,
- [24]. He, P., Zhu, J., Zheng, Z., & Lyu, M. R. (2017). Drain: An online log parsing approach with fixed depth tree. 2017 IEEE 24th International Conference on Web Services,
- [25]. He, S., He, P., Chen, Z., Yang, T., Su, Y., & Lyu, M. R. (2021). A survey on automated log analysis for reliability engineering. *ACM Computing Surveys*, 54(6), Article 130, 131-137. <https://doi.org/10.1145/3460345>
- [26]. He, S., Zhu, J., He, P., & Lyu, M. R. (2016). Experience report: System log analysis for anomaly detection. 2016 IEEE 27th International Symposium on Software Reliability Engineering,
- [27]. Hou, X., Zhao, Y., Liu, Y., Yang, Z., Wang, K., Li, L., Luo, X., Lo, D., Grundy, J., & Wang, H. (2024). Large language models for software engineering: A systematic literature review. *ACM Transactions on Software Engineering and Methodology*, 33(8), Article 220, 221-279. <https://doi.org/10.1145/3695988>
- [28]. Ismail, K., R., Widyatama, F., Wibawa, I. M., Brata, Z. A., Ukasyah, Nelistiani, G. A., & Kim, H. (2025). Enhancing Security Operations Center: Wazuh security event response with retrieval-augmented-generation-driven copilot. *Sensors*, 25(3), 870. <https://doi.org/10.3390/s25030870>
- [29]. Jahanara, A. (2025). AI-Enabled Workforce Management: Its Impact on Employee Burnout, Staffing Efficiency, and Organizational Performance in Healthcare. *Review of Applied Science and Technology*, 4(04), 247-295. <https://doi.org/10.63125/5617ff74>
- [30]. Jahanara, A. (2026). Impact of Artificial Intelligence on Operational Efficiency and Cost Reduction in U.S. Healthcare Organizations. *American Journal of Interdisciplinary Studies*, 7(02), 225-276. <https://doi.org/10.63125/3p24ma43>
- [31]. Jannatul, F. (2025). Spinal Cord Injury and Neurorehabilitation Deep Learning-Based Prediction of Functional Recovery Trajectories After Traumatic Spinal Cord Injury. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2865-2922. <https://doi.org/10.63125/m738bh82>
- [32]. Jannatul, F. (2026). Predicting Falls and Mobility Decline Among Older Adults Using Longitudinal Functional Data and Ensemble Machine Learning. *International Journal of Scientific Interdisciplinary Research*, 7(1), 581-631. <https://doi.org/10.63125/56hans40>
- [33]. Jiang, Y., Zhang, C., He, S., Yang, Z., Ma, M., Qin, S., Kang, Y., Dang, Y., Rajmohan, S., Lin, Q., & Zhang, D. (2024). Xpert: Empowering incident management with query recommendations via large language models. *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*,
- [34]. Jin, P., Zhang, S., Ma, M., Li, H., Kang, Y., Li, L., Liu, Y., Qiao, B., Zhang, C., Zhao, P., He, S., Sarro, F., Dang, Y., Rajmohan, S., Lin, Q., & Zhang, D. (2023). Assess and summarize: Improve outage understanding with large language models. *Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*,
- [35]. Jin, S., Bei, Z., Chen, B., & Xia, Y. (2025). Breaking the cycle of recurring failures: Generative AI and root cause analysis in legacy banking systems. 2025 IEEE/ACM International Workshop on Cloud Intelligence & AIOps (AIOps),

- [36]. Kazi Mohammad Khalid, A. (2026). A Systematic Review of GeoAI and Deep Learning for Automated Road Infrastructure Damage Detection Using Satellite Imagery. *American Journal of Data Science and Analytics*, 7(03), 208-255. <https://doi.org/10.63125/77cy0h19>
- [37]. Kazi Rakib Hasan, S., & Adnan, S. (2022). Quantitative Assessment of Machine Learning-Based Schedule Risk Prediction for Reducing Delays in Complex Technology Projects. *Review of Applied Science and Technology*, 1(04), 464-501. <https://doi.org/10.63125/dn8nkm85>
- [38]. Kohl, L., Eschenbacher, S., Besinger, P., & Ansari, F. (2024). Large language model-based chatbot for improving human-centricity in maintenance planning and operations. PHM Society European Conference,
- [39]. Kumari, P., & Kaur, P. (2021). A survey of fault tolerance in cloud computing. *Journal of King Saud University: Computer and Information Sciences*, 33(10), 1159-1176. <https://doi.org/10.1016/j.jksuci.2018.09.021>
- [40]. Landauer, M., Onder, S., Skopik, F., & Wurzenberger, M. (2023). Deep learning for anomaly detection in log data: A survey. *Machine Learning with Applications*, 12, 100470. <https://doi.org/10.1016/j.mlwa.2023.100470>
- [41]. Le, V.-H., & Zhang, H. (2021). Log-based anomaly detection without log parsing. 2021 36th IEEE/ACM International Conference on Automated Software Engineering (ASE),
- [42]. Le, V.-H., & Zhang, H. (2022). Log-based anomaly detection with deep learning: How far are we? Proceedings of the 44th International Conference on Software Engineering,
- [43]. Lee, C., Yang, T., Chen, Z., Su, Y., & Lyu, M. R. (2023). Eadro: An end-to-end troubleshooting framework for microservices on multi-source data. Proceedings of the 45th IEEE/ACM International Conference on Software Engineering,
- [44]. Lin, C.-M., Chang, C., Wang, W.-Y., Wang, K.-D., & Peng, W.-C. (2024). Root cause analysis in microservice using neural Granger causal discovery. Proceedings of the AAAI Conference on Artificial Intelligence,
- [45]. Loumachi, F. Y., Ghanem, M. C., & Ferrag, M. A. (2025). Advancing cyber incident timeline analysis through retrieval-augmented generation and large language models. *Computers*, 14(2), 67. <https://doi.org/10.3390/computers14020067>
- [46]. Mahbulul, I., Mahmudul, I., Shifa, T., Mahfuza, T., & Shima Ali, S. (2022). Exploring The Potential of Visual Narratives and Interactive Gamified Communication Systems to Prevent Disease, Counter Health Misinformation, And Strengthen Public Trust in Low-Literacy Communities: A Literature Review. *American Journal of Interdisciplinary Studies*, 3(02), 165-220. <https://doi.org/10.63125/zmq4n64>
- [47]. Mahfuj Ahmed, R. (2026). AI-Assisted Credit Evaluation Models for Improving Risk Assessment Accuracy in U.S. Banking Systems. *American Journal of Interdisciplinary Studies*, 7(01), 387-425. <https://doi.org/10.63125/aa031j21>
- [48]. Md Anisur Rahman, M. (2024). State Income Tax Differentials and High-Skilled Labor Mobility in The United States: A Time Series Analysis. *American Journal of Interdisciplinary Studies*, 5(04), 222-267. <https://doi.org/10.63125/295bsn47>
- [49]. Md Anisur Rahman, M. (2025). The Role of AI-Enabled Business Intelligence in Financial Risk Assessment and Liquidity Monitoring. *Review of Applied Science and Technology*, 4(04), 195-246. <https://doi.org/10.63125/p4eezd93>
- [50]. Md Anisur Rahman, M. (2026). AI-Driven Business Intelligence for Real-Time Fraud Risk Monitoring in Digital Payment Platforms: A Framework-Based Review. *International Journal of Scientific Interdisciplinary Research*, 7(1), 527-580. <https://doi.org/10.63125/0ef34271>
- [51]. Md Arif Uz, Z., Sharmin, S., & Md Abdur, R. (2025). Factors Influencing Behavioural Intention to Use he Innovative Open And Distance Learning Systems With The Role Of Continuance Intention. *American Journal of Scholarly Research and Innovation*, 4(01), 202-220. <https://doi.org/10.63125/pbjxp014>
- [52]. Md Ashfaq, S., & Abdullah Mohammad, S. (2022). CNT/PANI Composite Electrodes for Flexible Fiber-Shaped Dye-Sensitized Solar Cells: Synthesis, Characterization, and Photovoltaic Performance. *American Journal of Interdisciplinary Studies*, 3(02), 221-274. <https://doi.org/10.63125/m334mf41>
- [53]. Md Asif Ali Sheak, A., & Risha, A. (2022). The Role of IOT-Driven Energy Analytics in Improving Operational Efficiency and Sustainability in Modern Industrial Facilities. *American Journal of Interdisciplinary Studies*, 3(04), 807-841. <https://doi.org/10.63125/gm63q956>
- [54]. Md Asif Ali Sheak, A., & Tahmedur, R. (2023). A Data-Driven Framework for Engineering Project Risk Assessment Under Schedule and Cost Uncertainty. *International Journal of Scientific Interdisciplinary Research*, 4(2), 204-251. <https://doi.org/10.63125/kq4zzh16>
- [55]. Md Kaium, H. (2023). A GIS-Based Multi-Criteria Decision-Support and Land-Suitability Optimization Framework for Climate-Resilient Urban and Regional Planning. *American Journal of Data Science and Analytics*, 4(06), 43-103. <https://doi.org/10.63125/wvq0sx87>
- [56]. Md Kaium, H. (2024). Machine Learning Enhanced GIS And AHP Modeling for High-Resolution Flood-Susceptibility Prediction, Vulnerability Assessment, and Risk Classification. *Review of Applied Science and Technology*, 3(02), 92-140. <https://doi.org/10.63125/fz8hv245>
- [57]. Md Kaium, H. (2025). Integrating Artificial Intelligence, Semantic Indoor Geospatial Modeling, And Network-Based Routing for High-Precision NG911 Emergency Location Intelligence. *International Journal of Scientific Interdisciplinary Research*, 6(1), 616-670. <https://doi.org/10.63125/5hc1xx56>
- [58]. Md Kaium, H. (2026). An Artificial Intelligence Integrated Geospatial Decision-Support Framework for Scenario-Based Climate-Adaptive Land-Use Optimization and Environmental Risk Reduction. *American Journal of Data Science and Analytics*, 7(06), 425-483. <https://doi.org/10.63125/nyc7sh45>
- [59]. Md Mahamud Pervaz, P. (2023). Integration of MES, SAP, And PI Historian Platforms for Real-Time Industrial Asset Performance Management. *Review of Applied Science and Technology*, 2(04), 393-445. <https://doi.org/10.63125/9ebtas97>

- [60]. Md Mahamud Pervaz, P. (2025). Development of a CMMS-Integrated Predictive Maintenance Framework for Industrial PLC and Drive Systems. *American Journal of Scholarly Research and Innovation*, 4(01), 894-942. <https://doi.org/10.63125/j33gtf31>
- [61]. Md Mahamud Pervaz, P. (2026). Implementation of an OSHA-Compliant Lockout/Tagout and Arc-Flash Hazard Mitigation Framework for U.S. Industrial Maintenance Operations. *American Journal of Interdisciplinary Studies*, 7(02), 73-119. <https://doi.org/10.63125/8ky04n07>
- [62]. Md. Abdur, R., & Iftekhar, A. (2021). Customer Retention Forecasting in Mobile Wallet Services Using Neural Networks: A Comparative Quantitative Study. *International Journal of Business and Economics Insights*, 1(4), 70-102. <https://doi.org/10.63125/dyrpc387>
- [63]. Md. Rashedul, I., & Md Kaium, H. (2022). Development Of a Three-Dimensional Indoor Geospatial Network and Address Geocoding Framework for Next-Generation Emergency Dispatch and Response-Time Optimization. *Journal of Sustainable Development and Policy*, 1(02), 245-292. <https://doi.org/10.63125/tcw3mp48>
- [64]. Md. Shakhawat, H., & Md. F. (2024). Impact of Phishing Simulation Campaigns and Security Awareness Training on Human Risk Mitigation in Financial Institutions: A Quantitative Study. *American Journal of Data Science and Analytics*, 5(10), 48-85. <https://doi.org/10.63125/4j8h1484>
- [65]. Meng, W., Liu, Y., Zhu, Y., Zhang, S., Pei, D., Liu, Y., Chen, Y., Zhang, R., Tao, S., Sun, P., & Zhou, R. (2019). LogAnomaly: Unsupervised detection of sequential and quantitative anomalies in unstructured logs. *Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence*,
- [66]. Mohammad Abir Chowdhury, S. (2023). Role of AI-Assisted Risk Assessment in Enhancing Audit Planning Efficiency and Risk Prioritization in Public-Safety Organizations. *International Journal of Scientific Interdisciplinary Research*, 4(4), 529-576. <https://doi.org/10.63125/qd6nn437>
- [67]. Mohammad Abir Chowdhury, S. (2025). Application of Machine Learning and Anomaly-Detection Algorithms for Fraud Detection in U.S. Government Financial Operations. *American Journal of Interdisciplinary Studies*, 6(02), 139-184. <https://doi.org/10.63125/fkf19309>
- [68]. Mohammad Abir Chowdhury, S. (2026). Development Of a Machine-Learning Approach for Internal-Control Weakness Prediction and Audit-Risk Scoring In U.S. State Government Agencies. *American Journal of Data Science and Analytics*, 7(06), 380-424. <https://doi.org/10.63125/3v722074>
- [69]. Mohammad Abir Chowdhury, S., & Tonay, P. (2022). An Empirical Analysis of the Impact of Robotic Process Automation and Continuous Auditing on the Timeliness And Accuracy Of Financial Reporting Assurance. *International Journal of Business and Economics Insights*, 2(4), 73-126. <https://doi.org/10.63125/7p8dcr47>
- [70]. Mohammad Badrul, A. (2025). SCADA And IOT-Enabled Smart Water Metering: A Systematic Review of Resilient Supply Monitoring. *International Journal of Scientific Interdisciplinary Research*, 6(1), 576-615. <https://doi.org/10.63125/at8pnx81>
- [71]. Mohammad Badrul, A. (2026). A Machine-Learning Framework for Real-Time Non-Revenue Water Prediction in Aging Urban Distribution Networks. *American Journal of Interdisciplinary Studies*, 7(02), 01-52. <https://doi.org/10.63125/93km2h66>
- [72]. Mohammad Badrul, A., & Md. Mominul, H. (2023). Machine Learning-Based Assessment of Environmental and Public Health Risks in Sewerage Sludge Management Systems. *American Journal of Advanced Technology and Engineering Solutions*, 3(02), 33-77. <https://doi.org/10.63125/y3yfxa92>
- [73]. Mohammad Shoriful Hossan, S. (2022). A Performance-Based Framework for Arc-Flash Hazard Reduction and Electrical Reliability Improvement in Brownfield Industrial Distribution Systems. *Review of Applied Science and Technology*, 1(04), 447-463. <https://doi.org/10.63125/a70vj720>
- [74]. Molla Al Rakib, H., & Mohammad Towhidul, I. (2023). Cyber-Resilient Marketing Intelligence Systems for Fraud Detection and Data Integrity in Digital Campaigns. *American Journal of Scholarly Research and Innovation*, 2(02), 485-518. <https://doi.org/10.63125/b53pgr11>
- [75]. Mollik, R. H., Datta, A., Mollah, A. H., & Aljedaani, W. (2025). RCEGen: A generative approach for automated root cause analysis using large language models (LLMs). *Software*, 4(4), 29. <https://doi.org/10.3390/software4040029>
- [76]. Mst Kaniz, F. (2022). Language Access and Health Equity: Role of Multilingual Administrative Staff in Reducing Healthcare Disparities Among South Asian Immigrant Communities in The U.S. *International Journal of Scientific Interdisciplinary Research*, 1(01), 274-315. <https://doi.org/10.63125/xqhss825>
- [77]. Mst Shamima, A. (2026). Enhancing Financial Accountability and Cost Control in North American Outpatient Clinics Through Data Science: A Mixed-Methods Healthcare Administration Study. *American Journal of Data Science and Analytics*, 7(05), 01-41. <https://doi.org/10.63125/wksqy749>
- [78]. Mukut Kanti, B. (2024). AI-Enabled Predictive Asset Integrity Monitoring for Industrial Equipment in Oil & Gas and Energy Sector Facilities. *International Journal of Scientific Interdisciplinary Research*, 5(2), 746-791. <https://doi.org/10.63125/3mjcah04>
- [79]. Mukut Kanti, B. (2026). Digital-Twin And IOT-Based Condition Monitoring for Rotating Machinery and Process Equipment in Petrochemical and Industrial Environments. *American Journal of Scholarly Research and Innovation*, 5(01), 382-428. <https://doi.org/10.63125/mwdnqv55>
- [80]. Murad, M. D. H. R. (2026). Artificial Intelligence-Driven Enterprise Decision Support Systems: A Framework for Intelligent Business Process Automation in Digital Economies. *American Journal of Advanced Technology and Engineering Solutions*, 6(01), 332-373. <https://doi.org/10.63125/nnv83884>
- [81]. Nishat, J. (2023). Communicable Disease Prevention in a Post-Pandemic Era: A Global Review of Public Health Education, Surveillance, and Community-Level Interventions. *International Journal of Scientific Interdisciplinary Research*, 4(4), 630-678. <https://doi.org/10.63125/mnqefj36>

- [82]. Nishat, J. (2025). Leveraging Machine Learning to Identify and Address Maternal Health Disparities in Underserved U.S. Communities. *American Journal of Data Science and Analytics*, 6(12), 125-169. <https://doi.org/10.63125/c2t7r719>
- [83]. Nishat, J. (2026). Predictive Analytics for Program Effectiveness: A Machine Learning Approach to Health Education Programs in the United States. *American Journal of Health and Medical Sciences*, 7(03), 30-56. <https://doi.org/10.63125/2vw42878>
- [84]. Nishat, J., & Jahanara, A. (2024). Machine Learning Approaches for Early Prediction of High-Risk Pregnancy in Underserved U.S. Populations. *American Journal of Interdisciplinary Studies*, 5(04), 268-309. <https://doi.org/10.63125/5gh5df13>
- [85]. Nishat, J., & Mst Kaniz, F. (2022). A Review of the Impact of Covid-19 On Maternal and Child Health Service Utilization in Bangladesh. *American Journal of Scholarly Research and Innovation*, 1(02), 223-269. <https://doi.org/10.63125/vgv5s742>
- [86]. Notaro, P., Cardoso, J., & Gerndt, M. (2021). A survey of AIOps methods for failure management. *ACM Transactions on Intelligent Systems and Technology*, 12(6), Article 81. <https://doi.org/10.1145/3483424>
- [87]. Nuzhat Sadia, P. (2025). Integrating Business Intelligence Dashboards for Real-Time Supply Chain Visibility and Operational Decision Support. *American Journal of Data Science and Analytics*, 6(12), 170-216. <https://doi.org/10.63125/1es4f763>
- [88]. Nuzhat Sadia, P. (2026). An Integrated IT Management Framework for Scenario-Based Enterprise Analytics and Strategic Decision Optimization. *American Journal of Interdisciplinary Studies*, 7(02), 120-168. <https://doi.org/10.63125/3wtc3z49>
- [89]. Paduraru, C., Dumitru, B., & Stefanescu, A. (2025). Automated generation of cybersecurity response playbooks via large language models. *Procedia Computer Science*, 270, 2987-2996. <https://doi.org/10.1016/j.procs.2025.09.423>
- [90]. Palash Chandra, D. (2024). High-Performance Computing-Enabled Hydraulic and Flood Modeling for Urban Water Supply and Drainage Systems. *Journal of Sustainable Development and Policy*, 3(04), 245-286. <https://doi.org/10.63125/fcmas427>
- [91]. Pan, H., Zou, N., Wang, R., Ma, J., & Liu, D. (2025). Artificial intelligence usage and supply chain resilience: An organizational information processing theory perspective. *Systems*, 13(9), 724. <https://doi.org/10.3390/systems13090724>
- [92]. Rony, S., & Md, A. (2026). Multi-Agency Coordination in Sustained Healthcare Supply Shortages: Lessons from Covid-19, Drug Shortages, and Critical Medical Supply Disruptions. *American Journal of Data Science and Analytics*, 7(01), 181-221. <https://doi.org/10.63125/5v6t8515>
- [93]. Roy, D., Zhang, X., Bhawe, R., Bansal, C., Las-Casas, P., Fonseca, R., & Rajmohan, S. (2024). Exploring LLM-based agents for root cause analysis. Companion Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering,
- [94]. Rukaiya Khatun, M. (2026). Machine Learning-Based Transaction Risk Scoring Models for Financial Compliance Monitoring in Foreign Exchange Operations. *International Journal of Scientific Interdisciplinary Research*, 7(1), 172-203. <https://doi.org/10.63125/0nbg6w69>
- [95]. Sadia, Z. (2025). Predictive Analytics for Financial Performance Forecasting and Reporting Quality: Evidence from Data-Driven Financial Management Systems. *ASRC Procedia: Global Perspectives in Science and Scholarship*, 1(01), 2795-2812. <https://doi.org/10.63125/zstqn346>
- [96]. Shaiful, M., Anisur, R., & Md, A. (2022). A Systematic Literature Review on the Role of Digital Health Twins in Preventive Healthcare For Personal and Corporate Wellbeing. *American Journal of Interdisciplinary Studies*, 3(04), 1-31. <https://doi.org/10.63125/negjw373>
- [97]. Shamsul, A. (2026). Electrical Engineering Approaches for AI-Enabled Autonomous Robotics in U.S. Industrial and Defense Applications. *International Journal of Scientific Interdisciplinary Research*, 7(1), 72-110. <https://doi.org/10.63125/h255cq52>
- [98]. Shetty, M., Bansal, C., Upadhyayula, S. P., Radhakrishna, A., & Gupta, A. (2022). AutoTSG: Learning and synthesis for incident troubleshooting. Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering,
- [99]. Soldani, J., & Brogi, A. (2023). Anomaly detection and failure root cause analysis in (micro)service-based cloud applications: A survey. *ACM Computing Surveys*, 55(3), Article 59, 51-39. <https://doi.org/10.1145/3501297>
- [100]. Soldani, J., Forti, S., Roveroni, L., & Brogi, A. (2025). Explaining microservices' cascading failures from their logs. *Software: Practice and Experience*, 55(5), 809-828. <https://doi.org/10.1002/spe.3400>
- [101]. Srinivasan, R., & Swink, M. (2015). Leveraging supply chain integration through planning comprehensiveness: An organizational information processing theory perspective. *Decision Sciences*, 46(5), 823-861. <https://doi.org/10.1111/deci.12166>
- [102]. Srinivasan, R., & Swink, M. (2018). An investigation of visibility and flexibility as complements to supply chain analytics: An organizational information processing theory perspective. *Production and Operations Management*, 27(10), 1849-1867. <https://doi.org/10.1111/poms.12746>
- [103]. Sterbenz, J. P. G., Hutchison, D., Çetinkaya, E. K., Jabbar, A., Rohrer, J. P., Schöller, M., & Smith, P. (2010). Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. *Computer Networks*, 54(8), 1245-1265. <https://doi.org/10.1016/j.comnet.2010.03.005>
- [104]. Toffetti Carughi, G., Brunner, S., Blöchliger, M., Spillner, J., & Bohnert, T. M. (2017). Self-managing cloud-native applications: Design, implementation, and experience. *Future Generation Computer Systems*, 72, 165-179. <https://doi.org/10.1016/j.future.2016.09.002>

- [105]. Tonay, P. (2025). Machine Learning for Fraud Detection in Enterprise Financial Systems. *American Journal of Advanced Technology and Engineering Solutions*, 1(02), 304-318. <https://doi.org/10.63125/d0fhp873>
- [106]. Tonay, P. (2026). The Role of AI-Based Decision Support in Financial Risk Management and Anomaly Detection. *American Journal of Data Science and Analytics*, 7(06), 327-359. <https://doi.org/10.63125/wnb54w77>
- [107]. Tonay, P., Md Maruf, I., & Al, A. (2024). Artificial Intelligence-Based Decision Support Systems and Managerial Performance. *American Journal of Advanced Technology and Engineering Solutions*, 4(04), 154-184. <https://doi.org/10.63125/wmz8dc67>
- [108]. Uddin, H. M. M., & Risha, A. (2024). Hybrid Cloud Security and Compliance in U.S. Enterprises: Addressing Data Privacy Risks and Governance Challenges. *American Journal of Scholarly Research and Innovation*, 3(01), 153-197. <https://doi.org/10.63125/qcy0cj46>
- [109]. Wu, L., Tordsson, J., Elmroth, E., & Kao, O. (2020). MicroRCA: Root cause localization of performance issues in microservices. NOMS 2020: 2020 IEEE/IFIP Network Operations and Management Symposium,
- [110]. Xie, X., Wu, Y., Palacios-Marqués, D., & Ribeiro-Navarrete, S. (2022). Business networks and organizational resilience capacity in the digital age during COVID-19: A perspective utilizing organizational information processing theory. *Technological Forecasting and Social Change*, 177, 121548. <https://doi.org/10.1016/j.techfore.2022.121548>
- [111]. Xin, R., Chen, P., & Zhao, Z. (2023). CausalRCA: Causal inference based precise fine-grained root cause localization for microservice applications. *Journal of Systems and Software*, 203, 111724. <https://doi.org/10.1016/j.jss.2023.111724>
- [112]. Xu, W., Huang, L., Fox, A., Patterson, D., & Jordan, M. I. (2009). Detecting large-scale system problems by mining console logs. Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles,
- [113]. Yin, Q., Wang, Y., Song, D., Lai, F., Collins, B., & Guo, H. (2024). The impact of digitalization on operational risk: An organizational information processing perspective. *International Journal of Production Economics*, 276, 109369. <https://doi.org/10.1016/j.ijpe.2024.109369>
- [114]. Yu, Q., Zhao, N., Li, M., Li, Z., Wang, H., Zhang, W., Sui, K., & Pei, D. (2024). A survey on intelligent management of alerts and incidents in IT services. *Journal of Network and Computer Applications*, 224, 103842. <https://doi.org/10.1016/j.jnca.2024.103842>
- [115]. Zhang, D., Zhang, X., Bansal, C., Las-Casas, P., Fonseca, R., & Rajmohan, S. (2024). LM-PACE: Confidence estimation by large language models for effective root causing of cloud incidents. Companion Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering,
- [116]. Zhang, L., Jia, T., Jia, M., Wu, Y., Liu, A., Yang, Y., Wu, Z., Hu, X., Yu, P. S., & Li, Y. (2025). A survey of AIOps in the era of large language models. *ACM Computing Surveys*, 58(2), Article 44, 41-35. <https://doi.org/10.1145/3746635>
- [117]. Zhang, T., Jiang, Z., Bai, S., Zhang, T., Lin, L., Liu, Y., & Ren, J. (2024). RAG4ITOps: A supervised fine-tunable and comprehensive RAG framework for IT operations and maintenance. Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing: Industry Track,
- [118]. Zhang, X., Ghosh, S., Bansal, C., Wang, R., Ma, M., Kang, Y., & Rajmohan, S. (2024). Automated root causing of cloud incidents using in-context learning with GPT-4. Companion Proceedings of the 32nd ACM International Conference on the Foundations of Software Engineering,
- [119]. Zhang, Z., Li, S., Zhang, L., Ye, J., Hu, C., & Yan, L. (2025). LLM-LADE: Large language model-based log anomaly detection with explanation. *Knowledge-Based Systems*, 326, 114064. <https://doi.org/10.1016/j.knosys.2025.114064>
- [120]. Zhou, Y., Chen, Y., Rao, X., Zhou, Y., Li, Y., & Hu, C. (2024). Leveraging large language models and BERT for log parsing and anomaly detection. *Mathematics*, 12(17), 2758. <https://doi.org/10.3390/math12172758>
- [121]. Zhu, Y., Wang, J., Li, B., Zhao, Y., Zhang, Z., Xiong, Y., & Chen, S. (2024). MicroIRC: Instance-level root cause localization for microservice systems. *Journal of Systems and Software*, 216, 112145. <https://doi.org/10.1016/j.jss.2024.112145>