Journal of Cyber-Physical Security and Robotics
Volume 02, Issue 4, 55-76, 2026

Article

Advancements in Autonomous Incident Response: Integrating Large Language Models with Database Reliability Engineering Telemetry

Evans Ighodalo[1,*], Ayinoluwa Kolawale[2], Chukwudera Obumneke Anunagba[3], Oluranti Ogundapo[4], Harouna Wendpanga Yann Christian Sankara[5], Emmanuel Chukwuma Okeke[6], Aisha Ife Abdulwahab[7], Toussida Fatah Tanguy Minoungou[8]

[1]*Grand Canyon University, United States; ighodaloevans4@gmail.com*
[2]*Underdog Fantasy, USA; ayinoluwak@gmail.com*
[3]*Barclays, Whippany, New Jersey, USA; chiokemuo@gmail.com*
[4]*GTA, Nokia–Verizon Wireless Project, Canada; ogundapooluranti@gmail.com*
[5]*State of Missouri, Office of Administration, Information Technology Services Division, Jefferson City, Missouri, USA; christiansankara@gmail.com*
[6]*Arcesium, USA; emmanuelokeke68@gmail.com*
[7]*Cummins Inc., Indiana, USA; ifewahab@gmail.com*
[8]*Nationwide, Columbus, Ohio, USA; tanguyminoungou@gmail.com*

[*]Corresponding author: ighodaloevans4@gmail.com

Received: 24th September, 2026 Accepted: 10th October, 2026 Publication: 25th October, 2026

Abstract

Database incidents remain one of the most expensive classes of production failure, because the database sits beneath almost every user-facing service and its failure modes (lock contention, replication lag, plan regressions, storage exhaustion, connection storms) cascade quickly. Over the past decade, autonomous database research has largely concentrated on tuning and optimization, while incident response has stayed a human-centred discipline supported by dashboards and alerting. The arrival of capable large language models (LLMs) that can call tools, read heterogeneous telemetry and follow written procedures has changed this picture. Using an integrative literature review of 228 sources, comprising 18 core studies from the database systems, software engineering and AIOps literature and 210 seed studies screened from a consolidated corpus of 1,056 records, combined with conceptual modelling, this paper synthesizes the trajectory from self-tuning systems to LLM-assisted diagnosis and develops a conceptual model that couples Database Reliability Engineering (DRE) telemetry with an LLM reasoning agent inside a closed control loop. The architecture is organized around four ideas: an incident packet that compresses raw signals into a form an LLM can reason over; retrieval of operational knowledge such as runbooks and past postmortems; graded autonomy enforced by policy rather than by the model; and verification against service level objectives with automatic rollback. We present a taxonomy of database telemetry for LLM consumption, a five-level autonomy model for remediation, and an evaluation protocol with metrics that go beyond diagnostic accuracy to include time to mitigation, unsafe action rate and operator trust. The paper discusses implications for practice, research and governance, states the limitations of a conceptual review, and sets out a future research agenda covering telemetry hallucination, adversarial content in logs, evaluation realism and the shifting role of the database engineer.

Keywords: autonomous databases; integrative review; conceptual model; incident response; large language models; AIOps; database reliability engineering; observability; root cause analysis; agentic systems; human in the loop

DOI: 10.64235/bgd7kswx8

© *Journal of Cyber-Physical Security and Robotics*

1. Introduction

Modern organizations run fleets of databases that span managed cloud services, self-hosted relational engines, distributed SQL systems and specialized stores. Each instance emits a continuous stream of metrics, logs, wait events, query statistics and configuration changes. When something goes wrong, an on-call engineer must turn that stream into a diagnosis and a safe corrective action, often at night and under time pressure. The quality of the response depends heavily on the experience of whoever holds the pager, and on how well institutional knowledge has been written down. Studies of enterprise IT operations repeatedly find that service assurance at scale depends on standardized support processes, disciplined incident and problem management, and measurable service quality (Anyanwu, 2019; Anyanwu, 2020; Ladapo et al., 2023a; Ladapo et al., 2023c; Olagunju et al., 2025; Oteri and Edivri, 2026; Oteri et al., 2025; Wikiri, 2021), and these findings apply with particular force to the data tier, where a single degraded instance can affect every dependent application (Edivri and Oteri, 2024; Olagunju et al., 2024; Oteri and Edivri, 2024).

Autonomous database administration has been an explicit research goal at least since the self-driving database vision of Pavlo et al. (2017) and the machine learning based tuning of OtterTune (Van Aken et al., 2017). Commercial offerings such as Oracle Autonomous Database and the automatic tuning features of major cloud providers demonstrated that indexing, memory sizing and patching could be automated for many workloads. However, those systems mostly address steady-state optimization. Incident response is different: it is rare, high stakes, poorly labelled, and frequently caused by interactions between the database and the surrounding system, such as a deployment that changes a query shape or a network partition that triggers failover. Related work on cloud resource scaling, virtual machine placement, constraint-based network allocation, rightsizing and the computational complexity of cloud database optimization shows how far automation has progressed for capacity problems (Ahmed and Odejobi, 2018b; Ahmed et al., 2019; Ahmed et al., 2020; Odejobi et al., 2019; Upreti and Oteri, 2023), and predictive capacity planning models extend the same ideas to portfolio level forecasting (Edivri and Oteri, 2022; Olagunju et al., 2022). Capacity automation, however, operates on slow and well-measured signals, whereas incidents demand fast reasoning under uncertainty.

Large language models offer a plausible bridge. They can read unstructured logs and runbooks, form and test hypotheses through tool calls, and explain their reasoning in natural language that an operator can audit. Early work at Microsoft applied LLMs to cloud incident root cause and mitigation recommendation (Ahmed et al., 2023; Chen et al., 2024), and database-specific systems such as D-Bot (Zhou et al., 2024) and Panda (Singh et al., 2024) showed that LLM agents can diagnose database anomalies when grounded in metrics and expert knowledge. The difficulty is that a fluent model is not automatically a reliable operator. Controlled studies of LLM failure modes in multi-turn reasoning (Nwakamma et al., 2026a), reviews of hallucination in retrieval augmented systems (Ajala et al., 2026a) and analyses of attacks on agentic enterprise workflows (Nwakamma et al., 2024b) all indicate that model output must be checked before it is trusted, a conclusion consistent with the broader human-in-the-loop machine learning literature (Ladapo et al., 2022a; Ladapo et al., 2024b; Ladapo et al., 2026). The central question of this paper is therefore not whether LLMs can talk about database incidents, but how they should be integrated with DRE telemetry and controls so that autonomy increases safely.

Our contributions are as follows:

- an integrative synthesis of nine research streams that converge on LLM-assisted database incident response;
- a taxonomy of DRE telemetry organized by how useful and how risky each signal is when exposed to an LLM;
- a closed-loop reference architecture in which the model proposes and explains, while policy, verification and humans decide what is executed;
- a graded autonomy model, five research propositions and a validation pathway that measures safety and operational outcomes, not only diagnostic accuracy;
- a discussion of implications for practitioners, researchers and regulators, together with an explicit statement of limitations and a future research agenda.

The remainder of the paper is organized as follows. Section 2 describes the research method. Section 3 presents the results and discussion, comprising the literature synthesis, the conceptual model, the discussion of findings, the implications and the limitations

Table 1: Screening of the consolidated seed corpus

Stage	Subject areas	Records
Consolidated seed corpus	69	1,056
Excluded at subject-area level as unrelated	46	690
Screened by title and abstract	23	366
Excluded at record level		156
Seed studies retained and cited	23	210
Core studies added purposively		18
Total sources in the review		228

of the study. Section 4 concludes the paper and sets out directions for future research.

2. Research Method

2.1 Research design

This study adopts an integrative literature review combined with conceptual model development. An integrative review is appropriate when a topic draws on several disciplines that use different vocabularies and methods, and when the aim is to generate a new framework rather than to estimate a pooled effect. LLM-assisted database incident response sits at the intersection of database systems, site reliability engineering, security operations, IT service management, reliability engineering and AI governance, so a narrowly scoped systematic review restricted to a single field would miss much of the relevant evidence. The review was guided by three questions: (RQ1) which research streams inform autonomous incident response for databases; (RQ2) what architectural and governance elements are required to integrate LLMs safely with DRE telemetry; and (RQ3) how should such systems be evaluated.

2.2 Source identification and selection

Sources were drawn from two pools. The first was a purposive core set of 18 widely cited studies from database systems, software engineering and AIOps venues (for example SIGMOD, VLDB, CIDR, ICSE, EuroSys, MLSys and NeurIPS) and two standard reliability engineering texts, selected because they define the state of the art in database tuning, database diagnosis and LLM-based incident management. The second was a consolidated seed corpus of 1,056 peer-reviewed and preprint records organized into 69 subject areas. Screening of the seed corpus proceeded in two stages, summarized in Table 1. At the first stage, 46 subject areas with no plausible connection to the research questions (for example agricultural economics, nursing practice and livestock nutrition) were excluded. At the second stage, the titles and, where needed, the abstracts of the 366 records in the remaining 23 subject areas were screened against the inclusion criteria below.

- **Inclusion:** the study addresses monitoring, anomaly detection, incident or problem management, automated response, cloud or data infrastructure, identity and configuration governance, or the governance of AI systems; or
- **Inclusion:** the study addresses an analogous problem in another domain (such as predictive maintenance or fraud detection) whose methods are transferable to database operations.
- **Exclusion:** studies concerned primarily with administrative systems, marketing, physical sciences or domain topics with no transferable method for operational reliability.

Retained seed studies were classified as directly related when they addressed incident response, operational telemetry, cloud and IT operations or AI governance, and as semi-related when their contribution was methodological analogy. The largest contributing subject areas were enterprise IT systems, cloud and service management (29 studies), cybersecurity, data governance and IT risk (22), enterprise cyber defence engineering (22), operational technology security (19), IT service delivery and security operations (17), applied AI systems and model governance (15) and technology law and AI governance (13). All retained sources were published between 2016 and 2026.

2.3 Analysis and synthesis

Each source was coded for its domain, the operational problem addressed, the mechanism proposed (for example detection model, orchestration pattern, governance control or evaluation method) and its relevance to the three research questions. Codes were

grouped inductively into nine research streams, which structure the literature synthesis in Section 3.1. Where several studies offered similar findings, they were synthesized together and cited as a group, so that each paragraph of the synthesis represents a pattern in the literature rather than a summary of a single study.

2.4 Conceptual model development

The conceptual model in Section 3.2 was derived by mapping recurring mechanisms from the synthesis onto the stages of the incident lifecycle: detection, context assembly, diagnosis, planning, authorization, execution and verification. Mechanisms that appeared in multiple independent streams, such as closed-loop verification, graded autonomy and evidence-linked explanation, were treated as core design principles. The model was then expressed as a reference architecture, a telemetry taxonomy, an autonomy scale and a set of testable propositions. Because the model is conceptual, Section 3.3.1 specifies how it can be validated empirically, and Section 3.5 discusses the limitations of this approach.

3. Results and Discussion

This section reports the results of the review and discusses them. Section 3.1 presents the literature synthesis that answers RQ1. Section 3.2 presents the conceptual model that answers RQ2. Section 3.3 discusses the findings and sets out the validation pathway that answers RQ3. Sections 3.4 and 3.5 present the implications and limitations of the study.

3.1 Literature Synthesis

3.1.1 From self-tuning to autonomous databases

The first generation of database automation relied on advisors and rules, such as index and statistics advisors bundled with commercial engines. The second generation applied machine learning to configuration tuning, using Bayesian optimization and workload mapping (Van Aken et al., 2017) or reinforcement learning (Zhang et al., 2019) to search large knob spaces. Self-driving designs extended this to forecasting workloads and planning actions ahead of time (Pavlo et al., 2017). More recently, LLMs have been applied to tuning itself, for example by extracting tuning hints from manuals and forums (Lao et al., 2024) or by prompting models with workload summaries to propose configurations (Giannakouris and Trummer, 2025). These systems established that a database can safely change its own configuration under bounded conditions, which is a precondition for autonomous remediation.

3.1.2 Database reliability engineering and telemetry

Database Reliability Engineering adapts site reliability engineering principles to data stores: service level objectives, error budgets, blameless postmortems, automation of toil and treating infrastructure as code (Beyer et al., 2016; Campbell and Majors, 2017). DRE practice has produced rich telemetry. Engines expose wait event and session data (for example PostgreSQL pg_stat_activity and pg_stat_statements, MySQL Performance Schema, Oracle Active Session History), query plans, lock graphs, replication status and storage metrics. Observability standards such as OpenTelemetry increasingly carry database spans inside distributed traces, linking a slow request at the application edge to a specific statement. Prior diagnostic systems mined this data with statistical and causal methods, including DBSherlock (Yoon et al., 2016), which explains performance anomalies through predicates over metrics, and iSQUAD (Ma et al., 2020), which clusters slow queries to their root causes.

3.1.3 LLMs in incident management

AIOps research has moved from anomaly detection and alert correlation toward LLM-driven failure management (Zhang et al., 2024). In cloud incident management, fine-tuned and prompted LLMs have been evaluated for generating root cause and mitigation suggestions from incident descriptions (Ahmed et al., 2023), while RCACopilot combined automated diagnostic handlers with an LLM that predicts root cause categories and writes explanations (Chen et al., 2024). Xpert generated KQL queries to support incident investigation (Jiang et al., 2024). In the database domain, D-Bot organized expert knowledge from documentation and used tree-search style reasoning with multiple collaborating agents to diagnose anomalies (Zhou et al., 2024), and Panda argued that grounding, verification and feedback are essential for LLM debugging of databases (Singh et al., 2024). General agent techniques such as ReAct, which interleaves reasoning with actions (Yao et al., 2023), and retrieval augmented generation (Lewis et al., 2020) underpin most of these systems.

3.1.4 Lessons from security operations and automated response

Security operations has travelled the path from alerting to automated response earlier than database oper-

ations, and its literature offers transferable patterns. Log analytics pipelines feeding automated incident response (Mbonu et al., 2019b), security orchestration and automation models that shorten detection and response times (Dosunmu and Ogundele, 2025c), integrated network and security operation centres (Ladapo et al., 2024a), and AI-driven SOC architectures that fuse threat intelligence with behavioural analytics (Adegbite et al., 2024b) all describe the same loop of detection, enrichment, decision and containment that this paper applies to database incidents. Work on incident response and digital forensics for rapid containment (Dosunmu and Ogundele, 2021), intrusion detection and prevention (Ajagbe et al., 2025; Dosunmu and Ogundele, 2020), security analytics for enterprise risk (Ogbole et al., 2025) and the evolving threat landscape (Hussain and Adebayo, 2026; Okoruwa et al., 2024) emphasizes that response speed must be balanced against evidence preservation, a tension that also arises when an autonomous agent terminates database sessions or restarts replicas.

The security literature is also instructive on knowledge integration and continuous validation. Threat intelligence integration frameworks (Dosunmu and Ogundele, 2022; Dosunmu and Ogundele, 2026b), threat actor analysis (Dosunmu and Ogundele, 2023) and LLM embedding based de-duplication of shared indicators (Adebayo et al., 2026) parallel the retrieval of past incidents and runbooks proposed in Section 3.2. Breach and attack simulation, continuous security validation, threat-informed defence engineering, adversary simulation and deception architectures (Dosunmu and Ogundele, 2024a; Dosunmu and Ogundele, 2024c; Dosunmu and Ogundele, 2024d; Dosunmu and Ogundele, 2025a; Dosunmu and Ogundele, 2026a; Dosunmu and Ogundele, 2026c) show how controls can be tested continuously rather than trusted on paper, while cyber defence performance measurement and risk quantification frameworks (Dosunmu and Ogundele, 2024b; Dosunmu and Ogundele, 2025b) demonstrate how to report outcomes to executives. Deep learning approaches to autonomous threat detection in software engineering (Odejobi et al., 2025) and malware classification in cloud native microservices (Idika et al., 2021) further illustrate how learned models are being embedded into operational pipelines.

3.1.5 Cloud governance, identity and configuration control

Many database incidents originate in the cloud control plane rather than in the engine itself. Continuous misconfiguration monitoring (Aliliele et al., 2023a), infrastructure as code governance for Terraform deployments (Mbonu et al., 2020c) and blockchain-anchored audit trails for configuration management (Oshoba et al., 2020) offer mechanisms for detecting and attributing the configuration changes that so often precede an outage. Identity and access governance across hybrid, multi-cloud and federated environments (Mbonu et al., 2020a; Mbonu et al., 2022c; Oshoba et al., 2019), identity-centric zero trust (Ogbole et al., 2021a) and integrated governance of human and machine identities (Edivri et al., 2026) and privacy-driven access control policies (Ladapo et al., 2023d) are directly relevant to the scoped, short-lived credentials an autonomous agent should use. Studies of resilient cloud network architectures, secure messaging platforms, multi-cloud SaaS scaling and software-defined WAN deployments (Ahmed and Odejobi, 2018a; Ogunwola, 2026; Ukadike, 2024; Upreti and Oteri, 2025), together with research on cloud migration, firewall modernization and infrastructure consolidation during mergers (Fadero et al., 2025; Ladapo et al., 2022b; Ladapo et al., 2025; Ogunwola and Alozie, 2026b; Ogunwola et al., 2026), highlight the topological complexity in which database agents must operate.

3.1.6 IT service management and change control

Autonomous remediation must coexist with established IT service management. Governance models for change, incident and problem management in mission-critical environments (Olagunju et al., 2023), change management analytics (Oteri and Chibwaye, 2025), ServiceNow based orchestration (Ladapo et al., 2023a; Oteri et al., 2025) and KPI-driven service delivery frameworks (Edivri and Oteri, 2024) define the approval paths and records into which an LLM agent must write. Practical studies of directory services, their attack signatures and offline assessment of security-critical systems (Ladapo et al., 2018; Ladapo et al., 2019; Ladapo et al., 2023b), performance evaluation of multi-tenant collaboration platforms under high concurrency (Odejobi and Ahmed, 2018) and data-integrated ERP migration (Chibwaye and Oteri, 2023) add evidence on how operational knowledge is captured, and frequently lost, during large technology programmes.

3.1.7 Anomaly detection in operational technology and critical infrastructure

Industrial control systems offer a mature research base for anomaly detection in high-consequence environments. Systematic reviews of machine learning for threat detection in ICS and SCADA networks (Adebayo et al., 2023a; Adegbite et al., 2023), comparisons of LSTM, CNN and related architectures for SCADA anomaly detection (Amadi et al., 2025b), and autonomous continuously-learning frameworks for cyber-physical threat prevention (Amadi, 2025) address the same problem of separating genuine faults from noise in dense telemetry. Work on adversarial machine learning in critical infrastructure (Adebayo et al., 2022), physics-informed ransomware defence with digital twins (Ojukwu et al., 2023), the attack surface of legacy SCADA (Amadi et al., 2025c) and NTP amplification attacks (Jimoh and Ahmed, 2024) warns that the inputs to automated defences can themselves be manipulated. Governance architectures for OT security, IT and OT convergence, vulnerability management, cyber risk quantification, zero trust, NIST CSF posture management and continuous compliance (Adegbite et al., 2020; Adegbite et al., 2022; Adegbite et al., 2024a; Adegbite et al., 2025; Ahmed et al., 2021; Amadi et al., 2025a; Amadi, 2026), alongside research on substation resilience, secure SCADA data exchange, IoT-driven transportation security and national network resilience (Jimoh et al., 2023a; Ogunwola and Deborah, 2026; Shittu et al., 2022; Shittu et al., 2024), supply design principles for graded, auditable automation.

3.1.8 Predictive maintenance, reliability engineering and operational analytics

Reliability engineering in physical systems has long practised the shift from reactive to predictive operations that database teams now pursue. Predictive maintenance and condition monitoring in power infrastructure (Adaramola et al., 2018), vibration-based monitoring of rotating machinery (Omoegun et al., 2023), sensor-based fault detection in HVAC systems (Sunday and Omoegun, 2022), reliability-centred maintenance (Oyeleke et al., 2026), the transition from reactive to predictive maintenance (Sunday et al., 2020) and failure analysis in complex engineering systems (Gideon et al., 2019) provide conceptual vocabulary such as degradation signatures and maintenance windows. Data-driven maintenance in semiconductor fabs and lean predictive maintenance for deposition equipment (Olodo et al., 2026a; Olodo et al., 2026b), AI-based predictive maintenance for e-commerce platforms (Mayo et al., 2021), reliability simulation for large intermittent wireless infrastructures and predictive power management for IoT devices (Asiedu and Quainoo, 2023; Asiedu and Quainoo, 2024; Asiedu et al., 2026), and lifecycle performance management in infrastructure delivery (Adelanwa et al., 2023) show the same methods applied across domains.

Anomaly detection and early warning in business data offer further analogues. Conceptual models for anomaly detection in financial time series (Atakpa and Fobellah, 2023), adaptive real-time fraud risk scoring (Fadayomi et al., 2024), predictive analytics for anti-money laundering and fraud detection (Atakpa and Abetoh, 2022; Atakpa, 2021), AI-driven investigation support for analysts (Okoruwa et al., 2025) and predictive risk analytics for early-warning in enterprise technology estates (Okwesa et al., 2024) all confront class imbalance, concept drift and the need to explain alerts to humans. Real-time KPI tracking, integrated performance visualization, executive dashboards, performance intelligence for public services, AI decision support for operations planning, traffic forecasting and regression-based benchmarking of multi-site networks (Adelanwa et al., 2024a; Adelanwa et al., 2024b; Anene et al., 2023; Ogbole et al., 2021b; Oghenemaiga et al., 2024; Tonoyan et al., 2024; Walawalkar et al., 2025) inform the design of the operator-facing views described later.

3.1.9 Responsible AI governance and auditability

Finally, autonomous incident response falls within the scope of emerging AI governance. Reviews of algorithmic accountability and model risk management (Ominyi and Anichukwueze, 2023), responsible AI governance for automated decision systems in regulated industries (Ominyi and Anichukwueze, 2024), AI-assisted compliance monitoring (Ominyi et al., 2024a), readiness for the EU Artificial Intelligence Act (Ominyi et al., 2024b) and enterprise AI governance functions as institutional standards (Ominyi et al., 2026) define expectations for documentation, oversight and contestability. Responsible AI in IT auditing through evidence validation and human oversight (Elebe and Anunagba, 2025), AI-assisted continuous auditing (Aliliele et al., 2025a), implementation pathways from periodic audit to continuous control (Adebayo et al., 2025b), AI-enabled IT general controls (Mbonu et al., 2022a) and audits of AI-powered

Table 2: DRE telemetry classes and their role in LLM-assisted incident response

Telemetry class	Examples	Value to the model	Risks and handling
Resource metrics	CPU, IOPS, memory, disk latency, connections	Establishes symptoms and timing	Too dense; pass anomaly summaries and change points, not raw series
Wait events and sessions	Lock waits, I/O waits, active session samples	Points directly at contention class	Sampling bias; include sample counts and windows
Query statistics and plans	Top statements by time, plan hashes, plan changes	Explains regressions and hot spots	Statements may contain sensitive literals; normalize and redact
Logs and errors	Engine error log, slow query log, audit events	Captures failures not visible in metrics	Untrusted text; risk of prompt injection; quote, never obey
Replication and HA state	Lag, failover events, quorum status	Critical for data safety decisions	Stale reads; attach collection timestamps
Change and deploy history	Schema migrations, config changes, releases	Most incidents follow a change	Must be linked by time and service identity
Distributed traces	Database spans within request traces	Connects user impact to statements	High cardinality; pre-aggregate by endpoint
Operational knowledge	Runbooks, postmortems, architecture notes	Supplies local conventions and known fixes	May be outdated; rank by recency and outcome

financial systems (Fobellah, 2025) translate those expectations into control testing. Healthcare studies of AI governance, generative AI readiness and ethical adoption (Afrihyia et al., 2024; Afrihyia et al., 2025; Ekechi et al., 2026; Osinem et al., 2025), multi-agent quality control for regulated documents (Ominyi et al., 2025a), confidentiality in enterprise LLM deployment (Ominyi et al., 2025b), algorithmic accountability and anti-discrimination law (Annan, 2024; Annan, 2025a) and the role of business analysts as AI transformation brokers (Alieme et al., 2025b) complete the picture of the organizational conditions under which autonomy can be granted.

3.1.10 Synthesis of the literature

Read together, the nine streams converge on a small number of design principles. First, detection should remain deterministic and cheap, with learned models used for interpretation rather than for raising alarms. Second, operational knowledge such as runbooks, threat intelligence and past incidents is most useful when retrieved selectively and ranked by outcome. Third, automation is adopted successfully when it is graded, auditable and reversible, a pattern visible in security orchestration, OT security, IT service management and AI governance alike. Fourth, evaluation must measure operational outcomes and safety, not only accuracy.

Two gaps remain. First, most published systems stop at diagnosis or recommendation, leaving execution entirely to humans, so there is limited evidence about the safety of autonomous remediation. Second, evaluations typically report accuracy against labelled historical incidents, which says little about time to mitigation, the cost of a wrong action, or whether operators come to trust the system. The adjacent streams reviewed in Sections 3.1.4 to 3.1.9 offer methods for closing both gaps, and the conceptual model in Section 3.2 builds on them.

3.2 Conceptual Model

This section develops the conceptual model that answers RQ2. It is presented in four parts: a taxonomy of telemetry as model context, a closed-loop reference architecture, a graded autonomy scale, and a set of research propositions.

3.2.1 Telemetry as model context

An LLM cannot usefully read raw time series at production scale. A single busy cluster may produce millions of data points and gigabytes of logs during an incident window, far more than any context window, and most of it is noise. The integration problem is therefore largely a representation problem: what should the model see, in what form, and with what provenance? Table 2 summarizes the main telemetry classes from this perspective.

We propose that the telemetry layer emit an incident packet: a compact, structured document assembled when an alert fires. The packet contains the triggering SLO breach, a short list of anomalous signals with change points, the top statements and wait classes during the window compared with a baseline, recent changes ranked by temporal proximity, current topology and replication state, and links to raw data that the agent can query on demand. Each item carries a source and a timestamp so that every claim in the model output can be traced back to evidence. The

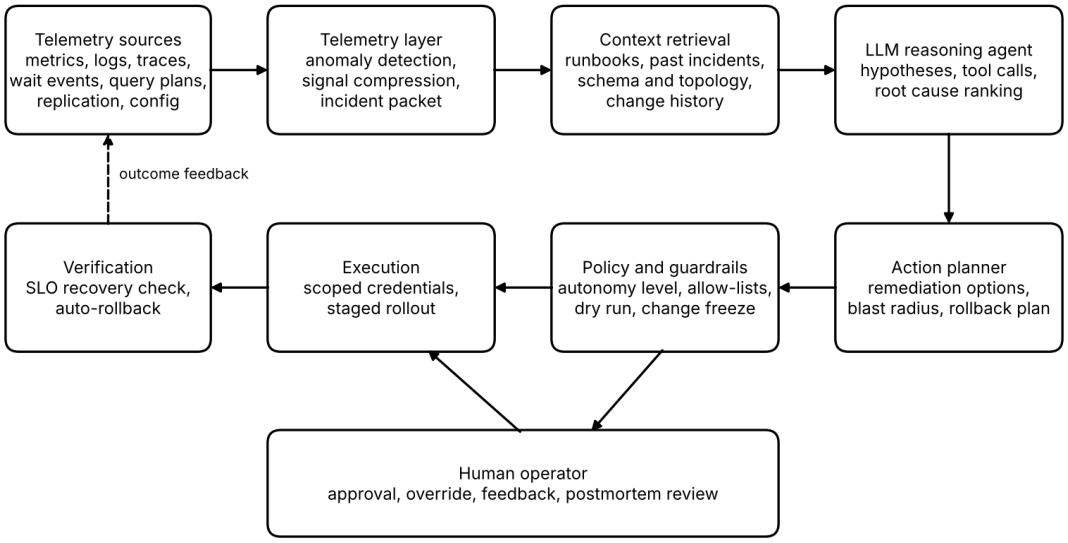


Figure 1: Closed-loop architecture for LLM-assisted database incident response

packet is deliberately small; the agent extends it through read-only tool calls rather than receiving everything up front.

Transport and integration choices shape what the packet can contain. Comparisons of Apache Kafka and WebSockets for real-time telemetry (Ajala et al., 2026b), modular event-driven messaging that unifies REST and WebSocket access (Sankara et al., 2026) and portable cloud-to-edge components built on WebAssembly (Ojukwu et al., 2025) suggest that a streaming backbone with on-demand query endpoints is the most practical design. ETL and integration patterns from enterprise CRM and ESB architectures (Badmus et al., 2019a; Badmus et al., 2022b) and integrated data management for forecasting (Agu et al., 2023b) provide reusable approaches to joining telemetry with change records and service catalogues.

Because the packet leaves the database boundary and may reach an external model, data governance is a first-order concern. Enterprise data sensitivity classification and regulatory traceability (Aliliele et al., 2024a), data lakehouse governance for loss prevention (Aliliele et al., 2025b), HIPAA-compliant secure analytics (Aliliele et al., 2024b), data protection impact assessment in multi-cloud systems (Mbonu et al., 2022b), comparative data protection regulation (Mbonu et al., 2019a) and legal and ethical risk modelling for data protection (Mbonu et al., 2018) supply the controls needed to classify and redact query literals and log content. Privacy-centric security engineering (Okoruwa et al., 2020), privacy-by-design role-based security (Badmus et al., 2024), health information governance (Peteranaba et al., 2022), cross-border data privacy governance (Annan, 2022), on-device privacy and zero-knowledge storage (Oyesiji et al., 2026b) and real-time compliance pipelines (Uchechi et al., 2022; Uchechi et al., 2025) reinforce the principle that redaction must happen before, not after, telemetry reaches the model.

3.2.2 Reference architecture

Figure 1 shows the proposed closed-loop architecture. Its organizing principle is a separation of concerns: the LLM is responsible for interpretation, hypothesis generation and explanation, while deterministic components own authorization, execution and verification.

3.2.3 Telemetry layer

Conventional detectors (thresholds, seasonal baselines, change point detection) remain the first line of defence because they are cheap, predictable and well understood. Their output, together with correlated signals, forms the incident packet described in Section 3.2.1. Keeping detection outside the LLM avoids paying inference cost for every data point and gives the system a stable trigger that does not depend on model behaviour.

3.2.4 Context retrieval

The agent retrieves runbooks, prior postmortems with similar signatures, schema and dependency information, and the change log. Retrieval should rank past incidents by both similarity and outcome, so that fixes that worked are preferred over fixes that were merely attempted. Embedding plan hashes, wait class profiles and error codes alongside text improves matching, because two incidents can be described very differently yet share the same technical fingerprint. Hallucination mitigation in retrieval augmented generation (Ajala et al., 2026a), context-aware curation of fine-tuning data (Oyesiji et al., 2024) and learned approaches to data wrangling and error detection (Ndupu et al., 2026b) indicate that the quality of the retrieval corpus matters as much as the model.

3.2.5 LLM reasoning agent

The agent follows a hypothesis-driven loop in the style of ReAct. It proposes candidate root causes, selects read-only diagnostic tools to discriminate between them (for example, inspecting the lock graph, comparing a current plan with a historical one, or checking replication lag on each replica), and updates its ranking as evidence arrives. Tool interfaces are typed and narrow; the agent calls functions such as get_top_waits(window) or explain_plan(statement_id) rather than receiving a general shell. This limits both errors and the damage a manipulated model could do. The agent output is a structured diagnosis containing ranked hypotheses, the evidence for and against each, a confidence estimate and the specific telemetry items cited.

Narrow tool interfaces are also the main defence against prompt injection, tool poisoning and memory manipulation, which recent work identifies as the principal threats to agentic enterprise workflows (Nwakamma et al., 2024b). Where data residency forbids hosted models, compressed on-device and small language models (Nwakamma et al., 2025; Oyesiji et al., 2025) can perform first-pass summarization close to the data. For complex incidents, multi-agent designs in which specialized agents coordinate, as in swarm coordination of autonomous robot fleets (Akanbi and Sunday, 2025; Akanbi et al., 2025) or multi-agent quality control of regulated documents (Ominyi et al., 2025a), offer a route to dividing diagnosis among storage, query and replication specialists.

3.2.6 Action planner

For the leading hypothesis the planner proposes one or more remediation options drawn preferentially from a catalogue of known, parameterized actions: terminate a blocking session, pin a previous query plan, scale read replicas, throttle a misbehaving client, roll back a configuration change, or fail over to a healthy replica. Each option is annotated with expected effect, blast radius, reversibility and a rollback procedure. Free-form actions generated by the model are permitted only at the lowest autonomy levels and always require human approval. The action catalogue is itself software and should be engineered as such: AI-assisted software testing and automated regression control (Borah et al., 2022; Mbonu et al., 2021c), CI/CD pipeline and version control governance (Badmus et al., 2018; Badmus et al., 2020; Badmus et al., 2022a), and hardware-in-the-loop and embedded CI validation (Ndupu et al., 2026a; Oyesiji et al., 2026a; Quainoo et al., 2025) provide practices for testing each remediation before it is admitted to the catalogue.

3.2.7 Policy, execution and verification

A policy engine, not the model, decides whether an action may run. Policies express the current autonomy level for the service, allow-lists of actions and targets, change freezes, required approvals and rate limits. Approved actions execute through short-lived, narrowly scoped credentials and, where possible, as staged rollouts beginning with a single instance or replica. After execution, a verification step checks whether the SLO indicators recover within an expected window. If they do not, or if new anomalies appear, the system rolls back automatically and escalates to a human with the full trace of evidence, reasoning and actions. Outcomes are written back to the incident store, improving future retrieval. Expressing policy as code follows the direction of real-time compliance pipelines and automated governance (Uchechi et al., 2022; Uchechi et al., 2025), risk-based internal control and audit models (Akomolafe and Agu, 2018; Akomolafe and Agu, 2019; Akomolafe et al., 2025a), cross-border SOX compliance frameworks (Agu et al., 2023a) and tamper-evident audit trails (Oshoba et al., 2020); API governance and risk prioritization frameworks (Aliliele et al., 2023b) and risk-based business intelligence architectures (Mbonu et al., 2021b) show how such policies can be prioritized by business impact.

Table 3: Autonomy levels for database incident remediation

Level	Name	System behaviour	Typical entry criteria
L0	Observe	Summarizes the incident and surfaces relevant runbooks; no diagnosis offered	Default for new services or new model versions
L1	Advise	Ranked root causes and suggested actions; humans execute everything	Diagnostic accuracy validated on historical replay
L2	Approve to act	Prepares exact commands and rollback; executes after explicit human approval	Low disagreement rate with on-call engineers over a trial period
L3	Act and notify	Executes catalogued, reversible actions within policy and notifies humans	Sustained record of safe execution at L2 for that action class
L4	Autonomous	Executes, verifies and closes routine incidents; escalates only exceptions	Reserved for low blast radius, fully reversible actions

3.2.8 Graded autonomy and governance

Autonomy should be earned per action class and per service, rather than switched on globally. Table 3 defines five levels, loosely analogous to driving automation levels. A fleet will typically operate at different levels for different actions at the same time; for example, cancelling a runaway analytical query may be fully autonomous, while failover remains at level 2.

Governance mechanisms support this model. Every decision is logged with its inputs, model version, prompts, tool results and policy evaluation, making postmortems possible when the system itself contributes to an incident. Promotion between levels should be based on measured outcomes and revisited whenever the model, prompts or tool catalogue change, because each of these can alter behaviour. Demotion should be automatic after an unsafe action or a failed verification. Finally, accountability remains with the human service owner; the system is a participant in the on-call rotation, not a substitute for ownership.

These mechanisms align with established governance research. Responsible AI structures for automated decision systems (Ominyi and Anichukwueze, 2024), institutional AI governance functions (Ominyi et al., 2026), EU AI Act readiness (Ominyi et al., 2024b) and evidence validation with human oversight in IT audit (Elebe and Anunagba, 2025) all require the traceability that decision logging provides. Human-in-the-loop research, including human-centred automated annotation and the disagreement problem in federated learning (Ladapo et al., 2022a; Ladapo et al., 2024b; Ladapo et al., 2026), informs how operator feedback should be weighted. Governance frameworks for AI-assisted CRM workflows and regulated platform management (Badmus et al., 2019b; Badmus et al., 2025), requirements engineering for AI-enabled automation (Alieme et al., 2024; Alieme et al., 2025a) and determinants of moving automation from pilot to scale (Dawud, 2026) describe the organizational readiness that promotion between autonomy levels presupposes.

Governance is also a matter of risk and assurance. Cybersecurity risk management and regulatory compliance frameworks for financial institutions (Bello et al., 2024), regulatory technology for transparency (Bello et al., 2025), cyber risk maturity assessed against national regulation (Fadero et al., 2021), risk-based assurance and data availability (Fadayomi et al., 2019), security audit and enterprise risk assessment (Dosunmu and Ogundele, 2019) and the role of frameworks in cybersecurity governance (Jimoh et al., 2023b) supply the assurance vocabulary. Evidence from healthcare on zero trust cost effectiveness, cyber risk pricing, secure distributed networks, cybersecurity investment returns and ransomware economics (Adebayo et al., 2023b; Adebayo et al., 2025a; Ogunwola and Alozie, 2026a; Ozowara et al., 2022; Ozowara et al., 2025), together with compliance as competitive advantage (Annan, 2025b), collaborative governance for secure data sharing (Akomolafe et al., 2025b), scalable blockchain gateway architectures (Akomolafe et al., 2024), attribute-based encryption for access control (Shittu and Nabil, 2023), agile transformation with embedded IT risk (Mbonu et al., 2020b) and forensic analytics for compliance monitoring (Mbonu et al., 2021a), illustrates how the cost of a wrong automated action can be quantified and insured against.

3.2.9 Research propositions

The model implies five propositions that future empirical work can test:

- **P1.** Presenting an LLM with a compact, provenance-linked incident packet yields higher diagnostic accuracy and fewer unsupported claims than presenting raw or unstructured

telemetry.

- **P2.** Retrieval ranked by remediation outcome reduces time to mitigation more than retrieval ranked by textual similarity alone.
- **P3.** Separating model reasoning from policy-based authorization reduces the unsafe action rate without a proportional loss in mitigation speed.
- **P4.** Automatic verification against SLO indicators with rollback lowers the severity of incidents caused by incorrect automated actions.
- **P5.** Graded, evidence-based promotion between autonomy levels increases operator trust and acceptance compared with a single global autonomy setting.

3.3 Discussion of Findings

The synthesis suggests that the main obstacle to autonomous database incident response is no longer the ability of models to reason about database behaviour. Systems such as D-Bot, Panda and RCACopilot already show useful diagnostic performance. The obstacle is integration: turning noisy, high-volume and sometimes sensitive telemetry into trustworthy evidence, and embedding model output into operational processes that preserve safety and accountability. The conceptual model therefore places most of its weight on components surrounding the model rather than on the model itself.

A second observation is that database operations can borrow heavily from adjacent fields. Security operations has already worked through the transition from alert triage to automated containment, and its experience with orchestration playbooks, continuous control validation and adversarial inputs maps closely onto the database setting. Operational technology security contributes a mature view of anomaly detection under high consequence, while IT service management supplies the change and problem records into which autonomous actions must be written. Reliability engineering in physical systems shows how predictive approaches gradually displace reactive ones once trust is established. These parallels support the principle of graded autonomy: in each field, automation expanded action class by action class, not all at once.

A third observation concerns the tension between speed and assurance. Greater autonomy shortens time to mitigation for routine incidents, but every additional control (policy checks, staged rollout, verification) adds latency. The model resolves this tension by making assurance proportional to risk: low blast radius, reversible actions move quickly, while irreversible or data-affecting actions such as failover retain human approval. This proportionality is consistent with the risk-based approaches found in the audit, compliance and AI governance literature reviewed in Section 3.1.9.

3.3.1 Pathway to empirical validation

Evaluating autonomous incident response is harder than evaluating diagnosis, because the consequences of actions unfold over time and depend on the environment. To answer RQ3 and test the propositions in Section 3.2.9, we recommend a three-stage protocol.

- **Historical replay.** Replay labelled historical incidents by reconstructing incident packets from archived telemetry, then score diagnoses and proposed actions against the postmortem. This is cheap and repeatable, but suffers from hindsight bias and from leakage if postmortems were used for retrieval.
- **Controlled fault injection.** Inject faults into staging or digital twin environments under realistic load: lock contention, index drops, plan regressions, disk filling, replica lag, connection pool exhaustion and misconfiguration. This allows the system to execute actions and be scored on recovery. Public benchmark efforts for AIOps agents, such as AIOpsLab (Chen et al., 2025), illustrate the approach.
- **Shadow mode in production.** Run the system at L0 or L1 alongside human responders in production, comparing its recommendations with what engineers actually did and how incidents resolved.

Table 4 lists the metrics we consider essential. The emphasis on safety and human factors reflects the asymmetric cost of errors: a slow but correct diagnosis is an inconvenience, whereas a confident wrong failover can cause data loss. LLM-as-a-judge methods and release gating for model governance (Nwakamma et al., 2024a) can scale the scoring of explanations, provided their own biases are controlled, while regression-based benchmarking (Anene et al., 2023), simulation-based process optimization (Tonoyan et al., 2022a) and predictive cost optimization (Tonoyan et al., 2022b) offer methods for estimating operational benefit. Cost governance in technolo-

Table 4: Recommended evaluation metrics

Dimension	Metric	Notes
Diagnosis	Top-1 and top-3 root cause accuracy; evidence citation precision	Citations must reference real telemetry items
Speed	Time to diagnosis; time to mitigation; reduction in MTTR versus baseline	Measure against human-only response on comparable incidents
Safety	Unsafe action rate; rollback rate; policy violations attempted	Attempted violations reveal model tendencies even when blocked
Calibration	Agreement between stated confidence and observed correctness	Enables confidence-based escalation thresholds
Robustness	Performance under missing telemetry, noisy logs and injected adversarial strings	Tests telemetry hallucination and prompt injection
Human factors	Operator acceptance rate, override rate, perceived workload, trust surveys	Collected during shadow mode and L2 operation
Cost	Inference cost per incident; tool calls per diagnosis	Compare with engineering hours saved

gy-intensive enterprises, predictive budgeting and AI-enabled financial analytics (Adesuyi et al., 2022; Adesuyi et al., 2023; Walawalkar et al., 2026) help translate reductions in time to mitigation into financial terms that justify investment.

3.4 Implications

3.4.1 Implications for practice

For database and reliability engineering teams, the model suggests a staged adoption path. Teams can begin at L0 and L1 by investing in the incident packet and in a curated, outcome-labelled incident store, which deliver value even before any automated action is permitted. Runbooks should be rewritten as parameterized, testable actions, because the quality of the action catalogue limits the safe level of autonomy. Credentials used by agents should be short-lived and narrowly scoped, and every agent action should be recorded in the existing change and incident management system so that it is visible to the same review processes as human actions.

3.4.2 Implications for research

For researchers, the review highlights the need to move beyond diagnostic accuracy on historical incidents. The propositions in Section 3.2.9 call for controlled experiments that measure time to mitigation, unsafe action rate and operator trust. The cross-domain synthesis also suggests that methods from security operations and OT anomaly detection deserve direct testing in database settings, and that shared fault injection environments for databases would make results comparable across studies.

3.4.3 Implications for governance and policy

For risk, audit and compliance functions, autonomous incident response creates a new category of automated decision that changes production systems. Organizations should define which action classes may be automated, who owns the policy, how decisions are logged and how autonomy is withdrawn after a failure. Where telemetry contains personal data, redaction and data residency controls must be in place before telemetry is sent to a model. Regulators and standards bodies may find the autonomy scale useful as a common vocabulary for describing how much control an AI system has over critical data infrastructure.

3.5 Limitations

This study has several limitations. First, it is an integrative rather than a systematic review. Core sources were selected purposively, and seed studies were drawn from a single consolidated corpus rather than from exhaustive searches of bibliographic databases, so relevant work may have been missed. Second, screening and thematic coding were performed by judgement against stated criteria, without independent double coding, which introduces a risk of selection and interpretation bias. Third, many seed studies are conceptual frameworks or reviews rather than empirical evaluations, and a substantial share were published in a small number of journals, which limits the strength of evidence they provide. Fourth, the semi-related streams were included as methodological analogies, and their transferability to database operations is argued rather than demonstrated. Finally, the conceptual model and propositions have not yet been tested empirically, and the field is evolving quickly, so specific technical details may date rapidly.

4. Conclusion

Autonomous database administration has matured from configuration tuning toward the harder problem of incident response. Large language models contribute something earlier automation lacked: the ability to combine heterogeneous telemetry, written operational knowledge and step-by-step investigation into an explanation a human can check. Their weaknesses, including hallucination, susceptibility to manipulated input and poorly calibrated confidence, mean that they should not be given unrestricted control. The architecture proposed here places the model inside a loop where telemetry is curated into evidence, actions come from a reviewed catalogue, policy decides what runs, and verification confirms recovery or triggers rollback. Combined with graded autonomy and an evaluation protocol focused on safety and outcomes, this approach offers a practical path for organizations in 2026 and beyond to reduce time to mitigation while keeping database engineers firmly accountable for the systems they operate.

4.1 Future Research

The synthesis and the limitations above point to the following priorities for future research.

- **Telemetry hallucination.** Models can assert metric values or events that do not appear in the data. Requiring every factual claim to cite a telemetry item, and validating citations mechanically, reduces but does not eliminate this risk (Ajala et al., 2026a; Nwakamma et al., 2024a; Nwakamma et al., 2026a).
- **Adversarial content in telemetry.** Logs, query text and error messages can contain attacker-controlled strings. If these are placed in the model context without isolation, an attacker could steer diagnosis or actions. Telemetry must be treated strictly as data, and execution authority must sit outside the model (Adebayo et al., 2022; Adeniyi et al., 2025; Nwakamma et al., 2024b).
- **Privacy and data governance.** Telemetry may contain personal data in query literals, connection metadata and logs. Redaction, data residency rules and decisions about whether to use hosted or self-hosted models are integral to the design, not afterthoughts (Annan, 2022; Mbonu et al., 2019a; Oyesiji et al., 2026b; Peteranaba et al., 2022). Migration to crypto-agile and post-quantum protection of telemetry channels is a further long-term requirement (Nwakamma et al., 2026b).
- **Evaluation realism and data scarcity.** Most incidents are novel combinations of familiar causes, and labelled datasets are small and organization specific. Shared, anonymized incident corpora and standardized fault injection suites would accelerate the field (Ndupu et al., 2026b; Oyesiji et al., 2024).
- **Cross-system coordination.** A database incident is often only one part of a wider failure involving applications, networks and dependencies. Database agents must cooperate with service-level agents and human incident commanders without conflicting actions (Akanbi et al., 2025; Ladapo et al., 2024a; Olagunju et al., 2023).
- **Skill erosion and the changing role of the DBA.** If routine incidents are handled automatically, engineers may lose the practice needed for the rare, severe ones. Deliberate drills, transparent explanations and keeping humans in charge of novel incidents help preserve expertise. Research on human factors in information security, awareness training and insider risk (Akeju et al., 2018; Onche et al., 2024; Onche et al., 2026), and on skill transfer and workforce competency in enterprise IT support (Anyanwu, 2022; Wikiri, 2021), suggests that training must evolve alongside automation.

Beyond these challenges, future studies should test propositions P1 to P5 through controlled fault injection and production shadow deployments, compare hosted and on-device models under realistic privacy constraints, develop open and anonymized benchmarks of database incidents, and examine longitudinally how operator roles, skills and trust change as autonomy increases.

References

Adaramola, T. S., Fadero, S., & Gideon, E. N. (2018). Predictive maintenance and condition monitoring in critical power and energy infrastructure. Iconic Research and Engineering Journals, 2(5), 454-477. https://doi.org/10.64388/IREV2I5-1722489

Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2022). Adversarial machine learning in critical infrastructure: A conceptual framework for threat modeling AI enabled OT systems. World Journal of Innovation and Modern Technology, 6(1), 184-234. https://doi.org/10.56201/wjimt.v6.no1.2022.pg184.234

Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023a). AI

augmented threat detection in industrial control systems: A systematic review of machine learning approaches for ICS anomaly detection. International Journal of Engineering and Modern Technology, 9(3), 287-340. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.340

Adebayo, A., Adepoju, P. A., & Ozowara, D. E. (2023b). Conceptual model for cyber risk pricing and insurance structuring in health technology platforms. Gyanshauryam, International Scientific Refereed Research Journal, 6(6).

Adebayo, A., Amadi, C., & Ijagbemi, A. O. (2025b). From audit to continuous control: Implementation pathways, governance, and organizational readiness for AI-enabled compliance in critical infrastructure. International Journal of Computer Science and Mathematical Theory, 11(8), 88-134. https://doi.org/10.56201/ijcsmt.vol.11.no8.2025.pg88.134

Adebayo, A., Amadi, C., & Ijagbemi, A. O. (2026). Semantic de-duplication of shared cyber threat indicators using large language model embeddings. Global Journal of Engineering and Technology Review, 2(9), 465-482. https://doi.org/10.65150/EP-gjetr/V2E9/2026-07

Adebayo, A., Anunagba, C. O., & Ozowara, D. E. (2025a). A review of zero trust security models and cost effectiveness in healthcare infrastructure. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2269-2283. https://doi.org/10.62225/2583049X.2025.5.6.6051

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2020). Securing operational technology networks in electric utilities: A systematic review of NERC CIP compliance and architectural threat mitigation. International Journal of Engineering and Modern Technology, 6(3), 103-146. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg103.146

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2022). A security architecture model for IT and OT convergence in regulated energy networks: Design principles and governance alignment. International Journal of Computer Science and Mathematical Theory, 8(2), 81-132. https://doi.org/10.56201/ijcsmt.v8.no2.2022.pg81.132

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2023). ICS and SCADA threat detection architectures in energy sector networks: A systematic review of SIEM, NDR, and anomaly detection approaches. World Journal of Innovation and Modern Technology, 7(2), 121-182. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.182

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024a). A vulnerability governance architecture for power and utilities corporations: From exposure mapping to remediation verification. World Journal of Innovation and Modern Technology, 8(6), 185-246. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.246

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2024b). An AI driven security operations architecture for utility sector SOCs: Integrating threat intelligence, behavioral analytics, and automated response. International Journal of Engineering and Modern Technology, 10(11), 197-256. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.256

Adegbite, M. P., Adebayo, A., & Ahmed, M. O. (2025). A cyber risk quantification and governance architecture for critical infrastructure: From posture measurement to executive reporting. International Journal of Computer Science and Mathematical Theory, 11(12), 232-293. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg232.293

Adelanwa, A., Basnet, A., & Anene, U. N. (2023). Data driven digital transformation models for lifecycle performance management in infrastructure delivery. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2646-2662. https://doi.org/10.62225/2583049X.2023.3.6.5968

Adelanwa, A., Basnet, A., & Anene, U. N. (2024a). Advanced AI based decision support systems for healthcare operations and resource planning. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 244-276. http://doi.org/10.32628/GISRRJ

Adelanwa, A., Basnet, A., & Anene, U. N. (2024b). Performance intelligence models for optimization and outcome measurement in large scale public services. Shodhshauryam, International Scientific Refereed Research Journal, 6(1).

Adeniyi, A. I., Odejobi, O., & Taiwo, T. (2025). Countermeasures against bias and spoofing in modern facial recognition systems. World Journal of Advanced Research and Reviews, 25(1), 1914-1930.

Adesuyi, M. O., Kalu, A., & Walawalkar, G. (2023). Data-led cost governance in technology-intensive enterprises. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 877-896. https://doi.org/10.32628/IJSRCSEIT

Adesuyi, M. O., Walawalkar, G., & Kalu, A. (2022). Predictive budgeting models using operational and market signals. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(5), 818-837. https://doi.org/10.32628/IJSRCSEIT

Afrihyia, E., Akinse, S. G., & Ojukwu, P. U. (2024). Comparative governance of AI-driven healthcare management: Executive oversight, regulatory structures, and accountability in the United States and developing countries. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3087-3102. https://doi.org/10.62225/2583049X.2024.4.6.5920

Afrihyia, E., Akinse, S. G., & Ojukwu, P. U. (2025). Organizational readiness for generative AI integration in healthcare operations: Comparative management capabilities between the U.S. and low- and middle-income countries. Iconic Research and Engineering Journals, 8(10), 1673-1697. https://doi.org/10.64388/IREV8I10-1714670

Agu, M. U., Akomolafe, O., & Bello, A. (2023a). A comparative review of SOX compliance frameworks in cross-border financial auditing. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2297-2306. https://doi.org/10.62225/2583049X.2023.3.6.5362

Agu, M. U., Akomolafe, O., & Bello, A. (2023b). A review of integrated data management systems for enhancing financial forecasting accuracy. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2335-2344.

Ahmed, K. S., & Odejobi, O. D. (2018a). Conceptual framework for scalable and secure cloud architectures for enterprise messaging. IRE Journals, 2(1), 1-15.

Ahmed, K. S., & Odejobi, O. D. (2018b). Resource allocation model for energy-efficient virtual machine placement

in data centers. IRE Journals, 2(3), 1-10.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2019). Algorithmic model for constraint satisfaction in cloud network resource allocation. IRE Journals, 2(12), 516-532.

Ahmed, K. S., Odejobi, O. D., & Oshoba, T. O. (2020). Predictive model for cloud resource scaling using machine learning techniques. Journal of Frontiers in Multidisciplinary Research, 1(1), 173-183.

Ahmed, M. O., Adegbite, M. P., & Adebayo, A. (2021). Zero trust architecture for operational technology in North American critical infrastructure: A framework for implementation and resilience optimization. International Journal of Engineering and Modern Technology, 7(1), 66-113. https://doi.org/10.56201/ijemt.vol.7.no1.2021.pg66.113

Ahmed, T., Ghosh, S., Bansal, C., Zimmermann, T., Zhang, X., and Rajmohan, S. (2023). Recommending root-cause and mitigation steps for cloud incidents using large language models. In Proceedings of the 45th International Conference on Software Engineering (ICSE).

Ajagbe, S. A., Akindolani, A., Akande, T. O., Adeyanju, K. I., Aiyeniko, O., & Ajiboye, G. O. (2025). Intrusion detection system with feature selection on machine learning algorithm. In Proceedings of the 6th International Conference and Workshop on Engineering and Technology Research (ICWETR) LAUFET 2025 (pp. 24-39).

Ajala, E. E., Sankara, H. W. Y. C., Minoungou, T. F. T., & Nwakamma, S. (2026b). Apache Kafka versus WebSockets for real-time telemetry in IoT and connected vehicle networks: A comparative review. International Journal of Academic Management Science Research, 10(9), 88-103.

Ajala, E. E., Sankara, H. W. Y. C., Oyesiji, S. O., & Nwakamma, S. (2026a). A review of hallucination mitigation techniques in retrieval-augmented generation systems. International Journal of Academic Engineering Research, 10(9), 162-176.

Akanbi, O., & Sunday, E. A. (2025). A systematic review of AI-driven autonomous mobile robots (AMR) in scalable micro-fulfillment centers. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2363-2379. https://doi.org/10.62225/2583049X.2025.5.6.6182

Akanbi, O., Ganiu, O. S., & Sunday, E. A. (2025). A multi-agent AI framework for swarm intelligence in autonomous mobile robot (AMR) fleet coordination. International Journal of Scientific Research in Humanities and Social Sciences, 2(1), 81-109.

Akeju, B., Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., & Abolaji, T. O. (2018). Conceptual model for insider threat classification and risk modeling in complex digital systems. Iconic Research and Engineering Journals, 1(9), 476-492. https://doi.org/10.64388/IREV1I9-1713778

Akomolafe, O., & Agu, M. U. (2018). A conceptual model for enhancing internal audit quality through technology-enabled risk assessment frameworks. Iconic Research and Engineering Journals, 1(9), 458-475.

Akomolafe, O., & Agu, M. U. (2019). A conceptual framework for developing risk-based internal control models in the insurance and banking sectors. Iconic Research and Engineering Journals, 2(8), 335-354.

Akomolafe, O., Agu, M. U., & Bello, A. (2025a). A conceptual model for advancing risk governance through data-driven compliance analytics in financial institutions. Journal of Accounting and Financial Management, 11(11), 211-228. https://doi.org/10.56201/jafm.vol.11.no11.2025.pg211.228

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2024). Scalable blockchain payment gateway architecture model for enterprise-grade adoption. International Journal of Advanced Multidisciplinary Research and Studies, 4(1), 1552-1568. https://doi.org/10.62225/2583049X.2024.4.1.5280

Akomolafe, O., Olaogun, B. O., Adesuyi, M. O., Ndukwe, V. U., & Sakyi, J. K. (2025b). Collaborative governance framework for secure cross-border payment data sharing. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 849-865. https://doi.org/10.62225/2583049X.2025.5.6.5283

Alieme, J. I., Sule, A., & Obukadata, V. O. (2024). From ambiguity to AI-ready requirements: A business analysis framework for structuring business problems for intelligent process automation. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 2088-2117. https://doi.org/10.54660/.IJMRGE.2024.5.6.2088-2117

Alieme, J. I., Sule, A., & Obukadata, V. O. (2025a). Requirements elicitation for AI-enabled process automation: A comparative review of Agile, Waterfall, and Hybrid implementation approaches. Gulf Journal of Computer Sciences, 1(4), 116-169.

Alieme, J. I., Sule, A., & Obukadata, V. O. (2025b). The business analyst as an AI-transformation broker: A framework for stakeholder alignment, responsible automation, and value realization in small and medium-sized enterprises. International Journal of Economics and Business Management, 11(8), 299-355. https://doi.org/10.56201/ijebm.vol.11.no8.2025.pg299.355

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023a). A conceptual framework for continuous cloud misconfiguration monitoring and enterprise risk mitigation strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), 373-394. https://doi.org/10.32628/CSEIT2361071

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023b). A review of API governance and risk prioritization frameworks in modern financial institutions. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(10), 395-433. https://doi.org/10.32628/CSEIT2361072

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024a). A conceptual framework for enterprise data sensitivity classification and regulatory traceability mechanisms. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3103-3124. https://doi.org/10.62225/2583049X.2024.4.6.5991

Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024b). Advances in HIPAA compliant data architecture and secure analytics frameworks for community healthcare organizations. Shodhshauryam, International Scientific Refereed Research Journal, 7(2), 277-324. https://doi.org/10.32628/SHISRRJ2472163

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025a). A review of AI assisted continuous auditing systems in technology risk and cybersecurity oversight. Gyanshauryam, International Scientific Refereed Research Journal, 8(4), 210-250.

https://doi.org/10.32628/GISRRJ258369

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025b). Advances in data lakehouse governance architectures for enterprise data loss prevention and compliance assurance. Shodhshauryam, International Scientific Refereed Research Journal, 8(4), 171-213. https://doi.org/10.32628/SHISRRJ258474

Amadi, C. (2025). An autonomous, continuously-learning framework for real-time cyber-physical threat prevention in legacy SCADA systems. World Journal of Innovation and Modern Technology, 9(8), 148-183. https://doi.org/10.56201/wjimt.v9.no8.2025.pg148.183

Amadi, C. (2026). The compliance gap: Why audit-based cybersecurity models fail critical infrastructure and the case for continuous control. Global Journal of Engineering and Technology Review, 2(9), 536-562. https://doi.org/10.65150/EP-gjetr/V2E9/2026-12

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025a). AI-based security posture management as an enabling layer for real-time NIST Cybersecurity Framework adherence: A theory-grounded conceptual framework. World Journal of Innovation and Modern Technology, 9(8), 99-147. https://doi.org/10.56201/wjimt.v9.no8.2025.pg99.147

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025b). Deep learning architectures for anomaly detection in SCADA networks: A comparative analysis of LSTM, CNN, and hybrid LSTM-autoencoder models. International Journal of Engineering and Modern Technology, 11(8), 352-392. https://doi.org/10.56201/ijemt.vol.11.no8.2025.pg352.392

Amadi, C., Adebayo, A., & Ijagbemi, A. O. (2025c). The cyber-physical attack surface of legacy SCADA networks: A systematic review of vulnerabilities, threats, and detection gaps in critical infrastructure. International Journal of Computer Science and Mathematical Theory, 11(8), 135-169. https://doi.org/10.56201/ijcsmt.vol.11.no8.2025.pg135.169

Anene, U. N., Ezeako, R., Alugwe, S., & Awulu, I. (2023). Benchmarking methodologies for multi-site operations networks: A review of advances in regression-based performance analysis. International Journal of Multidisciplinary Futuristic Development, 4(1), 142-158. https://doi.org/10.54660/IJMFD.2023.4.1.142-158

Annan, A. O. (2022). Data privacy governance models for cross-border digital platforms. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 949-964.

Annan, A. O. (2024). Algorithmic accountability and trade secret protection in artificial intelligence. Shodhshauryam, International Scientific Refereed Research Journal, 7(5), 315-347.

Annan, A. O. (2025a). Automated decision-making and anti-discrimination compliance under U.S. law. International Journal of Advanced Multidisciplinary Research and Studies, 5(2), 2522-2540.

Annan, A. O. (2025b). Cybersecurity compliance as a source of competitive advantage in technology markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(5), 456-487.

Anyanwu, K. C. E. (2019). Developing a maturity model for standardizing IT support operations across geographically distributed multi-office organizations. Iconic Research and Engineering Journals, 3(5)., 580-598.

Anyanwu, K. C. E. (2020). Balancing cost and operational continuity in hybrid remote and on-site IT support for multi-branch SMEs. International Journal of Economics and Financial Management, 5(2), 132-148. https://doi.org/10.56201/ijefm.v5.no2.2020.pg132.148

Anyanwu, K. C. E. (2022). Bridging enterprise IT operations and digital entrepreneurship: A systematic review of skill transfer mechanisms and pathways. World Journal of Entrepreneurial Development Studies, 7(1), 114-134. https://doi.org/10.56201/wjeds.v7.no1.2022.pg114.134

Asiedu, W., & Quainoo, R. (2023). Toward maintenance free wireless infrastructure: Simulating performance and reliability in large scale intermittently powered IoT networks. Gyanshauryam, International Scientific Refereed Research Journal, 6(1), 489-510.

Asiedu, W., & Quainoo, R. (2024). Rethinking energy, reliability, and latency trade-offs in green communication for next generation IoT. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1987-1994.

Asiedu, W., Quainoo, R., & Asiedu, A. (2026). Predictive power management for intermittent IoT devices using lightweight machine learning under uncertain energy harvest. Gulf Journal of Engineering and Technology, 2(4), 108-118.

Atakpa, M. I. (2021). A review of predictive analytics models for anti-money laundering detection in commercial banking systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(2), 778-804. https://doi.org/10.32628/CSEIT2064813

Atakpa, M. I., & Abetoh, N. F. (2022). A systematic review of machine learning advances in financial fraud detection for banking systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 771-801. https://doi.org/10.32628/CSEIT23906220

Atakpa, M. I., & Fobellah, A. N. (2023). Anomaly detection in financial time-series data: A conceptual model for healthcare and banking applications. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(2), 967-997. https://doi.org/10.32628/CSEIT2342441

Badmus, O., Dosunmu, A. A., & Anunagba, C. O. (2025). A governance framework for AI-assisted CRM workflows: Agentforce deployment, risk management, and organizational readiness in enterprise Salesforce environments. International Journal of Scientific Research in Humanities and Social Sciences, 2(1), 59-80.

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2018). A systematic review of CI/CD pipeline strategies in Salesforce DevOps: Tools, practices, and deployment outcomes. Iconic Research and Engineering Journals, 2(6).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019a). A conceptual model for ETL design and data integration in Salesforce-centric enterprise architectures. Iconic Research and Engineering Journals, 3(5).

Badmus, O., Dosunmu, A. A., & Ozowara, D. E. (2019b). A governance framework for Salesforce platform management in regulated healthcare environments. Iconic Research and Engineering Journals, 3(6).

Badmus, O., Dosunmu, A. A., Ozowara, D. E., & Anunagba, C. O. (2020). A comparative framework for Salesforce

DevOps tooling: Evaluating Copado, Flosum, and Salesforce DX across enterprise deployment contexts. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 1021-1031. https://doi.org/10.54660/.IJMRGE.2020.1.5.1021-1031

Badmus, O., Jooda, D., & Anunagba, C. O. (2024). A privacy-by-design framework for role-based security architecture in Salesforce environments handling sensitive personal data. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3244-3254. https://doi.org/10.62225/2583049X.2024.4.6.6243

Badmus, O., Jooda, D., Ozowara, D. E., & Anunagba, C. O. (2022a). A framework for Git-based version control and code review governance in Salesforce development teams. Shodhshauryam, International Scientific Refereed Research Journal, 5(2), 473-493.

Badmus, O., Jooda, D., Ozowara, D. E., & Anunagba, C. O. (2022b). A systematic review of MuleSoft ESB integration patterns in multi-cloud Salesforce architectures. Gyanshauryam, International Scientific Refereed Research Journal, 5(3), 462-481.

Bello, A. D., Elebe, O., Hammed, N. I., Okoruwa, P. O., Fadayomi, O., & Omoegun, G. O. (2025). An advanced regulatory technology framework for improving financial transparency and fraud reporting accuracy. International Journal of Advanced Multidisciplinary Research and Studies, 5(6).

Bello, A. D., Elebe, O., Hammed, N. I., Omoegun, G. O., & Fadayomi, O. (2024). A cybersecurity risk management and regulatory compliance framework for financial institutions. Iconic Research and Engineering Journals. https://www.irejournals.com/paper-details/1713553

Beyer, B., Jones, C., Petoff, J., and Murphy, N. R. (Eds.). (2016). Site Reliability Engineering: How Google Runs Production Systems. O'Reilly Media.

Borah, S., Aliliele, K. C., Rakshit, S., & Vajjhala, N. R. (2022). Applications of artificial intelligence in software testing. In P. K. Mallick et al. (Eds.), Cognitive informatics and soft computing (Lecture Notes in Networks and Systems, Vol. 375, pp. 727-736). Springer. https://doi.org/10.1007/978-981-16-8763-1_60

Campbell, L., and Majors, C. (2017). Database Reliability Engineering: Designing and Operating Resilient Database Systems. O'Reilly Media.

Chen, Y., Shetty, M., Somashekar, G., et al. (2025). AIOpsLab: A holistic framework to evaluate AI agents for enabling autonomous clouds. In Proceedings of Machine Learning and Systems (MLSys).

Chen, Y., Xie, H., Ma, M., et al. (2024). Automatic root cause analysis via large language models for cloud incidents. In Proceedings of the European Conference on Computer Systems (EuroSys).

Chibwaye, I. P., & Oteri, O. (2023). Advances and conceptual models in data integrated ERP migration for large scale government workforce transformation. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2712-2726.

Dawud, Y. (2026). From pilot to scale: Determinants of successful artificial intelligence, robotics, and automation adoption in supply chain and fulfillment operations. Advances in IT and Digital Security, 1(3), 1-28.

Dosunmu, A. A., & Ogundele, P. O. (2019). Security audit and enterprise risk assessment frameworks for resilient information systems. Iconic Research and Engineering Journals, 3(5), 434-447. https://doi.org/10.64388/IREV3I5-1713225

Dosunmu, A. A., & Ogundele, P. O. (2020). Intrusion detection and prevention models for enhancing organizational cyber defense effectiveness. Iconic Research and Engineering Journals, 4(6), 310-324. https://doi.org/10.64388/IREV4I6-1713226

Dosunmu, A. A., & Ogundele, P. O. (2021). Incident response and digital forensics strategies for rapid cyber attack containment. Gyanshauryam, International Scientific Refereed Research Journal, 4(4), 239-258.

Dosunmu, A. A., & Ogundele, P. O. (2022). Threat intelligence integration frameworks supporting proactive enterprise cybersecurity decision making. Gyanshauryam, International Scientific Refereed Research Journal, 5(3), 397-416.

Dosunmu, A. A., & Ogundele, P. O. (2023). Cyber threat actor analysis models for strategic enterprise security planning. Shodhshauryam, International Scientific Refereed Research Journal, 6(5), 513-531.

Dosunmu, A. A., & Ogundele, P. O. (2024a). Breach and attack simulation frameworks for continuous validation of enterprise security controls. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(3), 1100-1119.

Dosunmu, A. A., & Ogundele, P. O. (2024b). Cyber risk quantification models for prioritizing enterprise security investment decisions. International Journal of Multidisciplinary Research and Growth Evaluation, 5(6), 1777-1785. https://doi.org/10.54660/.IJMRGE.2024.5.6.1777-1785

Dosunmu, A. A., & Ogundele, P. O. (2024c). Enterprise scale continuous security validation models for regulated digital infrastructures. International Journal of Scientific Research in Humanities and Social Sciences, 1(2), 929-945.

Dosunmu, A. A., & Ogundele, P. O. (2024d). Threat informed defence engineering models for measuring security control effectiveness at scale. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2847-2858.

Dosunmu, A. A., & Ogundele, P. O. (2025a). Adversary simulation design frameworks for proactive cyber defense in complex environments. International Journal of Computer Science and Mathematical Theory, 11(12), 193-209. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg193.209

Dosunmu, A. A., & Ogundele, P. O. (2025b). Cyber defense performance measurement frameworks for executive and board level governance. Computer Science and IT Research Journal, 6(11), 895-913. https://doi.org/10.51594/csitrj.v6i11.2164

Dosunmu, A. A., & Ogundele, P. O. (2025c). Security orchestration and automation models for accelerating incident detection and response. Computer Science and IT Research Journal, 6(11), 878-894. https://doi.org/10.51594/csitrj.v6i11.2163

Dosunmu, A. A., & Ogundele, P. O. (2026a). Deception based defense architectures for disrupting advanced persistent threat operations. Engineering and Technology Journal, 11(1), 8475-8487. https://doi.org/10.47191/etj/v11i01.07

Dosunmu, A. A., & Ogundele, P. O. (2026b). Integrated threat intelligence automation and simulation models for next generation cyber defense. Engineering and Technology Journal, 11(1), 8451-8462. https://doi.org/10.47191/etj/v11i01.05

Dosunmu, A. A., & Ogundele, P. O. (2026c). Proxy firewall and endpoint validation frameworks using breach simulation methodologies. Engineering and Technology Journal, 11(1), 8463-8474. https://doi.org/10.47191/etj/v11i01.06

Edivri, J., & Oteri, O. (2022). Predictive capacity planning and resource utilization forecasting models for multi-program and multi-stakeholder IT portfolios. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(4), 826-845.

Edivri, J., & Oteri, O. (2024). A conceptual KPI-driven decision and optimization framework for IT service delivery, portfolio performance, and adoption. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 167-187. https://doi.org/10.32628/GISRRJ246643

Edivri, J., Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., & Akeju, B. (2026). Conceptual model for integrated human and machine identity governance in cloud-based security architectures [Manuscript in preparation].

Ekechi, N. V., Ozowara, D. E., & Anunagba, C. O. (2026). Conceptual framework for AI governance, data privacy compliance, and financial sustainability in digital health. Computer Science and IT Research Journal, 7(4), 275-299.

Elebe, O., & Anunagba, C. O. (2025). Responsible artificial intelligence in IT auditing through evidence validation, human oversight, and regulatory compliance. International Journal of Technology, Health and Sustainability, 1(2), 310-328.

Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., Okoruwa, P. O., & Akeju, B. (2019). Risk-based cybersecurity assurance and data availability: Limitations, advances and future research opportunities. Iconic Research and Engineering Journals, 2(12), 602-617. https://doi.org/10.64388/IREV2I12-1713779

Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2024). An adaptive fraud risk scoring model for real-time transaction monitoring at scale. IIARD International Journal of Banking and Finance Research, 10(10), 212-230.

Fadero, S., Jooda, D., Oyesiji, S. O., & Nwakamma, S. (2025). IT services decoupling after mergers, acquisitions, and ownership transitions: A framework for secure infrastructure separation. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2471-2485.

Fadero, S., Nwakamma, S., Jooda, D., & Oyesiji, S. O. (2021). Cyber risk management maturity in Nigeria's insurance sector: An assessment against the NAICOM and NDPR regulatory landscape. Iconic Research and Engineering Journals, 5(2), 401-420. https://doi.org/10.64388/IREV5I2-1722621

Fobellah, A. N. (2025). Navigating digital transformation: Auditing artificial intelligence-powered financial systems: A conceptual review. International Journal of Science and Research Archive, 16(2), 23-28. https://doi.org/10.30574/ijsra.2025.16.2.2274

Giannakouris, V., and Trummer, I. (2025). λ-Tune: Harnessing large language models for automated database system tuning. In Proceedings of the ACM SIGMOD International Conference on Management of Data.

Gideon, E. N., Adaramola, T. S., & Fadero, S. (2019). Reliability engineering and failure analysis in complex engineering systems. Iconic Research and Engineering Journals, 2(11), 703-727. https://doi.org/10.64388/IREV2I11-1722490

Hussain, N., & Adebayo, A. (2026). The role of artificial intelligence in strengthening modern cybersecurity systems. World Journal of Innovation and Modern Technology, 10(6), 125-181. https://doi.org/10.56201/wjimt.v10.no6.2026.pg125.181

Idika, C. N., Salami, E. O., Ijiga, O. M., & Enyejo, L. A. (2021). Deep learning driven malware classification for cloud-native microservices in edge computing architectures. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(4).

Jiang, Y., Zhang, C., He, S., et al. (2024). Xpert: Empowering incident management with query recommendations via large language models. In Proceedings of the 46th International Conference on Software Engineering (ICSE).

Jimoh, H. O., & Ahmed, M. O. (2024). Analyzing Network Time Protocol (NTP) based amplification DDoS attack and its mitigation techniques. Journal of Digital Innovations and Contemporary Research in Science, Engineering and Technology, 12(2), 17-24. https://doi.org/10.22624/AIMS/DIGITAL/V11N2P2x

Jimoh, H. O., Abolle-Okoyeagu, C. J., Ahmed, M. O., & Lawal, N. O. (2023a). Advancing security in IoT-driven critical infrastructure: A focus on smart transportation system. American Journal of Engineering Research, 12(12), 33-46.

Jimoh, H. O., Ahmed, M. O., & Fagbade, M. O. (2023b). The role of frameworks in cybersecurity governance. Journal of Behavioural Informatics, Digital Humanities and Development Research, 9(4), 7-16. https://doi.org/10.22624/AIMS/BHI/V9N4P2

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2018). Lessons learned from offline assessment of security-critical systems: The case of Microsoft Active Directory. Iconic Research and Engineering Journals, 2(6), 277-299. https://doi.org/10.64388/IREV2I6-1717205

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2022a). Human-in-the-loop machine learning: A state of the art. Journal of Frontiers in Multidisciplinary Research, 3(1), 656-669. https://doi.org/10.54660/.JFMR.2022.3.1.656-669

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023b). Active Directory attacks steps, types, and signatures. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2863-2874. https://doi.org/10.62225/2583049X.2023.3.6.6204

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023c). An IT service management literature review: Challenges, benefits, opportunities, and implementation practices. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2875-2889. https://doi.org/10.62225/2583049X.2023.3.6.6205

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2024a). Integrated network and security operation center: A systematic analysis. International Journal of Multidisciplinary Futuristic Development, 5(1), 65-80. https://doi.org/10.54660/IJMFD.2024.5.1.65-80

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2025). Migration of applications and information systems to cloud computing infrastructure: Lessons from a South African retail bank. International Journal of Multidisciplinary Research and Growth Evaluation,

6(6), 1361-1375. https://doi.org/10.54660/.IJMRGE.2025.6.6.1361-1375

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2019). Implementation of Active Directory for efficient management of enterprise networks. Iconic Research and Engineering Journals, 3(4), 608-627. https://doi.org/10.64388/IREV3I4-1717206

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2022b). Navigating digital transformation: Best practices for cloud migration strategies in the enterprise. Journal of Frontiers in Multidisciplinary Research, 3(1), 643-655. https://doi.org/10.54660/.JFMR.2022.3.1.643-655

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023a). A comprehensive survey on ServiceNow for IT service management. International Journal of Multidisciplinary Research and Growth Evaluation, 4(6), 1532-1545. https://doi.org/10.54660/.IJMRGE.2023.4.6.1532-1545

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023d). Systematic literature review on security access control policies and techniques based on privacy requirements in a BYOD environment. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2890-2904. https://doi.org/10.62225/2583049X.2023.3.6.6206

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024b). Keeping humans in the loop: Human-centered automated annotation with generative AI. International Journal of Multidisciplinary Futuristic Development, 5(1), 81-95. https://doi.org/10.54660/IJMFD.2024.5.1.81-95

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2026). On the disagreement problem in human-in-the-loop federated machine learning. International Journal of Multidisciplinary Research and Growth Evaluation, 7(3), 178-192. https://doi.org/10.54660/.IJMRGE.2026.7.3.178-192

Lao, J., Wang, Y., Li, Y., et al. (2024). GPTuner: A manual-reading database tuning system via GPT-guided Bayesian optimization. Proceedings of the VLDB Endowment, 17(8).

Lewis, P., Perez, E., Piktus, A., et al. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. In Advances in Neural Information Processing Systems (NeurIPS).

Ma, M., Yin, Z., Zhang, S., et al. (2020). Diagnosing root causes of intermittent slow queries in cloud databases. Proceedings of the VLDB Endowment, 13(8).

Mayo, W., Ogbole, J. I., Okoruwa, P. O., & Babatope, O. M. (2021). Designing an AI-predictive maintenance model for e-commerce systems using machine learning and cloud analytics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 416-440. https://doi.org/10.32628/IJSRCSEIT

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Oluoha, O. M. (2018). A conceptual framework for legal and ethical risk modeling in enterprise data protection governance systems. Iconic Research and Engineering Journals, 2(2), 207-226. https://doi.org/10.64388/IREV2I2-1714911

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2020a). A review of identity and access management integration strategies in hybrid and multi cloud environments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 795-810. https://doi.org/10.54660/.IJMRGE.2020.1.5.795-810

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021b). A conceptual framework for risk based business intelligence architecture in financial technology platforms. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 731-746. https://doi.org/10.54660/.IJMRGE.2021.2.6.731-746

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021c). Advances in artificial intelligence techniques for secure software testing and automated regression control mechanisms. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 468-496. https://doi.org/10.32628/CSEIT217565

Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2022a). A conceptual framework for AI enabled IT general controls and SOX audit automation processes. Gyanshauryam, International Scientific Refereed Research Journal, 5(5), 384-414. https://doi.org/10.32628/GISRRJ2256239

Mbonu, I. S., Aliliele, C., Uzoka, E., & Oluoha, O. M. (2019a). A review of comparative data protection regulations and secure cloud implementation strategies across jurisdictions. Iconic Research and Engineering Journals, 2(9), 482-501. https://doi.org/10.64388/IREV2I9-1714912

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020b). A conceptual framework for agile supply chain digital transformation with embedded IT risk and ISO compliance controls. Iconic Research and Engineering Journals, 3(11), 566-593. https://doi.org/10.64388/IREV3I11-1714916

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2020c). Advances in infrastructure as code governance for secure terraform based enterprise cloud deployments. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 811-828. https://doi.org/10.54660/.IJMRGE.2020.1.5.811-828

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2021a). A review of VoIP forensic analytics models for financial fraud detection and regulatory compliance monitoring. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 711-730. https://doi.org/10.54660/.IJMRGE.2021.2.6.711-730

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022b). A review of data protection impact assessment models in multi cloud financial infrastructure systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(1), 589-623. https://doi.org/10.32628/CSEIT25442

Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2022c). Advances in cloud identity and access governance optimization in large scale AWS enterprise environments. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 403-438. https://doi.org/10.32628/SHISRRJ225490

Mbonu, I. S., Iwuanyanwu, U., Uzoka, E., & Oluoha, O. M. (2019b). Advances in enterprise log analytics and automated incident response architectures using Python and SIEM platforms. Iconic Research and Engineering Journals, 3(2), 1000-1019. https://doi.org/10.64388/IREV3I2-1714915

Ndupu, K. C., Ajala, E. E., Oyesiji, S. O., & Nwakamma, S. (2026a). A hardware-in-the-loop CI/CD validation framework for IoT and vehicle embedded systems us-

ing C# and Azure DevOps. Global Journal of Engineering and Technology Review, 2(9), 507-516. https://doi.org/10.65150/EP-gjetr/V2E9/2026-10

Ndupu, K. C., Anunagba, C. O., Nwakamma, S., & Oyesiji, S. O. (2026b). Machine learning for biomolecular data wrangling and curation: A review of learned extraction, error detection, integration, and curation workflows. Advances in IT and Digital Security, 1(6), 1-17.

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024a). LLM-as-a-judge for automated model governance: A review of methods, biases, and release-gating practices. World Journal of Innovation and Modern Technology, 8(6), 185-216. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.216

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024b). Securing agentic AI enterprise workflows against prompt injection, tool poisoning, memory manipulation, and excessive agency threats. World Journal of Innovation and Modern Technology, 8(6), 217-248. https://doi.org/10.56201/wjimt.v8.no6.2024.pg217.248

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2025). On-device multimodal small language models for privacy-preserving edge intelligence through quantization, pruning, distillation, and energy-efficient inference. World Journal of Innovation and Modern Technology, 9(12), 271-302. https://doi.org/10.56201/wjimt.v9.no12.2025.pg271.302

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2026b). Crypto-agile migration to hybrid post-quantum cryptography in enterprise TLS, PKI, VPN, and cloud-native systems and services. Gulf Journal of Computer Sciences, 1(1). https://doi.org/10.51594/gjcs.v1i1

Nwakamma, S., Oyesiji, S. O., Ndupu, K. C., & Ajala, E. E. (2026a). Characterizing large language model failure modes in code refactoring and multi-turn reasoning: A controlled study design. International Journal of Academic and Applied Research, 10(9), 226-237.

Odejobi, O. D., & Ahmed, K. S. (2018). Performance evaluation model for multi-tenant Microsoft 365 deployments under high concurrency. IRE Journals, 1(11), 92-107.

Odejobi, O. D., Hammed, N. I., & Ahmed, K. S. (2019). Approximation complexity model for cloud-based database optimization problems. IRE Journals, 2(9), 1-10.

Odejobi, O. D., Okonkwo, C. S., Ahiaeke Patrick, M. C., Okeke, O. T., & Mayo, W. (2025). AI-augmented secure software engineering: Leveraging deep learning for autonomous threat detection and mitigation. International Journal of Engineering and Modern Technology, 11(12), 101-121. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg101.121

Ogbole, J. I., Okoruwa, P. O., Babatope, O. M., & Oyewole, T. (2021b). Developing an integrated data visualization model for continuous business performance monitoring and optimization. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 441-467. https://doi.org/10.32628/IJSRCSEIT

Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021a). Conceptual model for identity-centric zero trust architecture in enterprise security governance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 393-415. https://doi.org/10.32628/IJSRCSEIT217562

Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., & Abolaji, T. O. (2025). Security analytics and digital forensics for enterprise risk management, advances and practical implications. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2017-2028.

Oghenemaiga, E., Basnet, A., & Anene, U. N. (2024). Predictive analytics applications for forecasting traffic patterns across owned and operated media platforms. International Journal of Advanced Multidisciplinary Research and Studies, 4(6). https://doi.org/10.62225/2583049X.2024.4.6.5668

Ogunwola, T. A. (2026). Security and resilience considerations for software-defined wide area network deployments in multi-site enterprise environments. International Advanced Research Journal in Science, Engineering and Technology, 12(1). https://doi.org/10.17148/iarjset.2025.12150

Ogunwola, T. A., & Alozie, C. (2026a). Architecting secure and compliant distributed healthcare networks: Operational approaches to health insurance portability and accountability act and health information trust alliance alignment. International Journal of Computer Applications, 187(111), 1-6.

Ogunwola, T. A., & Alozie, C. (2026b). Enterprise firewall modernization for business continuity: A framework for secure migration and operational stability. Computer Science & IT Research Journal, 7(5), 347-361. https://doi.org/10.51594/csitrj.v7i5.2287

Ogunwola, T. A., & Deborah, F. O. (2026). Enterprise network resilience as a national security imperative: Strategies for protecting United States critical infrastructure. International Advanced Research Journal in Science, Engineering and Technology, 12(10). https://doi.org/10.17148/iarjset.2025.121048

Ogunwola, T. A., Owoyemi, T. A., & Iyanda, C. (2026). Cybersecurity and network integration risk management during corporate acquisitions and infrastructure consolidation. Computer Science & IT Research Journal, 7(6), 389-404. https://doi.org/10.51594/csitrj.v7i6.2305

Ojukwu, J., Oyesiji, S. O., & Nwakamma, S. (2023). Cyber-physical ransomware defense in operational technology using physics-informed detection, digital twins, network telemetry, and resilient recovery. International Journal of Computer Science and Mathematical Theory, 9(5), 193-228. https://doi.org/10.56201/ijcsmt.v9.no5.2023.pg193.228

Ojukwu, J., Oyesiji, S. O., & Nwakamma, S. (2025). WebAssembly component model and WASI for portable cloud-to-edge software: Language interoperability, security, performance, and container comparisons. International Journal of Computer Science and Mathematical Theory, 11(12), 232-263. https://doi.org/10.56201/ijcsmt.vol.11.no12.2025.pg232.263

Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., Ogbole, J. I., & Akeju, B. (2024). Enterprise cybersecurity trends and threat evolution, advances and emerging research directions. Global Multidisciplinary Perspectives Journal, 1(6), 194-204. https://doi.org/10.54660/GMPJ.2024.1.6.194-204

Okoruwa, P. O., Fadayomi, O., Akeju, B., Edivri, J., Ogbole, J. I., & Abolaji, T. O. (2020). Conceptual model for privacy-centric security engineering in digital and cloud computing systems. International Journal of Scientific Research in Computer Science, Engineering and In-

formation Technology, 7(5), 371-389.

Okoruwa, P. O., Fadayomi, O., Bello, A. D., Elebe, O., Hammed, N. I., & Omoegun, G. O. (2025). An artificial intelligence-driven financial crime investigation framework for analyst decision support. International Journal of Multidisciplinary Research and Growth Evaluation, 6(6).

Okwesa, I. J., Ashore-Onisemo, F., Oyesiji, S. O., & Abdulmalik, A. U. (2024). Predictive risk analytics for early-warning systems in enterprise technology estates. Shodhshauryam, International Scientific Refereed Research Journal, 7(6), 327-386. https://doi.org/10.32628/SHISRRJ24797 [Verify pages: the article running header reads 318-326.]

Olagunju, E. O., Edivri, J., & Oteri, O. (2022). Predictive capacity planning and resource utilization forecasting models for multi program and multi stakeholder IT portfolios. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 336-356.

Olagunju, E. O., Edivri, J., & Oteri, O. (2023). A conceptual governance model for change, incident, and problem management in mission-critical enterprise IT environments. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 365-384.

Olagunju, E. O., Edivri, J., & Oteri, O. (2024). Applied performance optimization frameworks for managing high-demand enterprise technology programs and system rollouts. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3059-3070. https://doi.org/10.62225/2583049X.2024.4.6.5915

Olagunju, E. O., Oteri, O., & Edivri, J. (2025). An operational reliability and service assurance framework for enterprise IT systems supporting large user populations. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2117-2128. https://doi.org/10.62225/2583049X.2025.5.6.5916

Olodo, A., Akanbi, O., & Adenuga, O. (2026a). Conceptualizing a lean-standardized predictive maintenance framework for high-vacuum deposition equipment. International Journal of Engineering and Modern Technology, 12(3), 295-322. https://doi.org/10.56201/ijemt.vol.12.no3.2026.pg295.322

Olodo, A., Akanbi, O., & Adenuga, O. (2026b). Data-driven maintenance and reliability in high-volume semiconductor fabs: A review of Industry 4.0 methodologies. International Journal of Engineering and Modern Technology, 12(3), 323-348. https://doi.org/10.56201/ijemt.vol.12.no3.2026.pg323.348

Ominyi, M., & Anichukwueze, C. C. (2023). A review of algorithmic accountability and model risk management approaches in financial services. Journal of Accounting and Financial Management, 9(12), 218-238. https://doi.org/10.56201/jafm.v9.no12.2023.pg218.238

Ominyi, M., & Anichukwueze, C. C. (2024). Conceptualizing responsible AI governance structures for automated decision systems in regulated industries. International Journal of Social Sciences and Management Research, 10(11), 403-430. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.403.430

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024a). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. World Journal of Innovation and Modern Technology, 8(6), 204-228. https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024b). A systematic review of organizational readiness for the EU Artificial Intelligence Act in multinational enterprises. World Journal of Innovation and Modern Technology, 8(6), 185-203. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.203

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025a). A conceptual framework for multi-agent AI quality control in the review of regulated documents. International Journal of Social Sciences and Management Research, 11(8), 534-557. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg534.557

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025b). Reviewing legal privilege and confidentiality challenges in enterprise deployment of large language models. Journal of Law and Global Policy, 10(3), 150-176. https://doi.org/10.56201/jlgp.vol.10.no3.2025.pg150.176

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026). Conceptualizing enterprise AI governance functions as institutional standards for auditable and defensible risk management. Journal of Accounting and Financial Management, 12(7), 326-356. https://doi.org/10.56201/jafm.vol.12.no7.2026.p326.356

Omoegun, G. O., Sunday, E. A., Essien, M. A., & Oluokun, O. A. (2023). Vibration-based condition monitoring of rotating machinery using LabVIEW. International Journal of Scientific Research in Civil Engineering, 7(6), 82-108.

Onche, V. O., Adegbite, M. P., & Ogbonna, C. S. (2026). Human factors in information security: A capability framework for administrative professionals in the digital workplace. World Journal of Innovation and Modern Technology, 10(5), 154-179. https://doi.org/10.56201/wjimt.v10.no5.2026.pg154.179

Onche, V. O., Ogbonna, C. S., & Adegbite, M. P. (2024). Effectiveness of cybersecurity awareness training on insider-threat behavior among university administrators: An integrative academic review. International Journal of Computer Science and Mathematical Theory, 10(2), 117-144. https://doi.org/10.56201/ijcsmt.v10.no2.2024.pg117.144

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2019). Secure identity and access management model for distributed and federated systems. IRE Journals, 3(4), 550-567.

Oshoba, T. O., Hammed, N. I., & Odejobi, O. D. (2020). Blockchain-enabled compliance and audit trail model for cloud configuration management. Journal of Frontiers in Multidisciplinary Research, 1(1), 193-201.

Osinem, H. E., Eribenne, F., Peteranaba, S. F., & Soyege, O. S. (2025). Conceptual foundations of ethical artificial intelligence adoption in healthcare organizations practice policy. International Journal of Technology, Health and Sustainability, 1(2). [Incomplete record; pages not given in source, verify on profile.]

Oteri, O., & Chibwaye, I. P. (2025). Advances and conceptual models in enterprise level change management analytics for large scale organizational system transitions. Gyanshauryam, International Scientific Refereed Research Journal, 8(5), 177-211.

Oteri, O., & Edivri, J. (2024). Applied performance optimiza-

tion frameworks for managing high-demand enterprise technology programs and system rollouts. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 188-210.

Oteri, O., & Edivri, J. (2026). An operational reliability and service assurance framework for enterprise IT systems supporting large user populations. Gulf Journal of Engineering and Technology, 2(1), 1-19. https://doi.org/10.51594/gjet.v2i1.205

Oteri, O., Olagunju, E. O., & Edivri, J. (2025). Conceptual models for cloud-based IT service management architecture and orchestration using ServiceNow platforms. Shodhshauryam, International Scientific Refereed Research Journal, 8(6), 185-203.

Oyeleke, A. V., Eze, F. C., & Asiedu, W. (2026). Reliability-centered maintenance strategies for minimizing downtime and maximizing performance in high-density GPU cluster environments. International Journal of Engineering Technology Research & Management, 10(7), 18-38.

Oyesiji, S. O., Anunagba, C. O., Nwakamma, S., & Sankara, H. W. Y. C. (2026a). Automated validation in embedded IoT development: A review of continuous integration and delivery across the fidelity ladder. Journal of Engineering Research and Reports, 28(9), 145-157. https://doi.org/10.9734/jerr/2026/v28i92005

Oyesiji, S. O., Ndupu, K. C., Anunagba, C. O., & Sankara, H. W. Y. C. (2026b). On-device privacy and zero-knowledge storage in mobile applications: A review with attention to cross-platform React Native development. Journal of Engineering Research and Reports, 28(9), 102-114. https://doi.org/10.9734/jerr/2026/v28i92001

Oyesiji, S. O., Nwakamma, S., & Ojukwu, J. (2024). A conceptual framework for context-aware data curation in fine-tuning pipelines. International Journal of Engineering and Modern Technology, 10(11), 197-228. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.228

Oyesiji, S. O., Nwakamma, S., & Ojukwu, J. (2025). Compressing recommender and ranking models for edge deployment: A survey. International Journal of Engineering and Modern Technology, 11(12), 205-237. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg205.237

Ozowara, D. E., Adebayo, A., & Anunagba, C. O. (2022). A systematic review of cybersecurity investments and their impact on healthcare financial performance. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 404-427.

Ozowara, D. E., Anunagba, C. O., & Adepoju, P. A. (2025). A review of ransomware economics and financial resilience strategies in hospital networks. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2284-2298. https://doi.org/10.62225/2583049X.2025.5.6.6052

Pavlo, A., Angulo, G., Arulraj, J., et al. (2017). Self-driving database management systems. In Proceedings of the Conference on Innovative Data Systems Research (CIDR).

Peteranaba, S. F., Osinem, H. E., Eribenne, F., & Soyege, O. S. (2022). Health information governance and regulatory compliance: Comparative frameworks for data verification, risk screening, and confidentiality in health and financial systems. International Journal of Science, Technology & Society, 6(1), 60-84.

Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025). Test automation in wireless hardware engineering: A comprehensive review of scripting frameworks and instrument control strategies. International Journal of Engineering and Modern Technology, 11(10), 405-464. https://doi.org/10.56201/ijemt.vol.11.no10.2025.pg405.464

Sankara, H. W. Y. C., Oyesiji, S. O., Ajala, E. E., & Minoungou, T. F. T. (2026). A modular event-driven messaging framework for web and mobile applications: Unifying REST and WebSocket access over declared channel semantics. Advances in IT and Digital Security, 1(5), 1-18.

Shittu, H., & Nabil, M. (2023). Smart supply chain management with attribute-based encryption access control. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 198-204). IEEE. https://doi.org/10.1109/CCWC57344.2023.10099268

Shittu, H., Olagunju, F., & Shittu, M. A. (2024). Cyber physical resilience in digital substations: IoT enabled adaptive protection for secure DER integration. International Journal of Science, Architecture, Technology and Environment, 1(3), 81-99. https://doi.org/10.63680/ijsate032532.08

Shittu, M. A., Adeniji, I. O., Shittu, H., & Opara, I. S. (2022). Blockchain-assisted secure data exchange architectures for SCADA-controlled power systems. Iconic Research and Engineering Journals, 6(3), 359-379. https://doi.org/10.64388/IREV6I3-1714041

Singh, V., Vijay, K. V., Kumar, S., et al. (2024). Panda: Performance debugging for databases using LLM agents. In Proceedings of the Conference on Innovative Data Systems Research (CIDR).

Sunday, E. A., & Omoegun, G. O. (2022). Smart fault detection in HVAC systems using sensor-based monitoring. International Journal of Scientific Research in Science, Engineering and Technology, 7(4), 380-403.

Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2020). Transitioning from reactive to predictive maintenance in mechanical systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 6(6), 425-447.

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2022a). Algorithmic process optimization and cost reduction: A review of simulation modeling and financial impact assessment. Journal of Accounting and Financial Management, 8(8), 139-169. https://doi.org/10.56201/jafm.vol.8.no8.2022.p139.169

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2022b). Conceptual model for predictive cost optimization: Machine learning applications in business transformation analysis. International Journal of Economics and Business Management, 8(6), 68-102. https://doi.org/10.56201/ijebm.v8.no6.2022.pg68.102

Tonoyan, A., Dada, O., & Ayivi-Donkor, S. S. (2024). Real-time KPI tracking systems: A review of automated performance monitoring and data-driven decision making. World Journal of Innovation and Modern Technology, 8(6), 247-281. https://doi.org/10.56201/wjimt.v8.no6.2024.pg247.281

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2022). Real-time compliance pipelines: A review of automated risk monitoring and enterprise data governance. International Journal of Multidisciplinary Futuristic Development, 3(2), 66-94.

https://doi.org/10.54660/IJMFD.2022.3.2.66-94

Uchechi, N., Ominyi, M., Anichukwueze, C. C., & Jones, B. C. (2025). Advances in automated governance: Mitigating operational and systemic risks in multi-country delivery networks. Gulf Journal of Advance Business Research, 3(12), 1626-1669. https://doi.org/10.51594/gjabr.v3i12.219

Ukadike, C. A. (2024). Scaling B2B SaaS ventures: An integrated framework for multi-cloud optimization, distributed agile delivery, and investment readiness. World Journal of Finance and Investment Research, 8(5), 196-217. https://doi.org/10.56201/wjfir.v8.no5.2024.pg196.217

Upreti, M., & Oteri, O. (2023). Analytical model for optimizing cloud resource allocation through rightsizing and long-term usage forecasting. Gyanshauryam, International Scientific Refereed Research Journal, 6(1), 400-424.

Upreti, M., & Oteri, O. (2025). Security design model for resilient network architectures in large scale cloud computing platforms. Shodhshauryam, International Scientific Refereed Research Journal, 8(5), 84-104.

Van Aken, D., Pavlo, A., Gordon, G. J., and Zhang, B. (2017). Automatic database management system tuning through large-scale machine learning. In Proceedings of the ACM SIGMOD International Conference on Management of Data.

Walawalkar, G., Adesuyi, M. O., Kalu, A., & Oduleye, T. E. (2025). Executive financial dashboards for real-time strategic oversight. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2042-2054.

Walawalkar, G., Oduleye, T. E., Adesuyi, M. O., & Kalu, A. (2026). Next-generation financial analytics frameworks for AI-enabled enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 6(1), 1779-1791.

Wikiri, M. (2021). Improving first-contact resolution in enterprise technology support: A workforce competency and service-quality framework. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 1212-1225. https://doi.org/10.54660/.IJMRGE.2021.2.6.1212-1225

Yao, S., Zhao, J., Yu, D., et al. (2023). ReAct: Synergizing reasoning and acting in language models. In International Conference on Learning Representations (ICLR).

Yoon, D. Y., Niu, N., and Mozafari, B. (2016). DBSherlock: A performance diagnostic tool for transactional databases. In Proceedings of the ACM SIGMOD International Conference on Management of Data.

Zhang, J., Liu, Y., Zhou, K., et al. (2019). An end-to-end automatic cloud database tuning system using deep reinforcement learning. In Proceedings of the ACM SIGMOD International Conference on Management of Data.

Zhang, L., Jia, T., Jia, M., et al. (2024). A survey of AIOps for failure management in the era of large language models. arXiv preprint arXiv:2406.11213.

Zhou, X., Li, G., Sun, Z., et al. (2024). D-Bot: Database diagnosis system using large language models. Proceedings of the VLDB Endowment, 17(10).