AI-Assisted Risk and Incident Analysis: Advances and Future Opportunities

Uchechi Mary-Linda Unamma[1], Ifeanyichukwu Jeffrey Okwesa[2], Serif Oyindamola Oyesiji[3], Abubakar Umar Abdulmalik[4]
[1] Peace House, Utah, USA; Ucheunamma91@gmail.com
[2] Barclays, New Jersey, USA; ifeanyieb96@gmail.com
[3] Independent Researcher, Lagos, Nigeria; oyesijiserif@gmail.com
[4] UX Thrive, Abuja, Nigeria; maleek.dev1@gmail.com
Corresponding Author: Ucheunamma91@gmail.com
DOI: 10.56201/wjimt.v9.no8.2025.pg99.142

Abstract
Operational risk and security incidents now unfold across distributed, cloud-native estates that generate volumes of telemetry no human team can manually triage at speed. Over the past decade, artificial intelligence (AI) and machine learning (ML) have moved from experimental log-mining prototypes to production components of security operations centres, site reliability engineering practices, and enterprise risk functions. This paper synthesises the advances that have made AI-assisted risk and incident analysis viable and examines the opportunities and limitations that will shape the next phase of adoption. We organise the state of the art into five capability areas: anomaly and detection analytics over logs, metrics, and traces; alert triage, deduplication, and correlation; natural language processing (NLP) and large language models (LLMs) for incident summarisation, knowledge retrieval, and postmortem authoring; automation and orchestration of response workflows; and human–AI collaboration in the analyst loop. We map these capabilities to established incident-handling and risk-management frameworks and present a structured capabilities table describing typical inputs, methods, and outputs. We then interrogate the open challenges that temper enthusiasm: model hallucination and reliability, the sensitivity and governance of incident data, the immaturity of evaluation methodology, and the operational hazards of over-automation. Finally, we propose a research agenda spanning benchmarking, retrieval-grounded and explainable reasoning, evaluation of human–AI teams, and resilience-aware automation. We argue that the near-term value of AI in this domain lies less in autonomous decision-making than in augmenting scarce expert attention, and that trustworthy deployment depends on grounding, evaluation, and human oversight rather than on model scale alone.

Keywords: *incident analysis, operational risk, anomaly detection, large language models, AIOps, retrieval-augmented generation, explainable AI, security operations, human–AI collaboration*

1. Introduction

Modern organisations operate sprawling digital estates whose availability, integrity, and confidentiality are continuously tested by faults, misconfigurations, and adversaries. When something goes wrong (a service degradation, a data exposure, an intrusion) the speed and quality of the analytical response determine the magnitude of the loss. Yet the raw material of that

response, machine-generated telemetry, has grown far faster than the pool of expert analysts able to interpret it. A single mid-sized platform can emit millions of log lines, metric samples, and trace spans per hour, of which only a vanishing fraction is diagnostically relevant during any given event. This asymmetry between signal volume and expert attention is the central motivation for applying artificial intelligence (AI) to risk and incident analysis.

The asymmetry is not merely quantitative; it is structural, and understanding its structure clarifies why naïve scaling of human effort cannot resolve it. The cost of an incident does not grow linearly with its duration but tends to compound: a latent database exhaustion that would be trivial to correct in its first minute can, if undetected, cascade into connection-pool starvation, retry storms, and dependent-service collapse that take hours to unwind. Analytical latency therefore sits on a steep and often convex loss curve, and any capability that shaves minutes from detection and diagnosis captures value out of proportion to the raw time saved. At the same time, the diagnostic signal is buried in an overwhelmingly benign background: the base rate of genuine incidents among candidate anomalies is low, so even a highly accurate detector can, in absolute terms, produce more false alarms than true ones. These two facts, convex loss in time and extreme class imbalance in signal, define the operating regime that AI-assisted analysis must actually serve, and they explain why techniques that look impressive on balanced benchmarks can disappoint in production.

A further complication is that the estate under analysis is non-stationary. Software is redeployed many times a day, dependency graphs are rewired, traffic patterns shift with product launches and time zones, and adversaries deliberately alter their behaviour to evade detection. The "normal" against which anomalies are judged is thus a moving target, and any model that encodes a fixed notion of normality will decay. This non-stationarity is qualitatively different from the settings in which many machine-learning methods were validated, and it places a premium on approaches that are transparent enough to be audited, cheap enough to be retrained, and modest enough in their claims that human analysts can catch them when they drift. These considerations frame the argument, developed throughout the paper, that the near-term contribution of AI here is to concentrate scarce expert attention rather than to replace it.

The field has matured rapidly. Early work framed the problem as anomaly detection over system logs and network traffic, treating deviations from learned baselines as candidate incidents [1]. The subsequent decade brought deep learning to sequence-structured telemetry [2], the transformer architecture that underpins contemporary language understanding [3], and, most recently, large language models (LLMs) capable of summarising, reasoning over, and generating the natural-language artefacts (tickets, chat threads, runbooks, postmortems) that surround every incident [4]. In parallel, operational disciplines such as site reliability engineering (SRE) codified the incident lifecycle and made structured telemetry a first-class engineering concern [5], while incident-handling standards formalised the phases of preparation, detection, containment, eradication, recovery, and post-incident learning [6].

This convergence has produced a genuine capability shift, but also a gap between demonstration and dependable practice. Anomaly detectors that excel on curated benchmarks can flood analysts with false positives in the open world [7]. LLMs that fluently summarise an incident may also fabricate plausible but incorrect causal claims [8]. Automation that accelerates routine response can, if unchecked, propagate errors at machine speed. The purpose of this paper is therefore twofold: to consolidate what AI-assisted risk and incident analysis can reliably do today, and to set out where the research and engineering frontier should move next.

It is worth being precise about the nature of this gap, because it recurs in each capability area we survey and shapes the research agenda we propose. Demonstrations are typically conducted under conditions that quietly remove the very features that make operational incidents hard: labels are clean, the distribution is stationary, the cost of a mistake is symmetric, and a single well-posed task is evaluated in isolation. Dependable practice must contend with the opposite of each of these, noisy and delayed labels, drift, sharply asymmetric costs, and tasks that are entangled with one another and with human workflow. A model that performs well in the first setting therefore carries no guarantee of value in the second, and the burden of the field is to close this distance rather than to celebrate benchmark records. Much of what follows can be read as an inventory of where the distance is smallest today (structured detection and correlation over well-instrumented systems) and where it remains largest (faithful natural-language reasoning about causation and high-autonomy action).

A second framing commitment deserves statement at the outset. We treat the appropriate unit of analysis not as a model but as a socio-technical system comprising telemetry pipelines, models, interfaces, playbooks, and the analysts and engineers who operate them under pressure. Judged at this level, the questions that matter are not only "how accurate is the model?" but "how does the model change what a tired analyst does at three in the morning?", "what happens when it is wrong?", and "how does the organisation learn from the episode?" These questions cut across the five capability areas and motivate our repeated emphasis on grounding, explanation, evaluation, and human oversight.

We make three contributions. First, we provide a structured synthesis of advances across five capability areas, anchored to established risk and incident frameworks. Second, we present a capabilities table that clarifies, for practitioners, the inputs, methods, and outputs of each class of technique. Third, we articulate the open challenges and a corresponding research agenda, arguing that the defensible near-term posture is augmentation of human expertise rather than autonomous decision-making. The paper is intended for researchers, security and reliability engineers, and risk leaders seeking a grounded view of the domain.

Contributions on an allied portfolio of studies spanning trade law and compliance, AI and data governance, and semiconductor and edge-computing engineering inform the framing adopted here [9]–[41]. Cognate work addressing operational-technology and critical-infrastructure security provides complementary grounding [42]–[50]. A related stream of research on financial-fraud detection, audit analytics, and risk analytics reinforces these observations [51]–[65].

2. Background and Scope

2.1 Risk analytics and the operational risk view

Risk analysis concerns the identification, estimation, and prioritisation of events that could impair an organisation's objectives. In the technology and information-security context, this is operationalised through frameworks that decompose risk into threats, vulnerabilities, likelihood, and impact, and that prescribe a repeatable assessment process [66], [67]. Operational risk analytics extends this from periodic, qualitative assessment toward continuous, data-driven monitoring: rather than estimating annualised loss expectancy from expert judgement alone, teams increasingly instrument systems so that leading indicators (error rates, latency distributions, authentication anomalies, control failures) can be measured and modelled in near real time. AI enters here as a means of turning high-dimensional telemetry into calibrated signals of elevated risk.

This shift from periodic to continuous assessment changes the character of the analytical problem in ways worth making explicit. A classical risk register is a slow-moving artefact revised on a quarterly or annual cadence, populated by human judgement and reasoned about deliberatively. A continuously monitored estate, by contrast, produces a stream of evidence whose implications for risk change from minute to minute, and the analytical task becomes one of maintaining an up-to-date posterior over the state of the system rather than issuing a one-off estimate. The two views are complementary rather than competing: the register supplies the structure (which assets matter, which failure modes are plausible, what impact they carry) while the telemetry supplies the evidence that moves likelihood estimates within that structure. A recurring failure in practice is to pursue one without the other, either instrumenting heavily without a model of what the signals mean for the business, or maintaining an elegant register disconnected from any live measurement. It also helps to distinguish leading from lagging indicators, because AI is most valuable where it can convert weak leading signals into actionable warning. Lagging indicators (an outage that has already occurred, a breach already confirmed) require little inference but arrive too late to prevent loss. Leading indicators, a slow creep in tail latency, a subtle rise in authentication failures from an unusual geography, a gradual divergence between a service and its historical seasonal profile, are individually ambiguous and collectively overwhelming, which is precisely the regime in which learned models can add value by integrating many weak signals into a calibrated estimate of elevated risk. The word "calibrated" is load-bearing here: a risk signal that cannot be trusted to mean what its magnitude implies is worse than no signal at all, because it consumes attention while eroding confidence.

2.2 The incident lifecycle

An incident is a materialised risk: an event that disrupts, or threatens to disrupt, normal operations or security posture. Standard guidance structures the response as a lifecycle, preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity [6]. SRE practice adds an operational vocabulary of detection latency, time-to-acknowledge, time-to-mitigate, and blameless postmortems that convert each incident into organisational learning [5]. This lifecycle is the scaffolding onto which AI capabilities attach: detection and triage compress the front of the lifecycle, summarisation and retrieval support analysis and coordination during an event, and generative assistance accelerates the post-incident learning that closes the loop. Adversary-behaviour taxonomies such as MITRE ATT&CK provide a shared structure for describing what happened during security incidents, enabling detections and analyses to be expressed in a common language of tactics and techniques [68].

Reading the lifecycle as a sequence of distinct phases is useful, but it can obscure that the phases impose different and sometimes conflicting demands on any assisting system. Detection rewards sensitivity and speed; containment rewards caution and reversibility; post-incident learning rewards completeness and honesty about what went wrong. A capability tuned for one phase can be actively harmful in another, an aggressive automated remediation appropriate during a fast-moving denial-of-service event would be reckless during a suspected data breach, where premature action can destroy forensic evidence or tip off an adversary. Effective deployment therefore matches the posture of AI assistance to the phase, and one of the more subtle design problems in the field is recognising, in real time, which phase an evolving event is actually in. Many severe incidents are misclassified early (a security breach mistaken for a performance regression, or vice versa) and assistance that helps responders revise that framing quickly may matter more than assistance that optimises any single phase.

The metrics that SRE practice attaches to the lifecycle also deserve scrutiny, because they become the targets against which AI assistance is justified and, if chosen carelessly, the targets it will exploit. Time-to-acknowledge and time-to-mitigate are attractive because they are measurable, but optimising them in isolation can encourage premature acknowledgement, superficial mitigation that masks rather than resolves a fault, or the suppression of alerts that would have lengthened the visible response time. A mature view treats these operational metrics as proxies for the outcomes that actually matter (avoided loss, preserved trust, durable learning) and remains alert to the ways in which a well-meaning optimisation can improve the proxy while degrading the goal. This tension recurs when we consider evaluation in Section 4.

2.3 AI, machine learning, and NLP foundations

Three technical threads underpin the advances that follow. The first is statistical and deep machine learning for detection: from ensemble methods such as random forests [69] to recurrent architectures able to model temporal dependence in event sequences [70], [71]. The second is representation learning for text, where the transformer [3] and bidirectional pretraining [72] enabled models to encode the semantics of logs, tickets, and analyst notes. The third is the emergence of large, generatively pretrained language models exhibiting few-shot and instruction-following behaviour [4], [73], later characterised as general-purpose "foundation models" adaptable across many downstream tasks [74]. Retrieval-augmented generation (RAG), which conditions a language model on documents fetched from an external corpus, is a fourth thread of particular relevance because it grounds generation in verifiable organisational knowledge [75]. The scope of this paper is the application of these threads to risk and incident analysis; we treat general model training as background rather than subject matter.

Each thread carries an inductive bias that determines what it is good for, and appreciating these biases prevents the common error of reaching for the most powerful available model regardless of fit. Tree ensembles and other tabular methods excel where features are engineered and interpretable and where labelled examples, though scarce, exist; they degrade gracefully and are comparatively easy to explain, which is why they remain a sensible default for many detection tasks despite the prestige of deeper alternatives. Recurrent and sequence architectures capture order and timing, making them apt for the execution-path structure of logs and traces, but they demand more data and are harder to interpret. Text encoders convert unstructured analyst language into vectors over which similarity and retrieval become tractable, unlocking the vast reservoir of prior tickets and postmortems that most organisations accumulate but rarely exploit. Generative language models add fluent synthesis and instruction-following, but they are the least constrained of the four and the most prone to assert beyond their evidence. A principled architecture for incident analysis composes these threads according to their strengths rather than treating the largest generative model as a universal solvent.

Retrieval-augmented generation warrants particular emphasis because it addresses the specific weakness that makes generative models risky in this domain. A language model asked a question about a past incident from its parametric memory alone will answer confidently whether or not it knows, and its training corpus contains none of the organisation's private operational history. Conditioning generation on documents retrieved at query time from the organisation's own runbooks, postmortems, and telemetry both supplies the missing knowledge and, crucially, produces an auditable chain from claim to source. This turns the interaction from an oracle to be trusted into an assistant whose reasoning can be checked, which, as later sections argue, is the

property that most determines whether such systems are safe to deploy under the adversarial and time-critical conditions of real incidents.

Contributions on semiconductor, RF/MEMS and microelectronic systems engineering and biomedical imaging inform the framing adopted here [76]–[80]. Cognate work addressing IoT security and network threat mitigation provides complementary grounding [81]–[83]. A related stream of research on internal audit, risk governance, and financial-sector controls reinforces these observations [84]–[94].

3. Advances and State of the Art

3.1 Detection and anomaly analytics

Detection is the most mature application area. System logs, being semi-structured and abundant, were an early target: log-parsing techniques convert free-form messages into structured event templates [95], over which sequence models learn the normal ordering and timing of events and flag deviations. DeepLog demonstrated that a long short-term memory network trained on normal log sequences could detect anomalies as violations of learned execution patterns and, importantly, localise them to specific log keys [2]. Beyond logs, anomaly detection spans metrics (seasonal and trend-aware models over time series) and traces (graph-structured spans across microservices), with the general framing surveyed by Chandola et al. [1]. In security specifically, detection models operate over network flows, endpoint telemetry, and authentication events, mapping suspicious activity to adversary techniques [68].

It is worth distinguishing the several senses in which “anomaly” is used, because they carry different operational consequences. A point anomaly is a single observation that departs from the norm, such as a spike in error rate; a contextual anomaly is normal in general but abnormal in its context, such as heavy database load that would be unremarkable at peak hours but is suspicious at three in the morning; and a collective anomaly is a sequence that is abnormal as a pattern even though each element is individually ordinary, such as a login followed by privilege escalation followed by bulk data access. Security-relevant behaviour is disproportionately collective and contextual, which is precisely why simple thresholding fails and why sequence-aware models that learn the normal grammar of events, as DeepLog does, mark a genuine advance. The same taxonomy explains a frequent disappointment: a detector tuned to point anomalies will miss the patient, low-and-slow adversary whose every individual action looks benign.

A recurring lesson tempers these successes. Sommer and Paxson [7] observed that machine learning excels at finding similarities but that intrusion detection demands finding novel, rare deviations under extreme class imbalance and high cost of error, conditions where benchmark accuracy translates poorly to operational value. The practical consequence is that raw detection is necessary but insufficient: without downstream triage and correlation, sensitive detectors overwhelm analysts, while conservative ones miss the events that matter. The mathematics of the base rate makes this concrete: when genuine incidents are rare, even a small false-positive rate applied to an enormous volume of benign events yields an alert stream dominated by noise, so that the practical figure of merit is not accuracy or even recall but the precision achievable at a recall the organisation can tolerate. This is why the most consequential engineering work often lies not in the detector itself but in everything downstream of it, the triage, correlation, and enrichment that convert a raw score into something an analyst can act on, and why detection quality cannot be assessed in isolation from the workflow it feeds.

3.2 Alert triage, deduplication, and correlation

The volume problem shifts from raw telemetry to alerts. Large estates generate alert storms in which a single root cause manifests as hundreds of correlated notifications. AI-assisted triage addresses this through deduplication (collapsing repeated or near-identical alerts), prioritisation (ranking by learned severity and business impact), and correlation (grouping alerts that share a probable cause across time, topology, or entity). These capabilities are central to the discipline of AIOps, applying machine learning to IT operations data to reduce noise and accelerate diagnosis, whose real-world challenges and research directions were articulated by Dang et al. [96]. Correlation often exploits service dependency graphs so that alerts propagating along known call paths are consolidated into a single incident narrative, sharply reducing the cognitive load on responders and shortening time-to-acknowledge.

The value of correlation is best understood through the phenomenon it counteracts. In a densely connected estate, a single failing dependency does not announce itself once; it radiates outward, tripping health checks, timeouts, and saturation alarms in every service that touches it, so that responders are confronted not with a fault but with a symptom cloud whose shape obscures its origin. Effective correlation inverts this radiation, using the topology through which the failure propagated to collapse the cloud back toward its source. When it works, the analyst sees one incident with a suggested root cause and a ranked set of contributing signals rather than three hundred alerts; when it fails, it either fragments one incident into many or, more dangerously, fuses two genuinely independent problems into a single misleading narrative. The failure modes matter because a correlation engine sits on the critical path of every response, and its errors are inherited by everything downstream.

Prioritisation raises a distinct and underappreciated difficulty: severity is not an intrinsic property of an alert but a function of business context that the telemetry rarely encodes directly. The same database error is trivial on a batch-analytics cluster and catastrophic on the checkout path, and a model that ranks purely on signal characteristics will misjudge both. Encoding business impact (which services are revenue-critical, which customers are affected, what regulatory clocks a given event starts) requires joining operational data to organisational knowledge that lives outside the monitoring stack, and doing so is often the difference between a triage system that analysts trust and one they learn to ignore. This dependence on context is a theme that recurs across every capability area: the model is only as useful as the organisational knowledge it can be grounded in.

3.3 NLP and LLMs for summarisation, retrieval, and postmortems

The most visible recent advances involve natural language. Incidents are surrounded by text (chat channels, ticket threads, deployment notes, prior postmortems) and LLMs are well suited to compress and organise it. Three uses stand out. First, *summarisation*: condensing a sprawling incident channel into a timeline and a current-state briefing for arriving responders or executives, reducing the handover cost that plagues long-running incidents. Second, *knowledge retrieval*: answering “have we seen this before, and what fixed it?” by retrieving relevant runbooks and historical postmortems. Here retrieval-augmented generation is decisive, because grounding answers in retrieved organisational documents both improves accuracy and yields citations analysts can verify [75]. Third, *postmortem authoring*: drafting structured post-incident reviews (timeline, contributing factors, action items) from the raw record, lowering the friction that often leaves learning incomplete [5]. Techniques such as chain-of-thought prompting can improve the quality of multi-step reasoning about causes when carefully applied [97], though, as Section 5 discusses, fluency must not be mistaken for correctness.

Each of these uses rewards a different relationship between the model and the truth, and conflating them leads to predictable trouble. Summarisation during a live incident is valuable precisely because it is fast and continuously updated, but it operates on a partial and shifting record; the responsible design treats its output as a mutable working hypothesis prominently timestamped and traceable to the underlying messages, not as an authoritative account. The greatest danger in live summarisation is anchoring: a confidently phrased early summary that names a probable cause can lodge in responders' minds and bias every subsequent interpretation, so that a summary which is merely plausible can actively lengthen an incident by steering the team down a false trail. This is a case where a fluent, decisive assistant is worse than a hesitant one, and where surfacing uncertainty and dissenting evidence is a feature rather than a hedge.

Knowledge retrieval and postmortem authoring sit at opposite ends of the time pressure spectrum, which changes what "good" means for each. Retrieval during an incident must be fast, precise, and honest about the limits of its evidence; returning three highly relevant prior incidents with their resolutions is far more useful than a fluent synthesis that blends them into a plausible but non-existent precedent. Postmortem authoring, by contrast, happens after the fact and can afford deliberation, but it carries a different hazard: because the drafted narrative will become the organisation's durable memory of the event and the basis for its corrective actions, subtle misattributions of cause are more damaging than in any live setting. A model that smooths a messy, multi-causal failure into a tidy single-because story produces a document that reads well and teaches the wrong lesson. Across all three uses, the consistent design principle is that the natural-language layer should make its evidence inspectable and its uncertainty visible, so that the analyst is reasoning with the model rather than deferring to it.

3.4 Automation and orchestration

Detection and analysis feed action. Security orchestration, automation, and response, together with reliability automation, encode routine remediation (isolating a host, rotating a credential, rolling back a deployment, scaling a resource) as executable playbooks that AI can select, populate, and, at higher autonomy levels, trigger. The engineering value is consistency and speed on well-understood, low-ambiguity tasks. The engineering hazard is that machine-learning components embedded in operational pipelines accrue "hidden technical debt" (entanglement, feedback loops, and configuration fragility) that makes automated systems difficult to reason about and prone to silent failure [98]. Mature practice therefore couples automation with guardrails: staged rollouts, reversibility, and explicit approval gates for actions whose blast radius is large.

The critical design variable is autonomy, and it is best treated not as a binary but as a spectrum matched to the reversibility and blast radius of each action. At the low-risk end sit actions that are cheap to undo and narrow in effect (enriching an alert with context, opening a ticket, gathering diagnostic snapshots) where full automation is not only safe but clearly beneficial, because human involvement adds latency without adding judgement. At the high-risk end sit actions that are hard or impossible to reverse and wide in effect, failing over a datastore, revoking access for a class of users, taking a production service offline, where automated execution without a human decision is difficult to defend regardless of how confident the model is. The interesting and contested territory is the middle, where the appropriate posture is often to have the AI fully prepare an action (select the playbook, populate its parameters, assemble the supporting evidence) and present it for a single human confirmation, capturing most of the speed benefit while preserving accountability at the moment of consequence.

A further subtlety is that automation changes the system it acts upon, creating feedback loops that can destabilise the very models that drive it. If an automated remediation suppresses the symptoms a detector was trained to recognise, the detector's future training data is quietly biased; if automated scaling masks a capacity problem, the leading indicators of that problem stop appearing until the masking capacity is itself exhausted. These loops are a concrete instance of the entanglement that Sculley et al. warn of, and they argue for instrumenting automation as heavily as the systems it manages (recording what was done, why, and with what effect) so that the automation remains legible after the fact. The recurring temptation to measure success by the fraction of incidents handled without human involvement is, in this light, a dangerous metric, because it rewards exactly the opaque, high-autonomy behaviour most likely to fail silently.

3.5 Human–AI collaboration

Across all four preceding areas, the effective unit is not the model but the analyst-plus-model team. Explainability techniques help analysts calibrate trust by exposing why a detector fired or which features drove a score, whether through local surrogate explanations [99], additive feature attributions [100], or the broader programme of explainable AI surveyed by Arrieta et al. [101]. Interaction design matters as much as model quality: guidelines for human–AI interaction emphasise making system capabilities and limitations clear, conveying uncertainty, supporting efficient correction, and learning from analyst feedback [102]. The consistent finding is that AI's value in incident analysis is realised through augmentation (surfacing candidates, drafting artefacts, and retrieving precedent) while judgement about consequential action remains with accountable humans. The goal of explanation in this setting is specifically calibration, bringing the analyst's trust in a given output into line with that output's actual reliability, rather than transparency for its own sake. Miscalibration runs in both directions and both are costly. Under-trust wastes the assistance: an analyst who re-derives every result the model offers gains nothing from it and would be faster working alone. Over-trust is more dangerous, because it substitutes the model's judgement for the analyst's at exactly the moments (novel, high-severity, ambiguous incidents) when human reasoning is most needed and the model is least likely to be reliable. A well-designed explanation helps the analyst decide not merely what the model concluded but whether to believe it this time, which is why exposing the evidence behind a conclusion is often more useful than a post-hoc rationalisation of the conclusion itself. There is also a temporal dimension to the collaboration that static notions of explainability miss. Incident response is a loop, and the analyst's corrections (dismissing a false grouping, relabelling a severity, rejecting a proposed remediation) are among the most valuable signals the system can capture, both to improve future models and to build an audit trail of human judgement. Designing interactions so that correction is cheap and its consequences are visible turns each incident into a source of durable learning rather than a one-way dispensing of model outputs. This reframing, from model-as-oracle to model-as-collaborator whose outputs are continuously adjudicated and whose adjudications feed back into the system, is the through-line that connects explainability, interaction design, and the augmentation posture we advocate throughout.

3.6 Described capabilities

Table 1 summarises the five capability areas in terms of typical inputs, representative methods, and outputs, with an indication of the appropriate level of autonomy.

Table 1. AI-assisted risk and incident analysis: described capabilities.

Capability area	Typical inputs	Representative methods	Primary outputs	Appropriate autonomy
Detection & anomaly analytics	Logs, metrics, traces, network/endpoint telemetry	Log parsing; sequence models (LSTM); time-series and graph anomaly detection; supervised classifiers	Scored anomalies and candidate incidents localised to entities	Advisory; human confirmation for action
Alert triage & correlation	Raw alerts, topology/dependency graphs, historical labels	Deduplication, learned prioritisation, causal/temporal correlation (AIOps)	Consolidated, ranked incidents with probable groupings	Advisory to semi-automated suppression
NLP/LLM analysis	Chat threads, tickets, runbooks, prior postmortems	Summarisation, retrieval-augmented generation, reasoning prompts	Timelines, briefings, grounded answers, draft postmortems	Draft-and-review with human sign-off
Automation & orchestration	Verified incident state, playbook library	Playbook selection/population; policy-gated execution	Remediation actions or prepared action proposals	Automated for low-risk, gated for high-blast-radius
Human–AI collaboration	Model outputs, feature attributions, analyst feedback	Explainability (LIME, SHAP, XAI); interaction design	Calibrated trust, corrections, feedback for retraining	Human-in-the-loop by design

Contributions on enterprise cybersecurity and cyber-defense engineering inform the framing adopted here [103]–[114]. Cognate work addressing human factors and security awareness in organizational cybersecurity provides complementary grounding [115]. A related stream of research on financial analytics, planning, and enterprise decision systems reinforces these observations [116]–[130].

4. Open Challenges

4.1 Hallucination and reliability

The most acute challenge for language-model assistance is hallucination: the generation of fluent content that is unsupported or false [8]. In incident analysis the stakes are high, because a confidently stated but incorrect root cause can misdirect a response under time pressure. Retrieval

grounding mitigates but does not eliminate the problem; models can still misattribute retrieved evidence or over-generalise from it [75]. Reliability also encompasses detection models, whose performance can drift as systems, workloads, and adversary behaviour evolve, degrading silently unless monitored. The practical requirement is that AI outputs in this domain be treated as hypotheses to be verified against primary telemetry, with provenance and citations exposed by default. What makes hallucination especially corrosive here, as opposed to in casual uses of language models, is the combination of high stakes, time pressure, and the difficulty of verification at the moment of use. A responder mid-incident has neither the time nor, often, the independent information to check a confidently asserted causal claim, and the very fluency that makes the output easy to read also makes error hard to detect. The failure is not random noise that an alert reader would catch but plausible, well-formed, domain-appropriate prose that happens to be wrong, the hardest kind of error to notice. Grounding helps by attaching claims to sources, but it introduces its own failure surface: the retrieval step can surface irrelevant or outdated documents, and the model can cite a real source while misrepresenting what it says. Robust deployment therefore treats grounding not as a solved guarantee but as a chain of fallible steps, each of which must be made inspectable. Detection reliability fails in a quieter but no less serious way. Because models decay as the estate and the threat landscape shift, a detector that was well-calibrated at deployment can drift into uselessness without any visible error, it simply stops firing on events it once caught, or begins firing on benign changes it now misreads. Unlike a crash, this degradation produces no signal of its own, which means reliability in this domain is not a property a system has but a property that must be continuously measured, with the performance of the models themselves treated as telemetry to be monitored, alerted on, and periodically re-validated against fresh ground truth.

4.2 Data sensitivity and governance

Incident data is among the most sensitive an organisation holds: it contains security posture, vulnerabilities, credentials, personal data, and, in breaches, evidence of legal significance. Applying AI raises questions of where data is processed, how it is retained, whether it is used to train shared models, and how access is controlled during an active incident when normal controls may be under stress. Foundation models trained on broad corpora carry additional governance considerations around provenance and leakage [74]. Deployment must therefore respect data-handling obligations, isolate sensitive corpora, and ensure that retrieval and logging do not themselves become an exfiltration path. A distinctive feature of this domain is that the AI system becomes a concentrated repository of exactly the information an adversary most wants. A retrieval index over an organisation's runbooks and past incidents is, in effect, a curated map of its weaknesses and its standard responses to them; a compromised summarisation assistant sees the full internal narrative of a live breach. The tooling built to defend the estate thus expands its attack surface, and any assessment of these systems must weigh the risk they introduce against the risk they mitigate. This is sharpened during an active incident, when the ordinary assumption that access controls are intact may be exactly what is in question, and when responders under pressure are tempted to relax controls to move faster. Governance is further complicated by the tension between grounding and confidentiality. The same retrieval that makes generation trustworthy also copies sensitive content into prompts, embeddings, logs, and, potentially, third-party model providers, each of which is a place the data can leak or be retained beyond its intended life. Decisions that seem purely technical, where embeddings are computed, whether prompts are logged for debugging, whether interactions are used to improve a shared model, carry real

confidentiality consequences, and they must be made deliberately rather than inherited by default from a vendor's convenience. The through-line is that data governance cannot be bolted on after a system is designed for capability; it has to shape the architecture, from where computation happens to what is retained and who can see it.

4.3 Evaluation

Evaluation is arguably the field's weakest link. Detection benchmarks often fail to reflect open-world class imbalance and cost asymmetry [7], so reported accuracy overstates operational value. For LLM assistance, there is no settled methodology for measuring whether a summary is faithful, whether a retrieved answer is correct and complete, or whether a drafted postmortem improves organisational learning. Meaningful evaluation must be end-to-end and human-centred, measuring effects on time-to-mitigate, error rates, and analyst workload rather than intrinsic model metrics alone. The absence of shared, realistic benchmarks impedes both research comparability and procurement. The difficulty is partly intrinsic to the subject matter. Genuine incidents are rare, heterogeneous, and confidential, which is precisely why the public benchmarks that drive progress in other areas of machine learning are so scarce here, and why the ones that exist tend to be dated, synthetic, or narrow. An organisation cannot readily publish its breaches, and a synthetic incident stripped of the messy context that makes real ones hard is a poor proxy for the phenomenon of interest. This scarcity pushes evaluation toward each organisation's private data, which improves realism at the cost of comparability, so that claims about a technique's value become difficult to reproduce or contest across settings. The deeper problem is that the intrinsic metrics researchers can compute cheaply are only loosely connected to the outcome's practitioners care about. A summary can score well on lexical overlap with a reference while omitting the one fact that would have changed the response; a retrieval system can achieve high relevance scores while failing on the rare queries that matter most; a detector can post excellent aggregate numbers while missing the specific class of stealthy attack the organisation is most worried about. Because the ultimate criterion is a causal one, did the assistance make the human-plus-machine team faster, more accurate, or better at learning? rigorous evaluation ultimately requires studying that team, ideally through controlled comparison, and not the model alone. Such evaluation is expensive and slow, which is exactly why it is rare and why the field's confidence in its own tools outruns its evidence.

4.4 Over-automation and de-skilling

Automation that acts at machine speed can amplify errors as readily as it accelerates remediation, and the hidden technical debt of embedded ML compounds this fragility [98]. A subtler hazard is de-skilling: if analysts habitually accept AI proposals, their ability to reason independently during the novel, high-severity incidents that most demand human expertise may atrophy. Over-reliance is a known failure mode of automation generally, and it argues for interaction designs that keep humans genuinely engaged rather than nominally "in the loop" [102].

De-skilling in this domain has a cruel structure often called the irony of automation: automation handles the routine cases well, which are exactly the cases through which analysts would otherwise have built and maintained the intuition needed for the hard ones. Expertise is largely tacit, accumulated by working through many ordinary incidents, and if the ordinary incidents are handled silently by machines, the pipeline that produces senior analysts quietly dries up. The organisation then finds, at the worst possible moment (a novel, severe, fast-moving crisis that the automation cannot handle) that the humans it needs to take over have lost the fluency the

automation was built to spare them. This is a systemic risk that no single incident reveals and that accrues precisely when the automation is performing well.

There is also a failure mode in which nominal human oversight provides only the appearance of control. A responder asked to approve a stream of machine-generated proposals under time pressure, most of which are correct, will rationally lapse into rubber-stamping, and the "human in the loop" becomes a human who legitimises decisions they did not truly make. Genuine oversight requires that the human be given the evidence, the time, and the incentive to dissent, and that dissent be cheap and consequential; oversight that is merely a required click is a liability dressed as a safeguard, transferring accountability to a person who has been designed out of the actual decision. Countering both hazards points toward interaction designs that deliberately preserve human engagement, surfacing uncertainty, occasionally routing routine cases to humans to keep skills fresh, and treating the maintenance of expertise as an explicit objective rather than an assumed by-product.

Contributions on cybersecurity, data governance, and IT-risk management inform the framing adopted here [131]–[151]. Cognate work addressing enterprise IT systems, cloud migration, and service management provides complementary grounding [152]–[164]. A related stream of research on predictive analytics and data-driven decision-support systems reinforces these observations [165]–[171].

5. Future Opportunities and Research Agenda

The challenges above map onto a concrete agenda. What follows is organised as a set of directions, but they share a common logic: each seeks to close the gap between demonstration and dependable practice by making AI assistance verifiable, measurable, and controllable rather than merely more capable. The ordering reflects our judgement of near-term tractability and value, beginning with the directions most likely to yield trustworthy systems soon and ending with the socio-technical questions that will determine whether those systems are adopted well.

Grounded, verifiable reasoning. The most valuable near-term direction is to make LLM assistance verifiable by construction, tightly coupling generation to retrieval so that every claim carries provenance to primary telemetry or authoritative documents [75]. Research should target incident-specific retrieval (over heterogeneous logs, metrics, traces, and text), faithfulness metrics, and interfaces that make grounding legible to analysts under time pressure. The retrieval problem here is unusually hard because the corpus is not a homogeneous document store but a mixture of structured time series, semi-structured logs, graph-shaped traces, and free text, and the most relevant evidence for a given claim may live in a modality different from the query. Progress will require retrieval that spans these modalities and reasoning that can hold a claim accountable to evidence of a different type, grounding a natural-language assertion about a cause in the specific metric excursion and log sequence that support it. Equally important is research on faithfulness measurement itself, since a grounded system is only as trustworthy as our ability to detect when its grounding has failed.

Realistic, end-to-end evaluation. The field needs shared benchmarks and evaluation protocols that reflect open-world conditions (class imbalance, concept drift, and cost asymmetry) for detection [7], and human-centred, task-level metrics for LLM assistance. Living datasets drawn from realistic (safely anonymised) incident records, and evaluation of the human–AI team rather than the model in isolation, would materially advance the field. Because raw incident data cannot generally be shared, progress may depend on intermediate constructs: high-fidelity simulation

environments that reproduce the statistical texture of real estates, carefully anonymised or synthesised incident corpora that preserve difficulty while removing sensitivity, and standardised task definitions that let different organisations report comparable results on their own private data. The aspiration should be a "living" benchmark that evolves with the threat landscape rather than a static snapshot that degrades into a solved puzzle, and evaluation protocols that measure the human–AI team through controlled comparison rather than inferring team performance from model metrics. Establishing even modest shared conventions for reporting would let the field accumulate evidence rather than repeatedly asserting improvement.

Explainable and calibrated detection. Detectors should not only score but justify, exposing the evidence behind an alert so analysts can adjudicate quickly [99]–[101]. Coupling explanations with well-calibrated uncertainty would let triage systems route confident cases to automation and ambiguous ones to humans. Calibration deserves as much research attention as accuracy, because a system that knows what it does not know is what makes graduated autonomy possible: a detector whose confidence scores are trustworthy can safely automate the cases it is sure of and escalate the rest, whereas one whose confidence is poorly calibrated cannot be trusted to make that routing decision at all. This suggests a research programme that treats uncertainty as a first-class output, distinguishing, where possible, uncertainty arising from genuinely ambiguous evidence from uncertainty arising from the model encountering conditions unlike anything in its training, and that validates calibration under the drift and distribution shift characteristic of live estates rather than only on held-out data drawn from the same distribution as training.

Resilience-aware automation. Rather than pursuing maximal autonomy, research should formalise graduated autonomy, matching the level of automation to the reversibility and blast radius of an action, and treat the AI-in-the-loop pipeline itself as a system whose failure modes must be engineered against [98]. Techniques for safe rollback, staged action, and automation "circuit breakers" deserve systematic study. The framing worth pursuing is that the automation is itself a component of the production system, subject to the same discipline of blast-radius analysis, staged rollout, reversibility, and monitoring that mature engineering applies to any change with the potential to cause harm. This implies concrete research artefacts: formal models that relate an action's reversibility and reach to the level of autonomy it may be granted; mechanisms that detect when an automated response is failing to converge and halt it before it compounds the incident; and designs that make the automation's own state observable so that responders can understand and, if necessary, override what it is doing. The objective is not to minimise human involvement but to spend it where it changes outcomes, reserving human judgement for the irreversible and the ambiguous.

Knowledge-centred and adversary-aware analysis. Structuring institutional memory around shared taxonomies such as MITRE ATT&CK [68] would let retrieval and summarisation reason over adversary behaviour, not just surface text, and would connect incident analysis back to proactive risk assessment [67]. Because adversaries adapt, future systems must anticipate attempts to poison training data or manipulate model behaviour, making robustness an explicit design goal. Anchoring institutional memory to a shared taxonomy would let a system move beyond matching the surface text of past incidents toward reasoning about the underlying behaviours they exemplified, so that a novel intrusion can be related to prior ones through the tactics and techniques it shares even when its specific indicators are new. This same structuring closes the loop back to

proactive risk assessment, letting the patterns learned from incidents inform where controls should be strengthened before the next event. The adversarial dimension is what most distinguishes security applications from general operations: an adversary who understands that a defender relies on a learned model has an incentive to manipulate it, whether by feeding it poisoned training data, crafting inputs designed to evade detection, or probing an assistant to extract the sensitive knowledge it indexes. Robustness against a thinking opponent, rather than merely against noise, must therefore be a design goal from the outset rather than a hardening step applied afterward.

Human–AI teaming and the future of the analyst role. Finally, the field should invest in the socio-technical design of analyst–AI collaboration: how to preserve and grow human expertise, how to convey model uncertainty, and how to capture analyst corrections as durable learning signals [102]. The objective is a partnership in which AI expands the reach of scarce expertise rather than displacing the judgement on which trustworthy incident response depends. This agenda is as much organisational as technical. It asks how career paths and training must change when the routine work through which analysts once built expertise is increasingly automated, how teams should be structured so that human skill is maintained rather than eroded, and how the corrections and judgements that analysts contribute during real incidents can be captured as a durable asset rather than lost. Treating these questions as first-order research rather than as implementation details is what will determine whether the capabilities surveyed in this paper translate into resilient practice or into brittle systems that perform well in demonstrations and fail when it matters. The measure of success is not how much human effort the systems remove but how much more effective they make the expertise that remains.
Contributions on enterprise IT service delivery and security operations inform the framing adopted here [172]–[178]. Cognate work addressing financial analytics, audit, IT-risk and governance across the wider research portfolio provides complementary grounding [179]–[350]. A related stream of research on the foundational and directly cited literature underpinning the present study reinforces these observations [1]–[8], [66]–[75], [95]–[102].

6. Conclusion

AI-assisted risk and incident analysis has crossed the threshold from research curiosity to operational practice. Detection analytics compress the flood of telemetry into candidate signals; triage and correlation tame alert storms; NLP and large language models summarise, retrieve, and draft the textual artefacts that surround every incident; and automation executes well-understood remediation at speed. Mapped onto the incident lifecycle and established risk frameworks, these capabilities demonstrably shorten the path from event to understanding. Yet the same synthesis reveals why enthusiasm must be disciplined: models hallucinate, incident data is exquisitely sensitive, evaluation remains immature, and unchecked automation can propagate error as fast as it resolves it. The through-line of our analysis is that the defensible role for AI in this domain is augmentation, grounding generation in verifiable evidence, explaining detections, and keeping accountable humans in genuine control of consequential decisions. The research agenda we set out (verifiable reasoning, realistic evaluation, explainable detection, resilience-aware automation, adversary-aware knowledge, and human–AI teaming) describes the work required to convert today's capabilities into dependable practice. Progress will be measured not by model scale but by whether these systems help expert teams respond faster, more accurately, and with better learning, under the adversarial and time-critical conditions that define real incidents.

References

1. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15, 1–58. https://doi.org/10.1145/1541880.1541882
2. Du, M., Li, F., Zheng, G., & Srikumar, V. (2017). DeepLog: Anomaly detection and diagnosis from system logs through deep learning. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1285–1298). Association for Computing Machinery. https://doi.org/10.1145/3133956.3134015
3. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. In *Advances in Neural Information Processing Systems* (Vol. 30, pp. 5998–6008). https://doi.org/10.48550/arXiv.1706.03762
4. Brown, T. B., Mann, B., Ryder, N., Subbiah, M., Kaplan, J., Dhariwal, P., Neelakantan, A., Shyam, P., Sastry, G., Askell, A., et al. (2020). Language models are few-shot learners. In *Advances in Neural Information Processing Systems* (Vol. 33, pp. 1877–1901). https://doi.org/10.48550/arXiv.2005.14165
5. Beyer, B., Jones, C., Petoff, J., & Murphy, N. R. (2016). *Site reliability engineering: How Google runs production systems*. O'Reilly Media.
6. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61 Revision 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2
7. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25
8. Ji, Z., Lee, N., Frieske, R., Yu, T., Su, D., Xu, Y., Ishii, E., Bang, Y. J., Madotto, A., & Fung, P. (2023). Survey of hallucination in natural language generation. *ACM Computing Surveys, 55*(12), Article 248, 1–38. https://doi.org/10.1145/3571730
9. Adenuga, O. M. (2022). Smart grid architectures and energy distribution for high renewable penetration: A comprehensive review of technologies, operations, and deployment pathways. International Journal of Engineering and Modern Technology, 8(5), 125–155. https://doi.org/10.56201/ijemt.v8.no5.2022.pg125.155
10. Atta, S., Onyishi, E. E., Appiah, S. A., & Adenuga, O. M. (2024). Theoretical analysis of charge transport and recombination losses in thin film solar cell architectures. International Journal of Engineering and Modern Technology, 10(10), 147–170. https://doi.org/10.56201/ijemt.v10.no10.2024.pg147.170
11. Jones, B. C., & Ominyi, M. (2020). A review of legal barriers to import-export participation for Nigerian entrepreneurs. IIARD International Journal of Economics and Business Management, 6(4), 51–70. https://doi.org/10.56201/ijebm.vol.6.no4.2020.pg51.70
12. Jones, B. C., & Ominyi, M. (2021). Developing a conceptual framework linking West African agricultural value chains to household economic stability. International Journal of Economics and Financial Management, 6(2), 89–114. https://doi.org/10.56201/ijefm.v6.no2.2021.pg89.114
13. Jones, B. C., & Ominyi, M. (2022a). A systematic review of market access outcomes from free trade agreements and duty preference programs for locally made African goods. IIARD International Journal of Economics and Business Management, 8(6), 67–95. https://doi.org/10.56201/ijebm.v8.no6.2022.pg67.95
14. Jones, B. C., & Ominyi, M. (2022b). Toward a conceptual framework for agricultural export promotion under the African Continental Free Trade Area. IIARD Journal of

Business and African Economy, 8(1), 88–118. https://doi.org/10.56201/jbae.v8.no1.2022.pg88.118

15. Jones, B. C., & Ominyi, M. (2023). Reviewing compliance frameworks for technology transfers between developed and emerging markets in an era of export controls and sanctions. World Journal of Innovation and Modern Technology, 7(2), 121–149. https://doi.org/10.56201/wjimt.v7.no2.2023.pg121.149
16. Jones, B. C., & Ominyi, M. (2024a). Applications of artificial intelligence in customs administration and trade facilitation: A review. World Journal of Innovation and Modern Technology, 8(6), 181–217. https://doi.org/10.56201/wjimt.v8.no6.2024.pg181.217
17. Jones, B. C., & Ominyi, M. (2024b). A conceptual framework for harmonizing digital trade regulations in cross-border e-commerce between the United States and Nigeria. International Journal of Economics and Financial Management, 9(9), 337–364. https://doi.org/10.56201/ijefm.v9.no9.2024.pg337.364
18. Jones, B. C., & Ominyi, M. (2025a). Conceptualizing AI-driven advisory services for expanding trade compliance access to small and medium enterprises. IIARD International Journal of Economics and Business Management, 11(12), 441–474. https://doi.org/10.56201/ijebm.vol.11.no12.2025.pg441.474
19. Jones, B. C., & Ominyi, M. (2025b). A review of legal and policy evidence on guaranteed income programs as poverty alleviation tools in the United States. Journal of Humanities and Social Policy, 11(10), 138–164. https://doi.org/10.56201/jhsp.vol.11.no10.2025.pg138.164
20. 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
21. 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
22. 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
23. 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
24. 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
25. Olodo, A., Akanbi, O., & Adenuga, O. (2025). Conceptualizing a closed-loop digital twin for real-time plasma control in large-area magnetron sputtering systems. International

Journal of Engineering and Modern Technology, 11(12), 205–227. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg205.227

26. Ominyi, M. (2020). Developing a conceptual framework for post-merger compliance integration in multi-jurisdictional banking transaction. IIARD International Journal of Banking and Finance Research, 6(3), 78–95. https://doi.org/10.56201/ijbfr.vol.6.no3.2020.pg78.95
27. Ominyi, M. (2021). Toward a conceptual framework for embedding privacy by design in corporate restructuring and transaction structuring. Journal of Accounting and Financial Management, 7(5), 152–173. https://doi.org/10.56201/jafm.vol.7.no5.2021.p152.173
28. Ominyi, M., & Anichukwueze, C. C. (2020). A review of regulatory clearance frameworks for cross-border mergers and acquisitions in African financial markets. Journal of Accounting and Financial Management, 6(4), 73–99. https://doi.org/10.56201/jafm.vol.6.no4.2020.pg73.99
29. Ominyi, M., & Anichukwueze, C. C. (2021). A systematic review of anti-money laundering and anti-bribery compliance regimes across emerging and developed markets. International Journal of Economics and Financial Management, 6(2), 89–118. https://doi.org/10.56201/ijefm.v6.no2.2021.pg89.118
30. Ominyi, M., & Anichukwueze, C. C. (2022a). A conceptual framework for harmonizing data protection compliance across GDPR, NDPR, and United States privacy regimes. International Journal of Social Sciences and Management Research, 8(5), 148–174. https://doi.org/10.56201/ijssmr.v8.no5.2022.pg148.174
31. Ominyi, M., & Anichukwueze, C. C. (2022b). Reviewing greenhouse gas disclosure and ESG compliance obligations for energy and infrastructure enterprises under evolving regulatory regimes. International Journal of Economics and Financial Management, 7(6), 94–124. https://doi.org/10.56201/ijefm.v7.no6.2022.pg94.124
32. 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
33. 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
34. 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
35. 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
36. 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

37. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025b). A review of intermediary liability and content governance obligations for digital platforms under the DSA, DMCA, and CDA regimes. International Journal of Social Sciences and Management Research, 11(8), 558–582. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg558.582
38. Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025c). 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
39. Oyesiji, S. O., Nwakamma, S., & Ojukwu, J. (2023). Parameter-efficient multilingual adaptation of on-device language models: A survey. International Journal of Engineering and Modern Technology, 9(3), 287–320. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.320
40. 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
41. 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
42. 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
43. Adebayo, A., Adegbite, M. P., & Ahmed, M. O. (2023). 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
44. 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
45. 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
46. 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
47. 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
48. 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

49. 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
50. 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
51. Abetoh, N. F., & Atakpa, M. I. (2024). Audit analytics in healthcare financial oversight: Leveraging data science to strengthen accountability in multilateral grant ecosystems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2710-2747. https://doi.org/10.32628/CSEIT2410791
52. 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
53. 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
54. Atakpa, M. I., & Abolaji, T. O. (2022). A privacy-preserving data architecture model for regulated industry analytics under GDPR and HIPAA compliance. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(3), 781-808. https://doi.org/10.32628/CSEIT22558
55. 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
56. Atakpa, M. I., Abetoh, N. F., & Akeju, B. (2024a). Advances in artificial intelligence for healthcare payment fraud detection: A review of NHS applications. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(4), 1161-1194. https://doi.org/10.32628/CSEIT26123240
57. Atakpa, M. I., Abolaji, T. O., & Abetoh, N. F. (2024b). Statistical time-series models for long-range public health trend forecasting: A review and conceptual framework. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2748-2780. https://doi.org/10.32628/CSEIT2410792
58. Atakpa, M. I., Abolaji, T. O., & Akeju, B. (2023). A review of natural language processing for social media-based public health surveillance and analytics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(6), 1030-1060. https://doi.org/10.32628/CSEIT23906783
59. Eboh, E. E., & Aliliele, C. (2023). Portfolio risk optimization models for venture capital investment strategy and fraud exposure analysis. Iconic Research and Engineering Journals, 7(4), 759-792. https://doi.org/10.64388/IREV7I4-1715305

60. Eboh, E. E., & Aliliele, C. (2024). AI-driven data analytics framework for risk assessment and detection of venture capital and private equity investment fraud in U.S. capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2624-2665. https://doi.org/10.32628/CSEIT2410787
61. Eboh, E. E., & Aliliele, C. (2025a). Advanced financial due diligence models for preventing venture capital investment fraud and strengthening investor protection. Shodhshauryam, International Scientific Refereed Research Journal, 8(5), 153-197. https://doi.org/10.32628/SHISRRJ258526
62. Eboh, E. E., & Aliliele, C. (2025b). Predictive analytics systems for investment risk monitoring in SME FinTech companies and cross-border capital markets. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(2), 3969-4010. https://doi.org/10.32628/CSEIT25113398
63. Fobellah, A. N. (2025a). Cognitive biases in financial decision-making: Implications for audit and risk management in large corporations: A conceptual review. International Journal of Science and Research Archive, 16(2), 17-22. https://doi.org/10.30574/ijsra.2025.16.2.2273
64. Fobellah, A. N. (2025b). 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
65. Fobellah, A. N. (2025c). Unintended consequences of financial regulations: A study of corporate compliance burdens: A conceptual review. International Journal of Science and Research Archive, 16(2), 29-34. https://doi.org/10.30574/ijsra.2025.16.2.2275
66. Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk management guide for information technology systems* (NIST Special Publication 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30
67. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
68. Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and philosophy* (MITRE Technical Report MTR170202). The MITRE Corporation. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
69. Breiman, L. (2001). Random forests. *Machine Learning, 45*(1), 5–32. https://doi.org/10.1023/A:1010933404324
70. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. *Neural Computation, 9*(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735
71. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature, 521*(7553), 436–444. https://doi.org/10.1038/nature14539
72. Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2019). BERT: Pre-training of deep bidirectional transformers for language understanding. In *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies* (Vol. 1, pp. 4171–4186). https://doi.org/10.18653/v1/N19-1423
73. Ouyang, L., Wu, J., Jiang, X., Almeida, D., Wainwright, C. L., Mishkin, P., Zhang, C., Agarwal, S., Slama, K., Ray, A., et al. (2022). Training language models to follow

instructions with human feedback. In *Advances in Neural Information Processing Systems* (Vol. 35, pp. 27730–27744). https://doi.org/10.48550/arXiv.2203.02155

74. Bommasani, R., Hudson, D. A., Adeli, E., Altman, R., Arora, S., von Arx, S., Bernstein, M. S., Bohg, J., Bosselut, A., Brunskill, E., et al. (2021). On the opportunities and risks of foundation models. *arXiv*. https://doi.org/10.48550/arXiv.2108.07258
75. Lewis, P., Perez, E., Piktus, A., Petroni, F., Karpukhin, V., Goyal, N., Küttler, H., Lewis, M., Yih, W., Rocktäschel, T., Riedel, S., & Kiela, D. (2020). Retrieval-augmented generation for knowledge-intensive NLP tasks. In *Advances in Neural Information Processing Systems* (Vol. 33, pp. 9459–9474). https://doi.org/10.48550/arXiv.2005.11401
76. Ejofodomi, O. A., Gideon, E. N., Oladipo, G. O., & Oshomah, E. R. (2014). Automated detection of architectural detection in mammograms using template matching. International Journal of Biomedical Science and Engineering, 2(1), 1–6.
77. Gideon, E. N. (2025b). Exploring and developing advanced RF MEMS switches for 5G applications, focusing on high performance solutions for RF front end modules. Mikailalsys Journal of Advanced Engineering International, 2(2), 171–180.
78. Gideon, E., & Erhimefe, D. E. (2025). Damage mechanisms in semiconductor materials caused by non ionizing energy in space based solar systems. International Journal of Research Publication and Reviews, 6(4), 5940–5949.
79. Erhimefe, D. E., & Gideon, E. (2025). Developing advanced materials and manufacturing processes for high performance, energy-efficient, and scalable 3D integrated circuits (ICs) and devices focusing on applications like AI and quantum computing. International Journal of Research Publication and Reviews, 6(4), 2624–2630.
80. Gideon, E. N. (2025a). Evaluation of semiconductor risk mitigation strategies in the electric vehicle supply chain. International Journal of Research Publication and Reviews, 6(4), 5934–5939.
81. 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
82. 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.
83. 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
84. 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
85. 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.
86. Agu, M. U., Akomolafe, O., & Bello, A. (2025). Advances in predictive financial risk assessment using Python-based forecasting systems. International Journal of Computer Science and Mathematical Theory, 11(11), 131-148. https://doi.org/10.56201/ijcsmt.vol.11.no11.2025.pg131.148

87. 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.
88. Akomolafe, O., & Agu, M. U. (2019a). 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.
89. Akomolafe, O., & Agu, M. U. (2019b). A review of data-driven risk evaluation models for emerging market financial institutions. Iconic Research and Engineering Journals, 3(6), 433-448.
90. Akomolafe, O., & Agu, M. U. (2019c). Advances in financial resilience through integrated governance and compliance strategies. Iconic Research and Engineering Journals, 2(10), 607-620.
91. Akomolafe, O., Agu, M. U., & Bello, A. (2023a). A conceptual model for implementing risk-based auditing in strategic financial management. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2274-2286. https://doi.org/10.62225/2583049X.2023.3.6.5359
92. Akomolafe, O., Agu, M. U., & Bello, A. (2023b). A quantitative conceptual model for assessing compliance risk in emerging economies. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2287-2296. https://doi.org/10.62225/2583049X.2023.3.6.5360
93. Akomolafe, O., Agu, M. U., & Bello, A. (2025). 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
94. Bello, A., Akomolafe, O., & Agu, M. U. (2023a). A conceptual framework for data-driven procurement risk management in multinational enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2307-2316. https://doi.org/10.62225/2583049X.2023.3.6.5363
95. He, P., Zhu, J., Zheng, Z., & Lyu, M. R. (2017). Drain: An online log parsing approach with fixed depth tree. In *2017 IEEE International Conference on Web Services (ICWS)* (pp. 33–40). IEEE. https://doi.org/10.1109/ICWS.2017.13
96. Dang, Y., Lin, Q., & Huang, P. (2019). AIOps: Real-world challenges and research innovations. In *Proceedings of the 41st International Conference on Software Engineering: Companion Proceedings* (pp. 4–5). IEEE Press. https://doi.org/10.1109/ICSE-Companion.2019.00023
97. Wei, J., Wang, X., Schuurmans, D., Bosma, M., Ichter, B., Xia, F., Chi, E., Le, Q., & Zhou, D. (2022). Chain-of-thought prompting elicits reasoning in large language models. In *Advances in Neural Information Processing Systems* (Vol. 35, pp. 24824–24837). https://doi.org/10.48550/arXiv.2201.11903
98. Sculley, D., Holt, G., Golovin, D., Davydov, E., Phillips, T., Ebner, D., Chaudhary, V., Young, M., Crespo, J.-F., & Dennison, D. (2015). Hidden technical debt in machine learning systems. In *Advances in Neural Information Processing Systems* (Vol. 28, pp. 2503–2511). https://proceedings.neurips.cc/paper/2015/hash/86df7dcfd896fcaf2674f757a2463eba-Abstract.html

99. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. In *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1135–1144). Association for Computing Machinery. https://doi.org/10.1145/2939672.2939778
100. Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. In *Advances in Neural Information Processing Systems* (Vol. 30, pp. 4765–4774). https://doi.org/10.48550/arXiv.1705.07874
101. Arrieta, A. B., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., García, S., Gil-López, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion, 58*, 82–115. https://doi.org/10.1016/j.inffus.2019.12.012
102. Amershi, S., Weld, D., Vorvoreanu, M., Fourney, A., Nushi, B., Collisson, P., Suh, J., Iqbal, S., Bennett, P. N., Inkpen, K., Teevan, J., Kikin-Gil, R., & Horvitz, E. (2019). Guidelines for human-AI interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Paper 3, pp. 1–13). Association for Computing Machinery. https://doi.org/10.1145/3290605.3300233
103. 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
104. 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
105. 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.
106. 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.
107. 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.
108. 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.
109. 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
110. 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.
111. 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.

112. 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
113. 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
114. 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
115. 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
116. Lawal, O. A., & Oduleye, T. E. (2018a). A conceptual model for financial analytics driven enterprise value creation in technology firms. Iconic Research and Engineering Journals, 2(2).
117. Lawal, O. A., & Oduleye, T. E. (2018b). A review and conceptual framework for tax governance and cross-border compliance analytics. Iconic Research and Engineering Journals, 2(5).
118. Lawal, O. A., & Oduleye, T. E. (2019a). A conceptual risk assessment model for transfer pricing in multinational corporations. Iconic Research and Engineering Journals, 2(12).
119. Lawal, O. A., & Oduleye, T. E. (2019b). Conceptualizing data driven executive decision systems for strategic financial planning. Iconic Research and Engineering Journals, 3(3).
120. Lawal, O. A., & Oduleye, T. E. (2021a). A conceptual decision model for capital allocation using financial analytics. Gyanshauryam, International Scientific Refereed Research Journal, 4(2), 269-295.
121. Lawal, O. A., & Oduleye, T. E. (2021b). Aligning financial planning analytics with corporate strategy: A conceptual integration model. Shodhshauryam, International Scientific Refereed Research Journal, 4(3), 319-346.
122. Lawal, O. A., & Oduleye, T. E. (2023a). A review of decision analytics models for sustainable profitability in technology firms. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 455-475.
123. Lawal, O. A., & Oduleye, T. E. (2023b). Behavioral financial analytics: A conceptual model for explaining enterprise performance. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2590-2604.
124. Medon, J. J., & Oduleye, T. E. (2022). A comprehensive financial reporting model for strengthening compliance and organizational accountability systems. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 768-777.
125. Medon, J. J., & Oduleye, T. E. (2023). Developing a financial planning model for sustainable profitability in dynamic business environments. Shodhshauryam, International Scientific Refereed Research Journal, 6(3), 418-447. https://doi.org/10.32628/SHISRRJ236926
126. Medon, J. J., & Oduleye, T. E. (2024). An integrated predictive analytics model for enhancing strategic financial forecasting and decision accuracy. Gyanshauryam,

International Scientific Refereed Research Journal, 7(3), 258-279. https://doi.org/10.32628/GISRRJ247322

127. Oduleye, T. E., & Medon, J. J. (2023a). A predictive model for optimizing cash flow and working capital management in corporations. Gyanshauryam, International Scientific Refereed Research Journal, 6(5), 739-754. https://doi.org/10.32628/GISRRJ236537
128. Oduleye, T. E., & Medon, J. J. (2023b). A quantitative model for measuring the strategic impact of financial analysis on enterprise growth. International Journal of Advanced Multidisciplinary Research and Studies, 3(1), 1663-1672. https://doi.org/10.62225/2583049X.2023.3.1.5334
129. Walawalkar, G., Adesuyi, M. O., Kalu, A., & Oduleye, T. E. (2025a). Executive financial dashboards for real-time strategic oversight. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2042-2054.
130. Walawalkar, G., Kalu, A., Oduleye, T. E., & Adesuyi, M. O. (2025b). Capital efficiency optimization models in high-velocity business environments. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2029-2041.
131. 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
132. 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
133. Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2023c). Advances in predictive analytics models for student retention and institutional risk management systems. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2692-2711. https://doi.org/10.62225/2583049X.2023.3.6.5990
134. Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024b). 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
135. Aliliele, C., Mbonu, I. S., & Iwuanyanwu, U. (2024c). 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
136. Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025b). 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
137. Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025c). 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
138. 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

139. 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
140. 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
141. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021a). 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
142. Mbonu, I. S., Aliliele, C., Iwuanyanwu, U., & Uzoka, E. (2021b). 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
143. 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
144. 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
145. 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
146. 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
147. Mbonu, I. S., Iwuanyanwu, U., Aliliele, C., & Uzoka, E. (2021c). 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
148. 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
149. 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

150. 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
151. 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
152. 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.
153. 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
154. 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
155. 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
156. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023a). 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
157. Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2023b). 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
158. 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
159. 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
160. 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
161. 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

162. Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2023c). 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
163. 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
164. 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
165. Adelanwa, A., Basnet, A., & Anene, U. N. (2022). Advanced AI-based decision support systems for healthcare operations and resource planning. Gyanshauryam, International Scientific Refereed Research Journal, 7(1).
166. Adelanwa, A., Basnet, A., & Anene, U. N. (2023a). 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
167. Adelanwa, A., Basnet, A., & Anene, U. N. (2023b). Predictive analytics models for financial risk detection and fraud prevention in public systems. International Journal of Advanced Multidisciplinary Research and Studies, 3(6). https://doi.org/10.62225/2583049X.2023.3.6.5969
168. Adelanwa, A., Basnet, A., & Anene, U. N. (2024). Performance intelligence models for optimization and outcome measurement in large scale public services. Shodhshauryam, International Scientific Refereed Research Journal, 6(1).
169. Anene, U. N., & Clement, T. (2022). A resilient logistics framework for humanitarian supply chains: Integrating predictive analytics, IoT, and localized distribution to strengthen emergency response systems. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(5), 398-424.
170. Anene, U. N., & Clement, T. (2024). Localized supply chain solutions for sustainable community development: A strategic model for economic revitalization and regional resilience. International Journal of Scientific Research in Science and Technology, 11(5).
171. Basnet, A., Oghenemaiga, E., & Anene, U. N. (2021). Audience segmentation and forecasting models for enhancing targeted digital marketing effectiveness. Shodhshauryam, International Scientific Refereed Research Journal, 4(5), 279-305.
172. 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.
173. 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

174. Ogbole, J. I., Okoruwa, P. O., Fadayomi, O., Abolaji, T. O., Edivri, J., & Akeju, B. (2021b). 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
175. 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.
176. 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
177. 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 Information Technology, 7(5), 371-389.
178. Oteri, O., & Edivri, J. (2024). Applied performance optimization frameworks for managing high-demand enterprise technology programs and system rollouts. Gyanshauryam, International Scientific Refereed Research Journal, 7(1), 188-210.
179. Aliliele, C., Eboh, E. E., & Oluwo, K. (2024a). Advances in variance analytics for cost control in manufacturing and industrial enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3163-3185. https://doi.org/10.62225/2583049X.2024.4.6.6012
180. Aliliele, C., Eboh, E. E., & Odihi, F. (2025a). Conceptual model for financial sustainability and strategic resource allocation in nonprofit organizations. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(6), 612-651. https://doi.org/10.32628/CSEIT251117154
181. Bola-Sadipe, D., Aliliele, C., & Eboh, E. E. (2019). Conceptual model for strategic accounting systems strengthening financial transparency and regulatory compliance. IRE Journals, 3(6), 535-564. https://doi.org/10.64388/IREV3I6-1715327
182. Bola-Sadipe, D., Aliliele, C., & Odihi, F. (2023). Conceptual model for automated financial consolidation and transparency in multinational corporations. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 414-455. https://doi.org/10.32628/GISRRJ236645
183. Bola-Sadipe, D., Eboh, E. E., & Odihi, F. (2022). Advances in data-driven tax compliance and financial reporting systems in banking institutions. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 366-403. https://doi.org/10.32628/SHISRRJ247137
184. Eboh, E. E., Aliliele, C., & Odihi, F. (2025). Advances in financial governance and accountability systems in small and medium enterprises. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2223-2245. https://doi.org/10.62225/2583049X.2025.5.6.6013
185. Oluwo, K., Bola-Sadipe, D., & Aliliele, C. (2025). Conceptual framework for data analytics driven financial decision making in banking sector organizations. Shodhshauryam, International Scientific Refereed Research Journal, 8(5), 259-302. https://doi.org/10.32628/SHISRRJ258529

186. Dada, T., Isiekwu, C. P., & Oluwo, K. (2021a). Advances in multinational cash flow consolidation and FX risk control using tiered treasury architecture. Iconic Research and Engineering Journals, 4(11), 601–620. https://doi.org/10.64388/IREV4I11-1714351
187. Dada, T., Isiekwu, C. P., & Oluwo, K. (2021b). Designing CRM-based sales forecasting models for multichannel lending institutions. Iconic Research and Engineering Journals, 5(3), 451–466. https://doi.org/10.64388/IREV5I3-1714352
188. Oluwo, K., Dada, T., & Isiekwu, C. P. (2022). A review of integrated product innovation cycles in human capital and financial services. Iconic Research and Engineering Journals, 5(12), 560–586. https://doi.org/10.64388/IREV5I12-1714353
189. 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
190. 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
191. 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
192. 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
193. 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
194. Ogbole, J. I., Okoruwa, P. O., Babatope, O. M., & Oyewole, T. (2021a). 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
195. Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Okafor, C. M., & Wedraogo, L. (2025). Artificial intelligence and the future of work: Impacts on employment and job roles. International Journal of Multidisciplinary Futuristic Development, 6(1), 31–41. https://doi.org/10.54660/IJMFD.2025.6.1.31-41
196. Filani, O. M., Nnabueze, S. B., Sakyi, J. K., & Okojie, J. S. (2023). Scenario-based financial modelling for enhancing strategic decision-making and organizational long-term planning. Journal of Frontiers in Multidisciplinary Research, 4(2), 251–265. https://doi.org/10.54660/.JFMR.2023.4.2.251-265
197. Nnabueze, S. B., Filani, O. M., Sakyi, J. K., Okojie, J. S., & Okereke, M. (2023a). Developing sustainable business models for large-scale service organizations using predictive and strategic insights. International Journal of Multidisciplinary Evolutionary Research, 4(2), 76–88. https://doi.org/10.54660/IJMER.2023.4.2.76-88

198. Nnabueze, S. B., Sakyi, J. K., Filani, O. M., Okojie, J. S., Babatope, O. M., & Adanyin, A. (2023b). Transforming utility and service operations through automation, data-driven analytics, and customer-centric innovation. International Journal of Multidisciplinary Evolutionary Research, 4(2), 40–57. https://doi.org/10.54660/IJMER.2023.4.2.40-57
199. Nnabueze, S. B., Sakyi, J. K., Filani, O. M., Okojie, J. S., Abioye, R. F., Okereke, M., & Enow, O. F. (2024). Revenue optimization in energy distribution through integrated financial planning and advanced data-driven frameworks. International Journal of Advanced Multidisciplinary Research and Studies, 4(4), 1427–1445.
200. Okafor, C. M., Wedraogo, L., Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Babalola, A. S., & Adenuga, M. A. (2025). Analysis of human resource development initiatives and employee career progression. International Journal of Multidisciplinary Futuristic Development, 6(1), 55–64. https://doi.org/10.54660/IJMFD.2025.6.1.55-64
201. Okojie, J. S., Filani, O. M., Ihwughwavwe, S. I., & Sakyi, J. K. (2020). Sustainable procurement practices: ESG-integrated supply chain models for corporate responsibility and environmental performance. IRE Journals, 4(2).
202. Sakyi, J. K., Nnabueze, S. B., Filani, O. M., Okojie, J. S., & Okereke, M. (2022b). Customer service analytics as a strategic driver of revenue growth and sustainable business competitiveness. Journal of Frontiers in Multidisciplinary Research, 3(2), 109–123. https://doi.org/10.54660/.IJFMR.2022.3.2.109-123
203. Sakyi, J. K., Eboseremen, B. O., Adebayo, A. O., Essien, I. A., Okojie, J. S., & Soneye, O. M. (2024a). Designing a sustainable financing model for emerging economies: Addressing climate goals through green bonds and ESG investments. International Journal of Multidisciplinary Futuristic Development, 5(1), 20–33. https://doi.org/10.54660/IJMFD.2024.5.1.20-33
204. Sakyi, J. K., Filani, O. M., Nnabueze, S. B., Okojie, J. S., & Ogedengbe, A. O. (2022a). Developing KPI frameworks to enhance accountability and performance across large-scale commercial organizations. Journal of Frontiers in Multidisciplinary Research, 3(2), 81–93. https://doi.org/10.54660/.IJFMR.2022.3.2.81-93
205. Sakyi, J. K., Nnabueze, S. B., Filani, O. M., & Okojie, J. S. (2023). Revenue assurance strategies leveraging artificial intelligence and big data in service-intensive organizations. International Journal of Multidisciplinary Evolutionary Research, 4(2), 58–75. https://doi.org/10.54660/IJMER.2023.4.2.58-75
206. Sakyi, J. K., Nnabueze, S. B., Filani, O. M., Okojie, J. S., & Babatope, O. M. (2024b). Digital transformation in service delivery leveraging automation and risk reduction for long-term commercial efficiency. International Journal of Advanced Multidisciplinary Research and Studies, 4(4), 1446–1464.
207. Wedraogo, L., Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Okafor, C. M., Babalola, A. S., & Adenuga, M. A. (2025). Analysis of vendor management practices and their effects on supply chain performance. International Journal of Multidisciplinary Futuristic Development, 6(1), 42–54. https://doi.org/10.54660/IJMFD.2025.6.1.42-54
208. Michael, O. N., & Ogunsola, O. E. (2021b). Assessing the role of digital agriculture tools in shaping sustainable and inclusive food systems. Gyanshauryam, International Scientific Refereed Research Journal, 4(4), 154-181.
209. Michael, O. N., & Ogunsola, O. E. (2022a). Examining the socioeconomic barriers to technological adoption among smallholder farmers in remote rural areas. Shodhshauryam, International Scientific Refereed Research Journal, 5(6), 484-519.

210. Michael, O. N., & Ogunsola, O. E. (2025d). Evaluating the impact of sustainable agriculture curriculum integration on STEM education and career outcomes. Journal of Social Science and Human Research Studies, 1(5), 178-194. https://doi.org/10.65150/EP-jsshrs/V1E5/2025-03
211. Aminu-Ibrahim, A. Y., & Ogbete, J. C. (2023). Healthcare infrastructure as a public health intervention using evidence from large laboratory networks. Shodhshauryam, International Scientific Refereed Research Journal, 6(1), 256-286. https://doi.org/10.32628/SHISRRJ23678
212. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2018). Developing sustainable diagnostic laboratory infrastructure models for emerging and resource constrained health systems. Iconic Research and Engineering Journals, 1(8), 118-132. https://doi.org/10.64388/IREV1I8-1713586
213. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2019). Capital project delivery models for high risk healthcare infrastructure in developing national health systems. Iconic Research and Engineering Journals, 2(10), 626-649. https://doi.org/10.64388/IREV2I10-1713588
214. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2020). Infrastructure driven expansion of diagnostic access across underserved and rural healthcare regions. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 691-706. https://doi.org/10.54660/IJMRGE.2020.1.5.691-706
215. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Ambali, K. B. (2024). Governance and accountability models for public private partnerships in healthcare infrastructure development. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2943-2960. https://doi.org/10.62225/2583049X.2024.4.6.5699
216. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Iwuanyanwu, O. C. (2025a). Cost control and financial accountability frameworks for national healthcare construction programs. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 1970-1990. https://doi.org/10.62225/2583049X.2025.5.6.5700
217. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Iwuanyanwu, O. C. (2025b). Infrastructure resilience planning for national diagnostic systems under public health stress conditions. Gyanshauryam, International Scientific Refereed Research Journal, 8(1), 340-381. https://doi.org/10.32628/GISRRJ2582311
218. Aminu-Ibrahim, A. Y., Ogbete, J. C., & Iwuanyanwu, O. C. (2025c). Sustainable healthcare infrastructure performance metrics for long-term asset management and value creation. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(4), 566-601. https://doi.org/10.32628/CSEIT251116277
219. Ogbete, J. C., & Aminu-Ibrahim, A. Y. (2024). Translating healthcare infrastructure investment into measurable population health and diagnostic outcomes. International Journal of Scientific Research in Humanities and Social Sciences, 1(2), 955-985. https://doi.org/10.32628/IJSRSSH242775
220. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2018). Optimizing laboratory spatial planning strategies to improve diagnostic accuracy, safety, and clinical throughput. Iconic Research and Engineering Journals, 2(1), 87-113. https://doi.org/10.64388/IREV1I7-1713587
221. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2019). Regulatory compliant design systems for molecular and pathology laboratories in highly controlled environments. Iconic

Research and Engineering Journals, 3(4), 607-631. https://doi.org/10.64388/IREV3I4-1713589

222. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2020). Sustainable materials selection and energy efficiency strategies for modern medical laboratory facilities. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 674-690. https://doi.org/10.54660/IJMRGE.2020.1.5.674-690
223. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2021). Risk managed construction strategies for complex and highly regulated healthcare facility developments. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 362-392. https://doi.org/10.32628/CSEIT217561
224. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2022). Design standards and operational planning frameworks for scalable blood collection networks. Gyanshauryam, International Scientific Refereed Research Journal, 5(6), 267-300. https://doi.org/10.32628/GISRRJ225635
225. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Ambali, K. B. (2023). Lifecycle performance evaluation of purpose built diagnostic laboratories supporting long term healthcare delivery. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2605-2621. https://doi.org/10.62225/2583049X.2023.3.6.5698
226. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Iwuanyanwu, O. C. (2025a). Digital and BIM enabled coordination methods for delivering complex medical facility projects. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 1991-2010. https://doi.org/10.62225/2583049X.2025.5.6.5701
227. Ogbete, J. C., Aminu-Ibrahim, A. Y., & Iwuanyanwu, O. C. (2025b). Integrating healing-centered design principles into diagnostic and laboratory facility planning. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(6), 516-553. https://doi.org/10.32628/CSEIT251117149
228. Arumosoye, O. M., & Obriki, O. D. (2018). Development of an integrated heat stress risk conceptual model for industrial operations in extreme environments. Iconic Research and Engineering Journals, 1(12), 141-160. https://doi.org/10.64388/IREV1I12-1714415
229. Arumosoye, O. M., & Obriki, O. D. (2019). Systematic review of near-miss and hazard observation data utilization in industrial safety management. Iconic Research and Engineering Journals, 3(2), 981-999. https://doi.org/10.64388/IREV3I2-1714417
230. Arumosoye, O. M., & Obriki, O. D. (2020). A governance-oriented conceptual model for contractor safety performance in multi-contract industrial projects. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 728-740. https://doi.org/10.54660/.IJMRGE.2020.1.5.728-740
231. Arumosoye, O. M., & Obriki, O. D. (2021). Organizational learning-based conceptual maturity model for continuous safety performance improvement. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), 970-980. https://doi.org/10.54660/.IJMRGE.2021.2.1.970-980
232. Arumosoye, O. M., & Obriki, O. D. (2022). Conceptual risk pathway model for lifting and rigging operations in heavy industrial construction. Gyanshauryam, International Scientific Refereed Research Journal, 5(5), 346-369. https://doi.org/10.32628/GISRRJ2256237
233. Arumosoye, O. M., & Obriki, O. D. (2023). Conceptual model for emergency response readiness and capability in energy and process facilities. International Journal of Scientific

Research in Computer Science, Engineering and Information Technology, 9(3), 897-917. https://doi.org/10.32628/CSEIT25112791

234. Arumosoye, O. M., & Obriki, O. D. (2024). Conceptual model of safety leadership influence in large temporary project organizations. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3034-3047. https://doi.org/10.62225/2583049X.2024.4.6.5895
235. Arumosoye, O. M., Obriki, O. D., & Ozobu, C. O. (2025). Conceptual framework for environmental risk control and ESG performance through waste handling and operational discipline. Gyanshauryam, International Scientific Refereed Research Journal, 8(4), 177-198. https://doi.org/10.32628/GISRRJ258367
236. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020a). Advances in internal QHSE audit systems for industrial engineering operations. Iconic Research and Engineering Journals, 4(4), 399-417. https://doi.org/10.64388/IREV4I4-1715499
237. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020b). Conceptual risk management model for heavy lifting and crane installation engineering operations. Shodhshauryam, International Scientific Refereed Research Journal, 3(4), 122-144. https://doi.org/10.32628/SHISRRJ214441
238. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2020c). Critical review of occupational safety management systems in oil and gas maintenance projects. Shodhshauryam, International Scientific Refereed Research Journal, 3(4), 145-166. https://doi.org/10.32628/SHISRRJ214442
239. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2021a). Advances in proactive hazard recognition and near miss reporting systems. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 835-846. https://doi.org/10.54660/IJMRGE.2021.2.6.835-846
240. Obogo, S. F., Arumosoye, O. M., & Obriki, O. D. (2024a). Review of sustainable environmental practices in occupational safety management systems. International Journal of Scientific Research in Civil Engineering, 8(3), 164-196. https://doi.org/10.32628/IJSRCE248420
241. Obogo, S. F., Nwafor, M. I., & Ozobu, C. O. (2023). Conceptual leadership model for safety culture development in construction and engineering projects. International Journal of Scientific Research in Civil Engineering, 7(6), 121-153. https://doi.org/10.32628/IJSRCE237554
242. Obogo, S. F., Obriki, O. D., & Arumosoye, O. M. (2021b). Conceptual model for incident prevention in industrial maintenance engineering environments. International Journal of Multidisciplinary Research and Growth Evaluation, 2(6), 847-858. https://doi.org/10.54660/IJMRGE.2021.2.6.847-858
243. Obogo, S. F., Obriki, O. D., & Arumosoye, O. M. (2022). Conceptual safety governance model for large commercial facility operations. Gyanshauryam, International Scientific Refereed Research Journal, 5(6), 383-410. https://doi.org/10.32628/GISRRJ225639
244. Obogo, S. F., Ozobu, C. O., & Nwafor, M. I. (2024b). Conceptual environmental safety compliance framework for construction and infrastructure projects. International Journal of Scientific Research in Civil Engineering, 8(3), 132-163. https://doi.org/10.32628/IJSRCE248419

245. Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019a). Advances in leadership driven safety culture transformation in large construction workforces. Iconic Research and Engineering Journals, 3(5), 507-523. https://doi.org/10.64388/IREV3I5-1715497
246. Obogo, S. F., Ozobu, C. O., & Uduokhai, D. O. (2019b). Development of a construction safety risk governance model for multi contractor high rise projects. Iconic Research and Engineering Journals, 2(9), 502-522. https://doi.org/10.64388/IREV2I9-1715495
247. Obogo, S. F., Ozobu, C. O., Nwafor, M. I., & Adio, S. A. (2025a). Advances in hazard identification systems for large scale construction operations. International Journal of Scientific Research in Civil Engineering, 9(6), 37-70. https://doi.org/10.32628/IJSRCE2154969
248. Obogo, S. F., Ozobu, C. O., Sanusi, A. N., & Ajirotutu, R. O. (2025b). Conceptual integrated safety management model for multi zone urban infrastructure projects. International Journal of Scientific Research in Civil Engineering, 9(5), 22-55. https://doi.org/10.32628/IJSRCE2593012
249. Obogo, S. F., Uduokhai, D. O., & Ozobu, C. O. (2019c). Systematic review of hazard identification and risk control practices in urban construction projects. Iconic Research and Engineering Journals, 2(12), 666-681. https://doi.org/10.64388/IREV2I12-1715496
250. Obogo, S. F., Uduokhai, D. O., & Ozobu, C. O. (2021c). Review of contractor safety compliance systems in infrastructure engineering projects. International Journal of Scientific Research in Civil Engineering, 5(4), 76-100. https://doi.org/10.32628/IJSRCE215412
251. Obriki, O. D., & Arumosoye, O. M. (2018). Conceptual modeling of data-driven occupational safety risk control in large-scale energy infrastructure projects. Iconic Research and Engineering Journals, 1(7), 169-189. https://doi.org/10.64388/IREV1I7-1714414
252. Obriki, O. D., & Arumosoye, O. M. (2019). A conceptual framework linking management safety walkthrough frequency and coverage to safety culture outcomes in mega projects. Iconic Research and Engineering Journals, 2(8), 355-374. https://doi.org/10.64388/IREV2I8-1714416
253. Obriki, O. D., & Arumosoye, O. M. (2020). Conceptual framework for human error causation in high-risk construction and industrial activities. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 715-727. https://doi.org/10.54660/.IJMRGE.2020.1.5.715-727
254. Obriki, O. D., & Arumosoye, O. M. (2021). Conceptual model for institutionalizing life-preserving safety practices across project-based organizations. International Journal of Multidisciplinary Research and Growth Evaluation, 2(1), 961-969. https://doi.org/10.54660/.IJMRGE.2021.2.1.961-969
255. Obriki, O. D., & Arumosoye, O. M. (2022). Conceptual framework explaining recurrence mechanisms of unsafe behaviors in high-hazard worksites. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 380-402. https://doi.org/10.32628/SHISRRJ225489
256. Obriki, O. D., & Arumosoye, O. M. (2023). Conceptual framework for proactive hazard identification using digital safety data streams. Gyanshauryam, International Scientific Refereed Research Journal, 6(3), 457-481. https://doi.org/10.32628/GISRRJ236336
257. Obriki, O. D., & Arumosoye, O. M. (2024a). Conceptual governance framework for subcontractor safety performance management. International Journal of Advanced

Multidisciplinary Research and Studies, 4(6), 3020-3033. https://doi.org/10.62225/2583049X.2024.4.6.5894

258. Obriki, O. D., & Arumosoye, O. M. (2024b). Systematic review of incident investigation approaches and prevention-oriented learning in industrial operations. Shodhshauryam, International Scientific Refereed Research Journal, 7(4), 239-263. https://doi.org/10.32628/SHISRRJ247163
259. Obriki, O. D., Arumosoye, O. M., & Obogo, S. F. (2023a). Advances in continuous hazard monitoring systems for workplace safety. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2742-2759. https://doi.org/10.62225/2583049X.2023.3.6.6075
260. Obriki, O. D., Arumosoye, O. M., & Ozobu, C. O. (2025). Conceptual model linking leading safety signals to sustained injury-free project performance. International Journal of Scientific Research in Humanities and Social Sciences, 2(3), 233-254. https://doi.org/10.32628/IJSRHSS252342
261. Obriki, O. D., Obogo, S. F., & Arumosoye, O. M. (2022a). Advances in workforce safety training models for operational risk reduction. Gyanshauryam, International Scientific Refereed Research Journal, 5(6), 349-382. https://doi.org/10.32628/GISRRJ225638
262. Obriki, O. D., Obogo, S. F., & Arumosoye, O. M. (2022b). Review of emergency preparedness and evacuation systems in high density commercial buildings. Gyanshauryam, International Scientific Refereed Research Journal, 5(6), 411-438. https://doi.org/10.32628/GISRRJ225640
263. Obriki, O. D., Obogo, S. F., & Arumosoye, O. M. (2023b). Review of behavioral safety programs for risk reduction in large workforces. International Journal of Advanced Multidisciplinary Research and Studies, 3(6), 2760-2775. https://doi.org/10.62225/2583049X.2023.3.6.6076
264. Dagodzo, D. (2018a). A conceptual framework for UAV integration into national power grid inspection programs. Iconic Research and Engineering Journals, 2(5), 391-412. https://doi.org/10.64388/IREV2I5-1716082
265. Dagodzo, D. (2018b). A review of UAV applications in electrical transmission line inspection: Methods, technologies, and challenges. Iconic Research and Engineering Journals, 2(6), 234-254. https://doi.org/10.64388/IREV2I6-1716083
266. Dagodzo, D., & Ahiaeke Patrick, M. C. (2020). UAV-based pipeline and corridor monitoring: A review of current practices and emerging technologies. Iconic Research and Engineering Journals, 3(10), 574-597. https://doi.org/10.64388/IREV3I10-1716084
267. Dagodzo, D., & Ahiaeke Patrick, M. C. (2021a). A review of GIS applications in utility asset management and infrastructure planning. Iconic Research and Engineering Journals, 5(3), 468-492. https://doi.org/10.64388/IREV5I3-1716085
268. Dagodzo, D., & Ahiaeke Patrick, M. C. (2021b). An integrated framework for UAV, LiDAR, and GIS in infrastructure corridor management. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(5), 497-524. https://doi.org/10.32628/CSEIT217566
269. Dagodzo, D., & Ahiaeke Patrick, M. C. (2022). A review of right-of-way encroachment detection methods using geospatial technologies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(1), 638-667. https://doi.org/10.32628/CSEIT2281226

270. Dagodzo, D., & Ahiaeke Patrick, M. C. (2023a). A framework for integrating drone operations into enterprise GIS systems for utility companies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(4), 924-957. https://doi.org/10.32628/CSEIT23564536
271. Dagodzo, D., & Ahiaeke Patrick, M. C. (2023b). A review of UAV regulatory frameworks in developing economies: Progress, gaps, and recommendations. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(4), 958-994. https://doi.org/10.32628/CSEIT23564537
272. Dagodzo, D., & Ahiaeke Patrick, M. C. (2025). A framework for national-scale UAV deployment in power infrastructure: Lessons from developing economies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11(4), 779-824. https://doi.org/10.32628/CSEIT251116286
273. Dagodzo, D., Ahiaeke Patrick, M. C., & Aliliele, C. (2022). AI and deep learning for vegetation classification in power corridor management: A review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(1), 668-698. https://doi.org/10.32628/CSEIT2281227
274. Bello, K. A., Oyelaran, O. A., Tawose, O. M., Omoyi, C. O., & Yussouff, A. A. (2024). Development of a gum production machine from Manihot esculenta waste peels. FUOYE Journal of Innovation Science and Technology, 2(1). https://www.jist.fuoye.edu.ng/index.php/jist/article/view/48
275. Bello, K. A., Azeez, T. M., Tawose, O. M., Odesanya, K. O., Odumosu, O. A., & Oyelaran, O. A. (2023b). Investigating the influence of rubber seed oil and used cooking oil on diesel. E3S Web of Conferences, 430, Article 01217. https://doi.org/10.1051/e3sconf/202343001217
276. Monye, S. I., Bello, K. A., Omotehinse, S. A., Ikumapayi, O. M., Tawose, O. M., Adeleke, T. B., Awogbemi, O., Monye, N. S., & Boboye, O. (2025a). Achieving energy sustainability in Nigeria's telecommunications industry through renewable propane. NIPES Journal of Science and Technology Research, 7(2), 3320-3325. https://doi.org/10.37933/nipes/7.4.2025.SI398
277. Monye, S. I., Daniyan, I. A., Monye, N. S., Ikumapayi, O. M., Bello, K. A., Boboye, O., Awogbemi, O., Tawose, O. M., & Adesoji, A. A. (2025b). Hydrogen infrastructure for a sustainable future: Challenges, innovations, and global opportunities. NIPES Journal of Science and Technology Research, 7(2), 3302-3308. https://doi.org/10.37933/nipes/7.4.2025.SI395
278. 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.
279. Sunday, E. A., & Omoegun, G. O. (2018). Integrating solar power solutions in small-scale manufacturing industries in Nigeria. International Journal of Scientific Research in Science, Engineering and Technology, 4(8), 832-853.
280. Sunday, E. A., & Omoegun, G. O. (2019). Optimizing electrical load distribution for hybrid solar installations in developing economies. International Journal of Scientific Research in Mechanical and Materials Engineering, 3(6), 27-47.
281. 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.

282. Sunday, E. A., Omoegun, G. O., Essien, M. A., & Oluokun, O. A. (2019). Thermodynamic efficiency and control strategies in residential air conditioning systems. International Journal of Scientific Research in Civil Engineering, 3(3), 52-76.
283. 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.
284. Akanbi, O., & Sunday, E. A. (2024). An integrated path-planning and slotting optimization model for AMR-enabled high-density warehousing. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3226-3243. https://doi.org/10.62225/2583049X.2024.4.6.6181
285. 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
286. 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.
287. Boakye, K., Ofori, S. D., Ogbona, C. S., Yeboah, T. J., & Bobga, M. A. (2020). Integrating ICT and mathematical thinking: Exploring the effectiveness of digital tools in secondary mathematics instruction. Iconic Research and Engineering Journals, 4(4), 372-398. https://doi.org/10.64388/IREV4I4-1714179
288. Boakye, K., Ofori, S. D., Ogbona, C. S., Yeboah, T. J., & Bobga, M. A. (2021). Bridging the gap: A comparative study of mathematics curriculum reforms in Ghana and the United States. Iconic Research and Engineering Journals, 5(3), 429-450. https://doi.org/10.64388/IREV5I3-1714180
289. Bobga, M. A., Boakye, K., Ogbona, C. S., & Yeboah, T. J. (2018). Pedagogical strategies for teaching students with learning difficulties in resource-constrained schools. Iconic Research and Engineering Journals, 2(4), 173-194. https://doi.org/10.64388/IREV2I4-1714176
290. Bobga, M. A., Boakye, K., Ogbona, C. S., & Yeboah, T. J. (2025). Reforming teacher education curricula to address special learning needs: Lessons from U.S. and African institutions. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2087-2103.
291. Githinji, L., & Atobatele, F. (2025a). A structured advising and mentorship framework for academic recovery: Conceptualizing the pathways from probation to persistence in undergraduate STEM students. International Journal of Social Sciences and Management Research, 11(12), 700-720. https://doi.org/10.56201/ijssmr.vol.11no12.2025.pg700.720
292. Githinji, L., & Atobatele, F. (2025b). Belonging-centered retention: A conceptual model linking mentorship, advising, and institutional belonging to persistence among underrepresented STEM students. Journal of Humanities and Social Policy, 11(10), 138-152. https://doi.org/10.56201/jhsp.vol.11.no10.2025.pg138.152
293. Kpoka, M. I. (2023). Comparative analysis of administrative French in Francophone African states and its impact on translation practice. Journal of Public Administration and Social Welfare Research, 8(2), 149-163. https://doi.org/10.56201/jpaswr.v8.no2.2023.pg149.163

294. Kpoka, M. I. (2024). Terminological challenges in the translation of civil registry and administrative documents. International Journal of Social Sciences and Management Research, 10(11), 552-578. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.552.578
295. Lilian, I. N., Liadi, K. O., & Yeboah, T. J. (2024). Multilingual ecofeminism and environmental justice: Rethinking gender, language, and ecology in global contexts. Journal of Humanities and Social Policy, 10(6), 195-222. https://doi.org/10.56201/jhsp.v10.no6.2024.pg195.222
296. Lilian, I. N., Liadi, K. O., & Yeboah, T. J. (2025a). Intersectionality, language, and identity: Multilingual perspectives on inclusion and social justice. Iconic Research and Engineering Journals, 8(9), 1761-1788. https://doi.org/10.64388/IREV8I9-1713695
297. Lilian, I. N., Liadi, K. O., & Yeboah, T. J. (2025b). Language and collaboration across the humanities and social sciences: Addressing global challenges through multidisciplinary dialogue. Iconic Research and Engineering Journals, 9(1), 2024-2050. https://doi.org/10.64388/IREV9I1-1713696
298. Lilian, I. N., Liadi, K. O., Yeboah, T. J., & Apelehin, A. A. (2020). Understanding cross-cultural communication: Identity, diversity, and global interaction. Gyanshauryam, International Scientific Refereed Research Journal, 3(4), 153-176. https://doi.org/10.32628/GISRRJ21352
299. Ogbona, C. S., Bobga, M. A., Boakye, K., & Yeboah, T. J. (2024). Leadership practices supporting Black student-athletes' mental health in collegiate sport: A qualitative inquiry. International Journal of Multidisciplinary Research and Growth Evaluation, 5(5), 1192-1208. https://doi.org/10.54660/.IJMRGE.2024.5.5.1192-1208
300. Ogbona, C. S., Yeboah, T. J., Bobga, M. A., & Boakye, K. (2020a). Coaching education and career transition pathways: Comparative perspectives from Nigeria and the United States. Iconic Research and Engineering Journals, 4(5), 367-384. https://doi.org/10.64388/IREV4I5-1714566
301. Ogbona, C. S., Yeboah, T. J., Bobga, M. A., & Boakye, K. (2020b). Parental collaboration and student progress: Understanding home-school partnerships in special education. Iconic Research and Engineering Journals, 3(10), 552-573. https://doi.org/10.64388/IREV3I10-1714178
302. Ogbona, C. S., Yeboah, T. J., Bobga, M. A., & Boakye, K. (2023). Comparing behavioral intervention approaches for students with emotional and learning challenges. Journal of Frontiers in Multidisciplinary Research, 4(2), 349-362. https://doi.org/10.54660/.JFMR.2023.4.2.349-362
303. Oloto, A. M., & Yeboah, T. J. (2022). A comprehensive review of IDEA compliance frameworks in modern special education service delivery systems. Gyanshauryam, International Scientific Refereed Research Journal, 5(6), 323-348.
304. Oloto, A. M., & Yeboah, T. J. (2023). A systematic review of behavior intervention plan effectiveness in secondary special education programs. Gyanshauryam, International Scientific Refereed Research Journal, 6(6), 385.
305. Oloto, A. M., & Yeboah, T. J. (2024). A critical review of procedural safeguards and regulatory compliance in special education programs. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3125-3137.
306. Oloto, A. M., & Yeboah, T. J. (2025). Developing conceptual risk assessment models for special education documentation and accountability systems. International Journal of

Scientific Research in Computer Science, Engineering and Information Technology, 11(4), 691-734. https://doi.org/10.32628/CSEIT251116283

307. Seun, A., Ajayi, A., Bobga, M. A., Yeboah, T. J., Apelehin, A. A., Ofori, S. D., Elumilade, R. A., & Abutu, D. E. (2023). PearlAI and motivation paths: Advancing student engagement through AI-powered personalization in basic education. International Journal of Scientific Research in Science, Engineering and Technology, 10(4), 391-403. https://doi.org/10.32628/IJSRSET232532
308. Seun, A., Ajayi, A., Elumilade, R. A., Bobga, M. A., Yeboah, T. J., Ofori, S. D., Apelehin, A. A., & Abutu, D. E. (2024a). PearlAI: Hyperpersonalization and hyperlocalization as new AI affordances in basic education. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2553-2568. https://doi.org/10.32628/CSEIT25113574
309. Seun, A., Ajayi, A., Yeboah, T. J., Ofori, S. D., Elumilade, R. A., Apelehin, A. A., Abutu, D. E., & Bobga, M. A. (2024b). The PearlAI framework: Leveraging artificial intelligence to transform education in Africa. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(3), 1120-1132. https://doi.org/10.32628/CSEIT25113581
310. Yeboah, T. J., & Oloto, A. M. (2022). Advances in data driven IEP development: Conceptual models for supporting diverse learners. Shodhshauryam, International Scientific Refereed Research Journal, 5(1), 335-365.
311. Yeboah, T. J., & Oloto, A. M. (2023). Conceptual models for monitoring IEP implementation fidelity and educational service delivery outcomes. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9(3), 944-973.
312. Yeboah, T. J., & Oloto, A. M. (2024). Recent advances in inclusive instructional frameworks for students with diverse learning disabilities. International Journal of Scientific Research in Humanities and Social Sciences, 1(2), 1111-1135. https://doi.org/10.32628/IJSRSSH242781
313. Yeboah, T. J., & Oloto, A. M. (2025a). A review of PBIS integration models in special education behavioral support systems. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2189-2206.
314. Yeboah, T. J., & Oloto, A. M. (2025b). Advances in structured parent engagement frameworks within special education case management practices. Gyanshauryam, International Scientific Refereed Research Journal, 8(5), 93-124.
315. Yeboah, T. J., Bobga, M. A., Boakye, K., & Ogbona, C. S. (2019). Professional development and teacher competence in managing exceptional learners: A Ghanaian perspective. Iconic Research and Engineering Journals, 2(12), 618-636. https://doi.org/10.64388/IREV2I12-1714177
316. Yeboah, T. J., Bobga, M. A., Boakye, K., & Ogbona, C. S. (2022). Data-driven teaching: Using student progress data to personalize learning in special education classrooms. Journal of Frontiers in Multidisciplinary Research, 3(2), 225-240. https://doi.org/10.54660/.JFMR.2022.3.2.225-240
317. Yeboah, T. J., Bobga, M. A., Boakye, K., & Ogbona, C. S. (2024). Technology integration in special education: Enhancing student engagement and accessibility. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 2978-2993.

318. Yeboah, T. J., Bobga, M. A., Boakye, K., & Ogbona, C. S. (2025). Teacher resilience and retention in special education: Understanding the psychological factors behind burnout. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2069-2086.
319. Adenuga, O. M. (2023). Power electronics and energy efficiency in modern power systems: A comprehensive review of devices, converter topologies, and system-level practice. International Journal of Engineering and Modern Technology, 9(3), 287-312. https://doi.org/10.56201/ijcsmt.v9.no3.2023.pg287.312
320. Amayo, E. B. (2017). Multi algorithm of loss objective function of a single phase induction motor. International Journal of Development Research, 7(5), 12805-12810.
321. Amayo, E. B., & Popoola, T. T. (2017a). Multi algorithm of weight objective function of a single phase induction motor. International Journal of Trend in Research and Development, 4(2), 184-188.
322. Amayo, E. B., & Popoola, T. T. (2017b). Scientific study of telecommunication deployment in achieving quality network. International Journal of Trend in Research and Development, 4(5), 311-314.
323. Amayo, E. B., Ubeku, E., & Oshevire, P. (2015). Multi algorithm of a single objective function of a single phase induction motor. Journal of Multidisciplinary Engineering Science and Technology, 2(12), 3400-3403.
324. Oshevire, P., Eyenubo, O. J., & Amayo, B. (2017). Voltage control in the presence of distributed generation. ATBU Journal of Science, Technology and Education, 5(2), 165-173.
325. Liadi, K. O. (2022a). A policy alignment model for Nigeria's foreign policy and global climate diplomacy goals. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 790-801. https://doi.org/10.54660/.IJMRGE.2022.3.6.790-801
326. Liadi, K. O. (2022b). Developing a continental peace integration framework: Nigeria's role in African Union foreign policy initiatives. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 778-789. https://doi.org/10.54660/.IJMRGE.2022.3.6.778-789
327. Liadi, K. O. (2022c). Developing a peacebuilding effectiveness framework for Nigeria's foreign policy in West Africa. Gyanshauryam, International Scientific Refereed Research Journal, 5(1), 388-412. https://doi.org/10.32628/GISRRJ203359
328. Liadi, K. O. (2023a). A model for linking Nigeria's diplomatic engagement to sustainable development outcomes in ECOWAS states. Gyanshauryam, International Scientific Refereed Research Journal, 6(3), 392-420.
329. Liadi, K. O. (2023b). An economic interdependence model of Nigeria-China relations and its effects on industrial growth and infrastructure. Shodhshauryam, International Scientific Refereed Research Journal, 6(4), 570-599. https://doi.org/10.32628/SHISRRJ236175
330. Liadi, K. O. (2023c). Designing an oil diplomacy diversification model: Assessing the shift from petroleum influence to broader economic engagement. Shodhshauryam, International Scientific Refereed Research Journal, 6(3), 418-447. https://doi.org/10.32628/SHISRRJ236925
331. Liadi, K. O. (2024a). A soft power projection framework: Education, cultural diplomacy, and regional development in Nigeria's foreign policy. Gyanshauryam, International Scientific Refereed Research Journal, 7(2), 241-268.

332. Liadi, K. O. (2024b). Conceptualizing a governance reform impact model for Nigeria's peacekeeping missions in post-conflict states. International Journal of Advanced Multidisciplinary Research and Studies, 4(1), 1622-1636.
333. Liadi, K. O. (2024c). Designing a cross-border security cooperation model: Nigeria's foreign policy response to regional terrorism. Gyanshauryam, International Scientific Refereed Research Journal, 7(3), 311-338. https://doi.org/10.32628/GISRRJ247324
334. Liadi, K. O. (2024d). Developing a humanitarian diplomacy model: Nigeria's foreign policy and post-conflict recovery in the Sahel. Shodhshauryam, International Scientific Refereed Research Journal, 7(4), 204-233. https://doi.org/10.32628/SHISRRJ247161
335. Asiedu, C. S. (2022). Drug interaction risk in antenatal care: A conceptual framework for systematic interaction screening. Shodhshauryam, International Scientific Refereed Research Journal, 5(3), 465-484.
336. Asiedu, C. S. (2023). Diagnostic integration in infectious disease management: A review of microbiology, virology, and serology workflows. International Journal of Medical Evaluation and Physical Report, 7(4), 173-195. https://doi.org/10.56201/ijmepr.v7.no4.2023.pg173.195
337. Asiedu, C. S. (2024). Droplet digital PCR for HIV viral reservoir quantification: A review of diagnostic accuracy and clinical utility. International Journal of Medical Evaluation and Physical Report, 8(6), 253-273. https://doi.org/10.56201/ijmepr.v8.no6.2024.pg253.273
338. Asiedu, C. S., & Asiedu, A. A. (2023a). Comparative bioavailability of fresh versus dried botanical compounds: A review and cost-effectiveness modelling framework. Research Journal of Pure Science and Technology, 6(3), 226-244. https://doi.org/10.56201/rjpst.v6.no3.2023.pg226.244
339. Asiedu, C. S., & Asiedu, A. A. (2024a). Equitable access to chronic therapies in hospital pharmacy settings: A conceptual framework for continuity of care. International Journal of Medical Evaluation and Physical Report, 8(6), 274-298. https://doi.org/10.56201/ijmepr.v8.no6.2024.pg274.298
340. Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025a). Predicting throughput degradation in Wi-Fi 6 networks under varying channel conditions: A physical layer performance model. International Journal of Engineering and Modern Technology, 11(12), 205-264. https://doi.org/10.56201/ijemt.vol.11.no12.2025.pg205.264
341. Quainoo, R., Ogundapo, O., & Asiedu, W. A. (2025b). 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
342. Okojie, J. S., & Abioye, R. F. (2020). Reconciling chemical safety with circular-economy targets: A decision framework for post-consumer recycled polymers in consumer-goods packaging balancing REACH compliance, lifecycle GHG footprint, and regulatory risk. International Journal of Multidisciplinary Research and Growth Evaluation, 1(5), 992-1006.
343. Komi, N. M. (2025). Beyond one-for-one job replacement: Modeling diversification pathways for economic resilience in post-fossil-fuel regions. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2413-2446. https://doi.org/10.62225/2583049X.2025.5.6.6460
344. Komi, N. M., & Adeniji, I. O. (2020). Co-optimizing technical performance and community affordability in smart solar microgrids for underserved regions. International

Journal of Engineering and Modern Technology, 6(3), 173-212. https://doi.org/10.56201/ijemt.vol.6.no3.2020.pg173.212

345. Komi, N. M., & Adeniji, I. O. (2024b). Why energy projects survive or fail: Modeling the causal link between community trust and infrastructure durability. International Journal of Advanced Multidisciplinary Research and Studies, 4(6), 3263-3296. https://doi.org/10.62225/2583049X.2024.4.6.6459
346. Komi, N. M., & Ganiu, O. S. (2022). Grid-connected battery storage in hot and weak-grid regions: Advances, degradation challenges, and lifecycle equity. International Journal of Multidisciplinary Research and Growth Evaluation, 3(6), 1072-1095. https://doi.org/10.54660/.IJMRGE.2022.3.6.1072-1095
347. Komi, N. M., & Ganiu, O. S. (2025). When universal programs deepen inequality: A critical review of intersectional frameworks for climate justice and energy poverty. International Journal of Advanced Multidisciplinary Research and Studies, 5(6), 2380-2412. https://doi.org/10.62225/2583049X.2025.5.6.6458
348. Tackie, S. N., Komi, N. M., & Ozerdem, O. C. (2023). 31-level single-phase cascaded inverter with minimal component count. International Journal on Technical and Physical Problems of Engineering, 15(1), 271-282.
349. Adeyelu, O. O. (2019). An adaptive safety management system implementation model for aerodromes in developing economy contexts. Iconic Research and Engineering Journals, 3(4), 628-654. https://doi.org/10.64388/IREV3I4-1718479
350. Adeyelu, O. O. (2023). A risk-tiered oversight model for unmanned aircraft operations in shared controlled airspace over Nigerian airports. International Journal of Scientific Research in Civil Engineering, 7(4), 147-184. https://doi.org/10.32628/IJSRCE237419