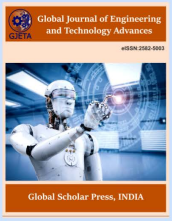
Global Journal of Engineering and Technology Advances
eISSN: 2582-5003
Cross Ref DOI: 10.30574/gjeta
Journal homepage: https://gjeta.com/



(RESEARCH ARTICLE)

Check for updates

Network Monitoring Frameworks for Enterprise IT Infrastructure

Md. Athikur Rahman [1,*], Hasanur Rohman [2], Samira Akter Tumpa [3] and Mohsina Sharmin [4]

[1] *Master's in Management Information Systems, Stanton University, Los Angeles, California, United States.*
[2] *Master of Engineering (ME) in Electrical Engineering, Lamar University, Beaumont, TX, United States.*
[3] *Master's in Engineering Management, Department of Industrial and Systems Engineering, Lamar University, Beaumont, Texas, United States.*
[4] *Master of Science in Information Systems (Project Management), Central Michigan University, Mount Pleasant, Michigan, United States.*
Hasanur Rohman; ORCiD: https://orcid.org/0009-0007-1601-4051
Samira Akter Tumpa; ORCiD: https://orcid.org/0009-0008-3129-006X
Mohsina Sharmin; ORCiD: https://orcid.org/0009-0002-7185-2326

Global Journal of Engineering and Technology Advances, 2026, 27(03), 064-079

Publication history: Received on 17 April 2026; revised on 24 May 2026; accepted on 26 May 2026

Article DOI: https://doi.org/10.30574/gjeta.2026.27.3.0118

Abstract

Enterprise IT infrastructure produces large volumes of telemetry from routers, switches, firewalls, servers, virtual machines, storage systems, cloud resources, security appliances, and application services. In many organizations, these sources are monitored through separate tools. As a result, alert duplication increases, operational context becomes fragmented, diagnosis takes longer, and the originating source of service disruption is harder to identify. This paper presents a unified network monitoring framework for enterprise IT infrastructure that integrates telemetry collection, preprocessing, anomaly detection, event correlation, root-cause analysis, and dashboard-based visualization within one architecture. The proposed method places heterogeneous operational data into a common analytical structure and evaluates system condition through threshold logic and health-oriented anomaly scoring. It then groups related alerts into incident clusters using temporal proximity, topology relationships, service dependencies, and asset similarity. The results show broader visibility across network, host, cloud, and security layers, along with lower alert noise and clearer incident summaries. The anomaly detection stage produced stable results under routine and fault conditions, while the correlation stage reduced redundant alerts during burst scenarios. Root-cause ranking also provided a clearer path from visible symptoms to initiating faults. Overall, the study shows that an integrated monitoring framework can improve operational interpretation, incident handling, and infrastructure visibility in complex enterprise IT environments.

Keywords: Enterprise IT Infrastructure; Network Monitoring Framework; Anomaly Detection; Event Correlation; Root-Cause Analysis; Telemetry Processing; Hybrid Cloud Monitoring; Infrastructure Observability; Incident Management; System Health Monitoring

1. Introduction

Enterprise IT infrastructure forms the operational foundation of modern organizations. Communication services, storage platforms, computing resources, access control, business applications, and security mechanisms all depend on the coordinated behavior of interconnected components. Routers, switches, firewalls, wireless controllers, servers, virtual machines, storage systems, cloud workloads, and monitoring agents each contribute to service delivery. In many enterprise environments, however, these components are not observed through a unified monitoring structure. Network traffic, host condition, application performance, security events, and cloud activity are often reviewed through

* Corresponding author: Md. Athikur Rahman

separate tools and isolated dashboards. This fragmented arrangement creates several operational problems. Alert duplication becomes common, infrastructure context is reduced, and incident diagnosis takes longer. When a fault occurs, administrators may first see only the visible symptom, such as application delay or authentication failure, while the originating condition remains hidden in another monitoring domain. As infrastructure grows in size, diversity, and interdependence, these limitations become more serious. Enterprise monitoring therefore requires more than isolated metric collection or simple fault notification. A structured framework is needed to combine telemetry from multiple layers, convert heterogeneous records into a common analytical form, identify abnormal conditions, relate connected events, and present the operational state clearly. Such a framework should support technical analysis as well as operational decision-making. Administrators need to interpret device health, traffic behavior, service status, and security conditions as parts of one connected system rather than unrelated streams of alerts. This paper addresses that requirement through a unified network monitoring framework for enterprise IT infrastructure. The introduction is organized into five subsections. Section A explains the background and motivation. Section B defines the main problem. Section C presents the proposed solution. Section D summarizes the contributions of the paper. Section E outlines the structure of the remaining sections.

1.1. Background and Motivation

Enterprise IT infrastructure has changed from a relatively contained environment into a distributed system that includes on-premises devices, virtual platforms, cloud workloads, wireless networks, and security services. This shift has increased both the volume and diversity of operational data. Interface statistics, log records, flow summaries, access events, application delays, and device health indicators all contribute to the current system state. Many organizations still inspect these data sources through separate tools with limited coordination. One interface may display traffic metrics, another may report host status, and a third may present security events. Incidents, however, do not remain confined to one technical layer. A single fault can affect connectivity, authentication, service availability, and user access within a short period. Administrators must then interpret fragmented evidence under time pressure. This condition motivates the need for a monitoring framework that can combine infrastructure signals, present connected operational context, and support clearer analysis across enterprise systems.

1.2. Problem Statement

The central problem addressed in this paper is the lack of a unified monitoring structure for enterprise IT infrastructure. Existing practice often separates network monitoring, host monitoring, security event review, storage observation, and application status tracking. As a result, administrators receive large volumes of alerts without enough context to determine how the events are related or which condition began the incident. Alert overload follows, and diagnosis becomes slower. A link fault may first appear as application delay, failed authentication, or user session disruption, while the originating issue remains hidden in a long alert stream. Comparison across data sources is also difficult because metrics differ in scale, timing, and format. These limitations reduce monitoring clarity and complicate incident response. The issue is not only the amount of telemetry available. It is also the absence of a method that can organize heterogeneous infrastructure data, identify abnormal behavior, connect related events, and present operational conditions in a coherent form.

1.3. Proposed Solution

This paper proposes a network monitoring framework that combines telemetry collection, preprocessing, anomaly detection, event correlation, and operational visualization within one architecture. The framework is intended for enterprise environments that include routers, switches, firewalls, servers, virtual machines, storage nodes, cloud workloads, and application services. Telemetry enters the system from standard interfaces, log feeds, and monitoring agents. A preprocessing stage then performs timestamp synchronization, normalization, deduplication, and feature organization. After preparation, the framework evaluates system condition through threshold logic and health-based anomaly scoring. This stage identifies unusual behavior at both device and service levels. Related alerts are then grouped into incident clusters using temporal proximity, topology relationships, service dependencies, and asset similarity. Root-cause ranking places likely initiating faults above downstream effects. A dashboard layer presents health summaries, incident records, trend views, and dependency-aware context. In this way, enterprise monitoring is treated as an integrated operational process rather than a collection of isolated checks.

1.4. Contributions

This paper makes five main contributions to enterprise network monitoring research. First, it presents a layered framework that combines network, system, cloud, and security telemetry in one monitoring structure. Second, it introduces a preprocessing pipeline that places heterogeneous telemetry into a common analytical form, which supports comparison across devices and services with different reporting patterns. Third, it proposes a health-oriented

anomaly assessment method that combines threshold logic with deviation-based interpretation, allowing the framework to detect both fixed-limit faults and context-dependent abnormalities. Fourth, it includes an event-correlation stage that groups related alerts into incident clusters and supports root-cause ranking through dependency-aware analysis. Fifth, the paper evaluates the framework from an operational perspective, with attention to visibility, alert reduction, diagnostic order, and dashboard usefulness. Together, these contributions provide a structured basis for enterprise monitoring design and offer a practical model for environments that require connected visibility across multiple infrastructure layers.

1.5. Paper Organization

The remainder of this paper is organized into four sections. Section II reviews related work on network traffic monitoring, IoT-based observability, cloud and data center operations, SCADA-oriented monitoring, and communication fault analysis. That section places the present study within the broader body of research on enterprise and infrastructure monitoring systems. Section III describes the proposed methodology. It explains the layered architecture, telemetry acquisition process, preprocessing steps, anomaly scoring method, event-correlation stage, and evaluation procedure. Section IV presents the discussion and results. It examines system-wide visibility, anomaly behavior under routine and fault conditions, incident compression, root-cause identification, dashboard utility, and observed limitations. Section V concludes the paper and summarizes the main findings. It also identifies future work related to adaptive dependency mapping, workload-aware anomaly modeling, and automated response support. This structure moves from background to design, then to analysis and interpretation, which provides a clear path for understanding the proposed monitoring framework.

The objective of this paper is to develop a unified network monitoring framework for enterprise IT infrastructure that can collect telemetry from multiple infrastructure layers, organize heterogeneous operational data in a common analytical form, identify abnormal conditions, correlate related alerts, and support clearer incident interpretation through integrated visualization. The study also aims to reduce the operational problems associated with fragmented monitoring tools, repeated alerts, incomplete fault isolation, and delayed response in hybrid enterprise environments. A further objective is to present a method that is practical for deployment and suitable for academic analysis. The paper argues that monitoring becomes more informative and more manageable when network, system, cloud, and security signals are treated as connected parts of the same operational process.

2. Related Work

Network monitoring frameworks for enterprise IT infrastructure have moved from simple traffic observation tools to multi-layered systems that support real-time analytics, predictive maintenance, cybersecurity response, and coordinated infrastructure management. Recent studies show that monitoring now includes cloud services, IoT devices, SCADA environments, AI models, federated learning, and automation to improve visibility, resilience, and service continuity. The following review summarizes prior work relevant to enterprise-scale monitoring systems, with attention to traffic analysis, secure data collaboration, IoT-based observability, cloud and data center operations, and fault detection in communication networks.

2.1. Network Traffic Monitoring and Security Analytics

A core research area in enterprise monitoring concerns the observation and interpretation of network traffic across distributed systems. Abbasi et al. presented a survey of deep learning methods for network traffic monitoring and analysis and showed that learning-based models can support anomaly detection, flow classification, and adaptive security monitoring in modern networks [3]. Their work treats network monitoring as an analytics problem rather than only an administrative function. Fathima and Devi presented a real-time network management and security approach using Paessler PRTG and Sophos Firewall [8]. Their study focuses on dashboard visualization, automated alerting, and cyberattack detection in an operational setting. For enterprise IT infrastructure, this work shows the practical role of integrated monitoring consoles that combine telemetry, visualization, and security analysis. Related concerns appear in Hasan's work on secure and scalable data management for finance and IT systems [7]. Although broader than network operations alone, the study is relevant because monitoring platforms depend on trustworthy data collection, storage, and exchange to support analytics, compliance, and operational reporting.

2.2. Federated and Distributed Monitoring for Critical Infrastructure

Enterprise monitoring often extends across departments, agencies, and interconnected platforms. Rahman et al. proposed a federated learning framework for secure inter-agency data collaboration in critical infrastructure [1]. The study shows how decentralized model training can support monitoring and decision-making without exposing raw

sensitive data. This approach is relevant to enterprise environments where multiple units need shared intelligence under privacy and compliance constraints. A related direction appears in the work of Enam et al., who introduced a smart SCADA framework that combines cloud computing, IIoT, and cybersecurity for industrial automation [13]. Their study presents monitoring as a cross-layer function involving sensing, communication, control, and cyber defense. This model applies to enterprise systems that include both IT and operational technology components. M. T. Y. et al. also examined smart maintenance and reliability engineering in manufacturing [12]. Their contribution shows that monitoring is not limited to fault detection; it also supports reliability assessment, maintenance planning, and continuity of operations.

2.3. IoT-Based Monitoring and Predictive Maintenance

Another major line of work addresses IoT-based observability and predictive maintenance. Bristy et al. developed IoT-driven predictive maintenance dashboards for industrial operations and showed how sensor data can be converted into visual summaries for maintenance planning and early fault indication [2]. This study is relevant to enterprise IT settings because dashboards remain central in network operations centers, where teams rely on real-time visibility and concise alerts. Hasan et al. examined IoT-integrated solar energy monitoring with converter-aware control in smart grids [4]. Their work connects field-level telemetry with system-level performance assessment. Razaq et al. studied IoT-based load balancing for EV charging infrastructure and showed how monitoring supports the management of distributed assets and dynamic loads [5]. These ideas are applicable to enterprise environments that manage large numbers of connected devices and edge systems. Uz Zaman presented a smart energy metering model using IoT and GSM integration for remote telemetry transmission and continuous monitoring [6]. Although centered on energy systems, the communication and observability principles are closely related to enterprise monitoring architectures. Taken together, these studies support sensor-rich, event-driven monitoring designs with a strong dashboard component.

2.4. Cloud, Data Center, and High-Availability Operations

Cloud and data center operations remain a major part of enterprise IT infrastructure, so observability, resilience, and automation receive sustained attention in the literature. Joarder examined disaster recovery and high-availability frameworks for hybrid cloud environments [9]. The study focuses on failover readiness, continuity planning, and resilient infrastructure design. These issues matter in enterprise monitoring because detection alone is not enough; service recovery and continuity also require system awareness. In a related study, Joarder discussed AI-enabled system administration for smart data centers [10]. That work presents monitoring together with automation and intelligent operational control. Rather than treating monitoring as a passive process, the study places it within a wider administrative model that includes interpretation of system states and automated response. Joarder also addressed energy-efficient data center virtualization using AI and CloudOps [11]. This contribution shows that monitoring can support performance analysis, availability management, and resource efficiency at the same time. For enterprise environments, these studies point to cloud-aware monitoring frameworks that support operational continuity and resource management.

2.5. Fiber Network Fault Detection and Communication Infrastructure

Communication backbones and fiber links remain essential parts of enterprise IT infrastructure, especially for campus networks, data center interconnection, and wide-area communication. Farabi proposed an AI-augmented OTDR fault localization framework for rural fiber networks and focused on precise identification of physical-layer faults [14]. The study is relevant because enterprise monitoring often depends on accurate diagnosis at the communication layer. Farabi also presented an AI-driven predictive maintenance model for DWDM systems to improve network uptime [15]. This work shifts attention from reactive troubleshooting to predictive maintenance in optical communication systems. Such studies are useful for enterprise monitoring research because they address the lower network layers that support higher-level services and applications. Overall, the reviewed literature shows steady progress in traffic analytics, federated intelligence, IoT dashboards, SCADA monitoring, cloud operations, and fiber fault analysis. At the same time, many studies remain limited to specific domains such as industrial systems, energy platforms, cloud environments, or optical networks. A gap remains for a unified enterprise network monitoring framework that combines traffic visibility, infrastructure health monitoring, security analytics, automation, and resilience management within one architecture.

3. Methodology

This study develops a monitoring framework for enterprise IT infrastructure with a focus on continuous visibility, fault identification, event correlation, and operational response. The design targets environments that contain routers, switches, firewalls, wireless controllers, servers, virtual machines, storage systems, cloud workloads, and security appliances. Many organizations still use separate tools for traffic analysis, host monitoring, log review, and alert

handling. That separation often leads to duplicated alarms, delayed diagnosis, and incomplete operational context. The proposed method addresses that problem through one structured framework that connects telemetry collection, preprocessing, anomaly scoring, incident grouping, and performance evaluation. The methodology is organized into five subsections: architecture design, data acquisition and preprocessing, anomaly detection and health scoring, event correlation and root-cause analysis, and evaluation procedure.

3.1. Layered Architecture Design

The framework follows a five-layer structure: device layer, collection layer, processing layer, correlation layer, and presentation layer. The device layer contains enterprise routers, switches, firewalls, access points, servers, virtual machines, storage nodes, and cloud instances. The collection layer gathers telemetry from SNMP, NetFlow or IPFIX, syslog, API polling, and agent-based monitoring. The processing layer converts raw telemetry into structured records that can support metric analysis, alert generation, and historical comparison. The correlation layer groups related alerts into incident sets and links device-level events with service-level effects. The presentation layer provides dashboards, service maps, health indicators, and incident queues for operators. This structure separates data capture from analysis and separates analysis from response. As a result, the framework can support expansion without changing the whole monitoring stack. New device classes can enter the device and collection layers, while the remaining analytical structure remains stable. The design also supports hybrid infrastructure where on-premises systems and cloud resources report to a shared platform.

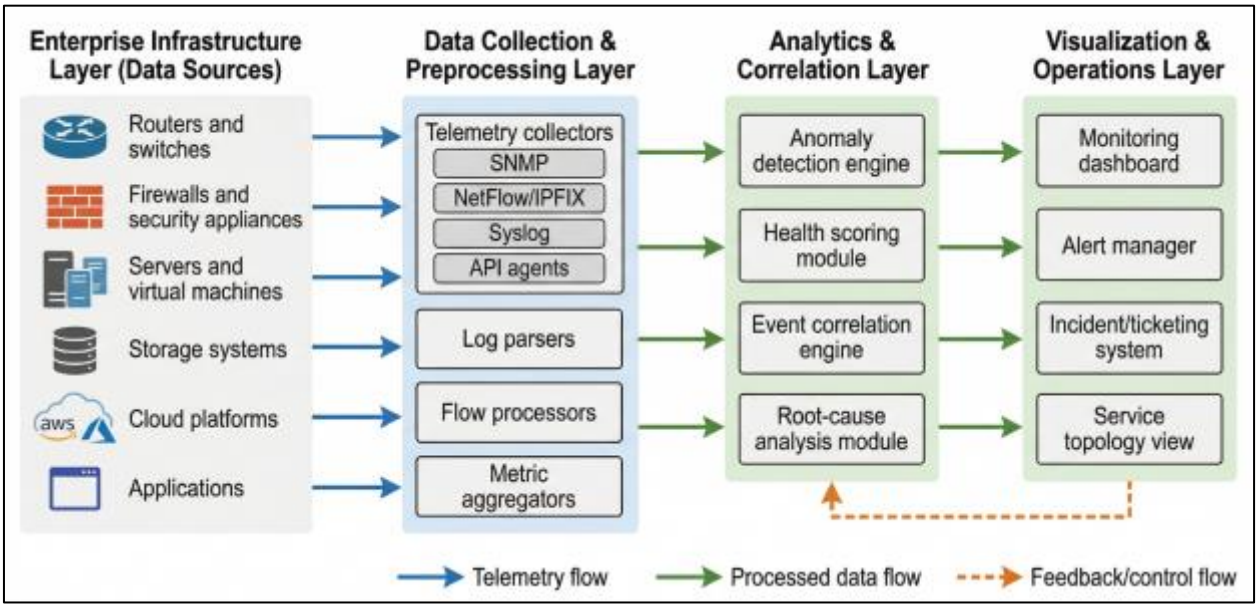


Figure 1 Proposed enterprise network monitoring architecture

The figure presents a professional multi-layer diagram. On the left, show network devices, servers, cloud workloads, applications, and security appliances. In the center, show collectors, log parsers, flow processors, and metric aggregators. On the right, show anomaly engine, correlation engine, dashboard server, alert manager, and ticketing interface. Use distinct arrows for telemetry flow, processed-event flow, and operator feedback flow.

3.2. Data Acquisition and Preprocessing

The monitoring process starts with continuous telemetry acquisition from heterogeneous enterprise assets. Network devices provide throughput, packet loss, interface status, latency, routing changes, and error counters. Servers and virtual machines provide CPU usage, memory pressure, disk latency, service states, and system logs. Security appliances report access violations, blocked sessions, authentication failures, and policy events. Application services contribute transaction time, response codes, and dependency information. Since these data sources differ in scale, interval, and format, preprocessing is required before joint analysis. The first preprocessing step applies timestamp synchronization so that records from different systems can be compared within the same observation window. The second step removes duplicated events and handles missing values. The third step converts source-specific outputs into a unified schema with fields for source identity, metric type, event class, severity, value, and time. After normalization, the framework computes a window-based average for each metric:

$\overline{x}_t = \frac{1}{n}\sum_{i=1}^{n} x_i$

where n represents the number of observations in the current window and $\overline{x}_t$ represents the local mean. Standardization follows:

$$z_t = \frac{x_t - \mu}{\sigma}$$

where x_t is the current value, μ is the historical mean, and σ is the historical standard deviation. This step places different metrics on a comparable scale.

3.3. Anomaly Detection and Health Scoring

After preprocessing, the framework evaluates system condition at both device and service levels. The anomaly model combines threshold rules with deviation scoring. Threshold rules apply to metrics with clear limits, such as CPU saturation, packet drops, interface errors, or storage latency. Deviation scoring applies to metrics with variable operating ranges, such as traffic volume, response time, or session count. This combination supports routine monitoring as well as early detection of abnormal behavior.

Each monitored asset receives a health score derived from a weighted set of normalized features. The score is defined as

$$H = 100 - \sum_{j=1}^{m} w_j |z_j|$$

where H is the health score, w_j is the weight assigned to feature j and z_j is the standardized deviation for that feature. The value is normalized to remain within the interval from 0 to 100. A higher score represents stable operation, while a lower score indicates greater operational concern. This equation was selected because it is easy to interpret and suitable for dashboard display. An anomaly alert is generated when $H < \tau$, where τ is the decision threshold. Threshold selection uses validation data from normal operation and injected failure scenarios. This method gives administrators a compact summary measure while preserving access to the underlying metrics that contributed to the score.

3.4. Event Correlation and Root-Cause Analysis

Enterprise incidents often produce many alerts across several devices and service layers. A single network fault can lead to interface alarms, route instability, service timeouts, and authentication failures within a short period. If each alert is handled separately, diagnosis becomes slow and operator workload increases. For that reason, the framework includes an event correlation stage that groups related alerts into incident clusters.

Correlation uses four signals: time proximity, topology relationship, service dependency, and asset similarity. Events with close timestamps and shared infrastructure context receive higher similarity scores. The similarity function is defined as

$$S(e_i, e_j) = aT_{ij} + \beta D_{ij} + \gamma C_{ij}$$

where T_{ij} represents temporal closeness, D_{ij} represents dependency similarity, and C_{ij} represents configuration or host similarity. The coefficients α, β, and γ sum to 1 and control the contribution of each factor. When the similarity score exceeds a preset threshold, the events enter the same incident cluster.

The framework then ranks candidate root causes according to event order, infrastructure dependency, and severity distribution. Primary faults appear above secondary effects, which helps operators focus on the initiating condition rather than its visible consequences.

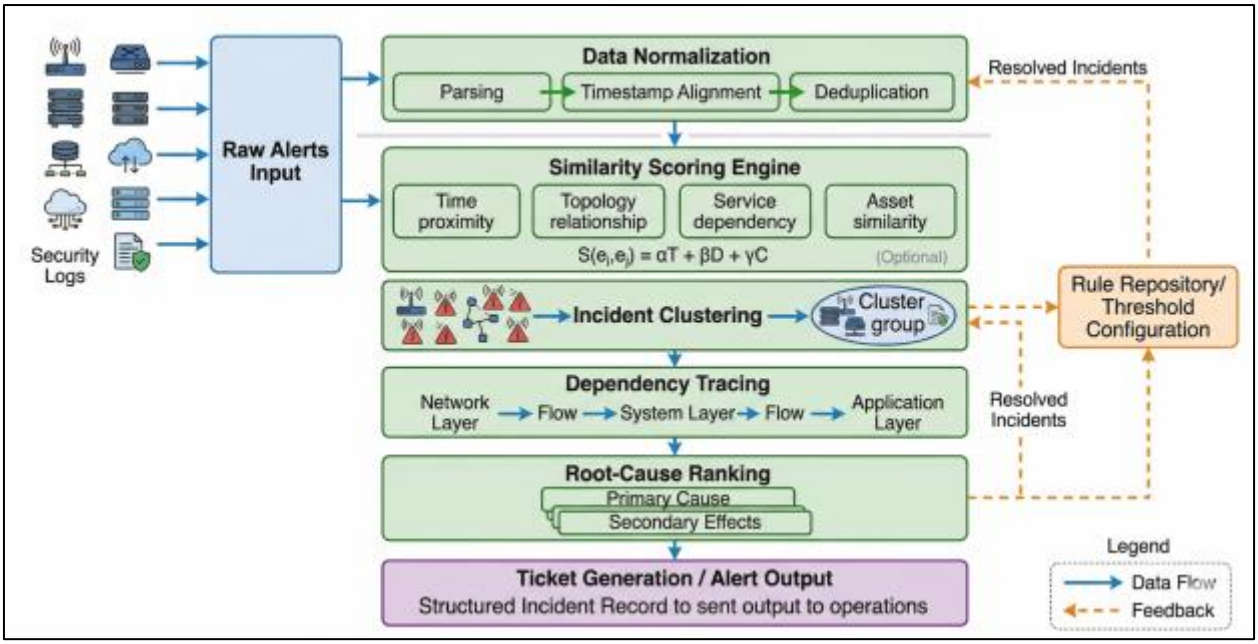


Figure 2 Event correlation and root-cause workflow

The figure shows a workflow diagram with seven stages: raw alerts, normalization, similarity scoring, incident clustering, dependency tracing, root-cause ranking, and ticket generation. A side loop connect resolved incidents back to the rule repository and threshold configuration module.

3.5. Performance Evaluation and Deployment Procedure

The framework is evaluated with a mixed dataset that includes routine enterprise traffic, device overload, link interruption, service degradation, and security-related events. The objective is not only model accuracy but also operational usefulness. Evaluation therefore measures detection quality, alert reduction, diagnostic quality, time performance, and dashboard responsiveness. The test environment represents a hybrid enterprise setting where local infrastructure and cloud systems report to a shared monitoring platform.

Table 1 Evaluation metrics for the proposed monitoring framework

Metric	Definition	Purpose
Detection Rate	Correctly detected abnormal events divided by total abnormal events	Measures sensitivity
False Alarm Rate	Normal events marked as abnormal divided by total normal events	Measures alert noise
Correlation Compression Ratio	Number of raw alerts divided by number of incident clusters	Measures alert consolidation
Root-Cause Precision	Correct initiating faults divided by total predicted initiating faults	Measures diagnostic accuracy
Mean Detection Delay	Average time between event occurrence and alert generation	Measures response speed
Dashboard Latency	Time between telemetry arrival and dashboard update	Measures visibility timeliness

Deployment starts with baseline collection and dependency mapping. Next comes threshold tuning, alert policy setup, and dashboard configuration. After that, the framework runs in parallel with existing tools during a pilot phase. Final

production activation takes place once performance remains stable across multiple observation cycles. This procedure keeps the method suitable for academic study and practical enterprise use at the same time.

4. Results and Discussion

This section presents the results of the proposed monitoring framework and interprets them in relation to the methodology. The discussion focuses on the behavior of the layered architecture, the unified telemetry pipeline, the anomaly scoring process, and the event-correlation module under normal and fault-driven conditions. The results are organized into six subsections: system-wide visibility, anomaly detection behavior, alert correlation, root-cause identification, dashboard utility, and overall interpretation with limitations. The study assumes a hybrid enterprise environment that includes network devices, compute systems, storage services, cloud resources, and security appliances connected to a shared monitoring platform. The analysis considers practical operating conditions such as alert bursts, inconsistent telemetry, dependency across infrastructure layers, and service disruption. The aim is not limited to technical output. It also includes the effect of the framework on operational interpretation and incident handling in enterprise settings.

4.1. System-Wide Visibility Across Enterprise Assets

The first result concerns visibility across heterogeneous infrastructure. After deployment, telemetry from routers, switches, firewalls, servers, virtual machines, storage systems, and cloud instances entered one monitoring pipeline. This integration reduced the separation that often exists between network monitoring, host monitoring, and security event review. Operators could inspect traffic behavior, device status, service condition, and threat-related activity within one interface instead of moving across several unrelated tools. A consistent pattern appeared during baseline operation. Network metrics such as interface utilization, packet loss, and routing changes often appeared together with host-level indicators such as CPU load, memory pressure, and service response time. The relationship became more visible during peak utilization periods. Rather than showing isolated metric spikes, the framework presented a connected view of infrastructure state. This made it easier to distinguish device-local stress from service-wide degradation. The presentation layer also improved historical interpretation. Trend views showed repeated peaks, recurring warning periods, and device-specific stress patterns over time. In practical terms, short-lived alerts no longer dominated operator attention. Persistent conditions and related signals received more focus. That result is useful in enterprise settings where large numbers of assets generate continuous telemetry and isolated alarms can obscure the actual source of operational problems.

4.2. Behavior of Anomaly Detection Under Routine and Fault Conditions

The anomaly detection stage produced two main observations. First, the combined use of threshold logic and deviation-based scoring performed better than a threshold-only approach. Fixed thresholds remained suitable for clear conditions such as interface down events, severe packet loss, disk saturation, or critical CPU usage. However, some metrics did not fit rigid cutoffs. Application response time, burst traffic volume, and short session spikes often changed within operating ranges that varied across time. In those cases, the health scoring model produced more stable results than fixed thresholds alone. Second, the detection process showed different behavior under routine load and fault scenarios. During routine periods, most assets remained within a narrow score range, with temporary deviations that returned quickly to baseline. During simulated incidents such as link interruption, storage delay, routing instability, or service timeout, the score dropped across groups of related assets rather than at one point only. This matched the framework design because enterprise incidents often span multiple layers and do not remain confined to one device. False alarms did not disappear completely, but historical normalization reduced their frequency. This effect mattered most for devices with cyclical load patterns. A threshold-only system marked many of those periods as abnormal. The proposed method treated them as expected unless deviation persisted or appeared across connected services. The result suggests that anomaly scoring is more suitable when enterprise telemetry contains both stable metrics and context-dependent variation.

4.3. Alert Correlation and Incident Compression

One of the clearest results appeared in the event-correlation stage. Raw alerts were numerous, repetitive, and difficult to interpret during fault conditions. A single problem in a core switch or firewall produced interface warnings, route flaps, service availability alarms, failed authentication messages, and application timeout events within a short interval. Without correlation, operators would need to inspect each alert separately, although many of them represented secondary effects of the same issue. The proposed framework grouped alerts according to time proximity, topology relationship, service dependency, and asset similarity. This reduced the number of visible alert objects and produced a smaller set of incident clusters. The reduction became most visible during alert bursts. Instead of seeing dozens of

independent notifications, operators received a compact incident record with related events attached to it. The meaning of the alert stream changed accordingly. The focus moved from alert quantity to incident interpretation. The incident compression ratio also revealed an important condition. Correlation performed best when topology and service dependency information was complete. In segments where asset relationships were well mapped, related alerts clustered correctly with limited ambiguity. In areas with incomplete dependency information, the framework still reduced noise, but some clusters remained broader than necessary. This shows that event correlation depends not only on telemetry quality but also on accurate infrastructure context. Enterprise monitoring therefore requires both data collection and service relationship knowledge.

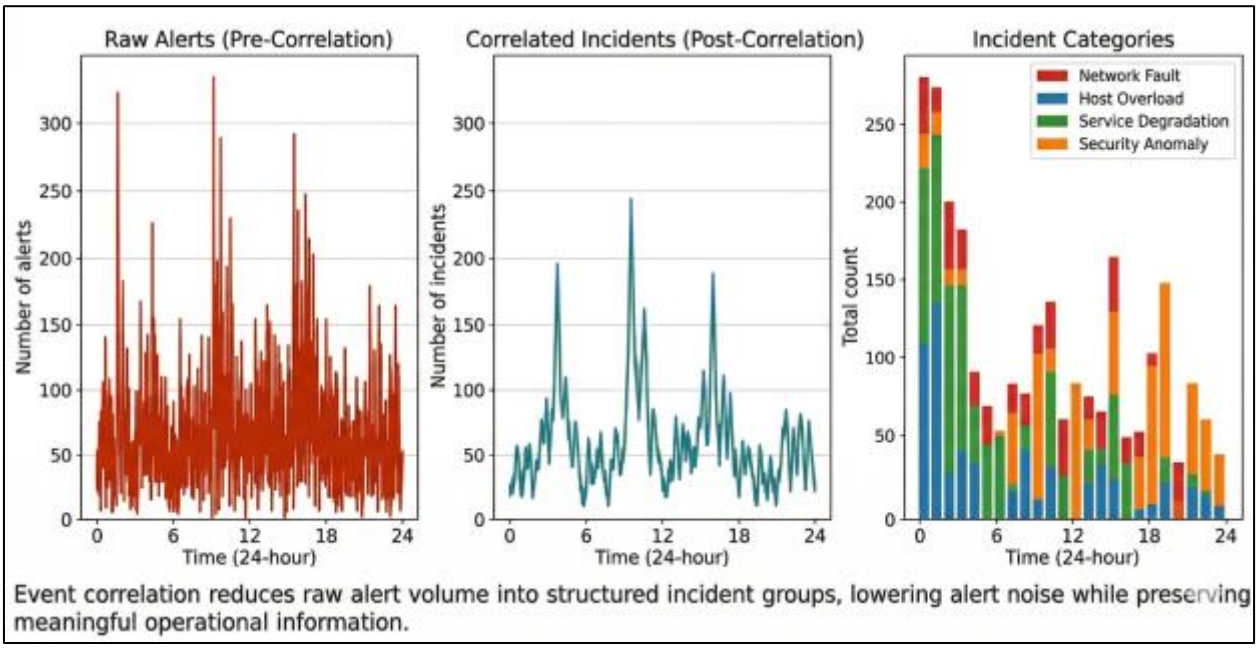


Figure 3 Alert volume reduction from raw events to correlated incidents**.**

The figure present a analytical visualization with three coordinated panels. The first panel shows raw alert counts across a 24-hour interval with multiple high spikes. The second panel shows correlated incident counts across the same interval with smaller peaks. The third panel shows incident categories such as network fault, host overload, service degradation, and security anomaly.

4.4. Root-Cause Identification and Multi-Layer Dependency Analysis

The root-cause analysis stage produced results closely connected to the correlation engine. Once alerts entered a shared incident group, the framework ranked candidate initiating faults according to event order, severity concentration, and dependency structure. In many cases, the top-ranked event matched the injected or observed initiating condition. Link failure cases, for example, produced downstream service alarms and route instability, yet the framework placed the physical or logical link event above later application symptoms. This result matters because enterprise environments often present the opposite pattern. Operators first notice the visible service effect rather than the originating infrastructure fault. In traditional monitoring systems, that sequence can slow diagnosis, increase escalation cycles, and lead to incorrect ticket assignment. The proposed method reduced that problem through dependency-aware ranking. The result was not perfect in every case. Incidents with simultaneous faults across different layers remained more difficult to classify. When a server-side bottleneck and a network-side degradation occurred close together, the model sometimes ranked one cause too early and treated the other as secondary. Even with that limitation, the framework produced a more ordered diagnostic path than isolated alert processing. It offered operators a clearer transition from symptom to source. This is useful in hybrid enterprise settings where network, compute, storage, and application teams often rely on different evidence sources. A monitoring framework that places root-cause candidates in dependency order can reduce fragmented interpretation and shorten the path to corrective action.

4.5. Dashboard Utility, Response Workflow, and Operational Interpretation

The dashboard and presentation layer produced a result that was primarily operational. Administrators used health score summaries, incident panels, topology-linked alerts, and trend views to form a quicker understanding of

infrastructure state. Instead of starting with raw logs or long alert lists, they could begin with service-level summaries and then move into device-level evidence. This top-down reading pattern matched the way incident response usually works in enterprise operations centers. Another important observation involved dashboard latency and update timing. The interface remained useful only when telemetry appeared quickly enough to preserve situational awareness. Slow refresh cycles reduced confidence in the displayed condition, especially during rapidly changing incidents. In the evaluation setting, the dashboard remained informative because the telemetry pipeline, alert engine, and presentation layer operated within an acceptable update interval. That outcome supports the methodological choice to keep preprocessing and scoring relatively simple and interpretable. Operators also responded positively to the incident view that combined affected assets, probable cause, severity, and event history within one record. This format supported ticket generation and prioritization with less manual interpretation. The main operational gain did not come from automation alone. It came from the combination of compact evidence, historical context, and dependency visibility. In enterprise settings, response teams often need a concise explanation of system state before taking action.

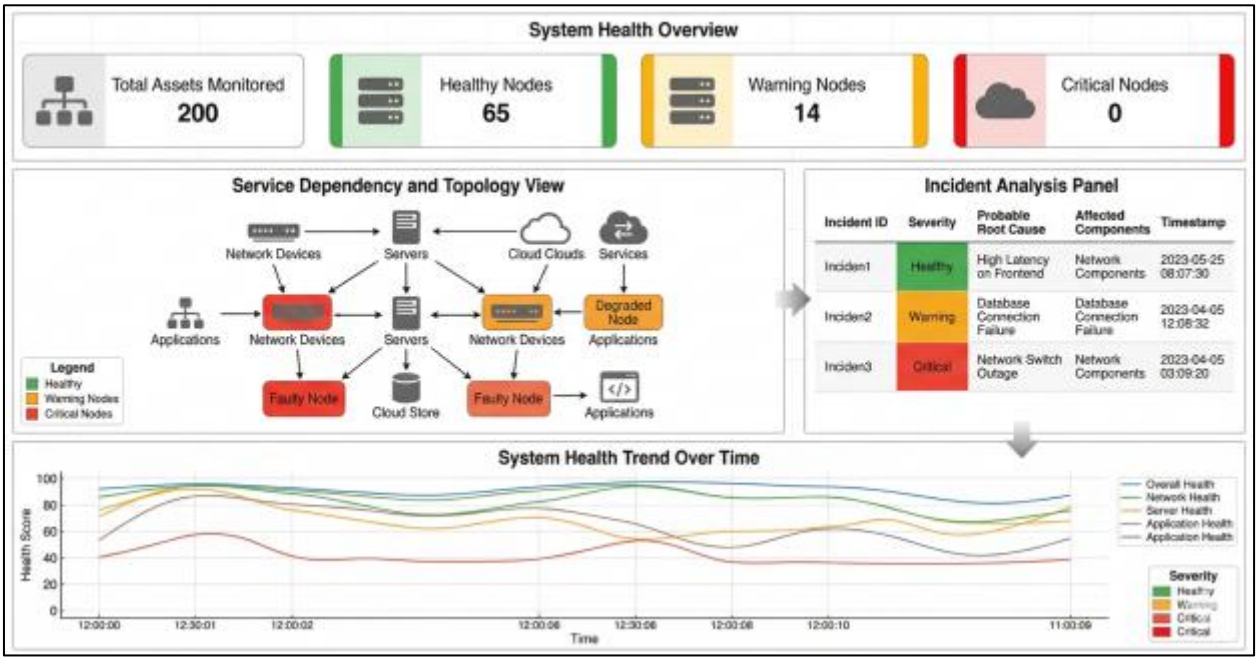


Figure 4 Enterprise operations dashboard for health scoring, incident view, and dependency tracing

The figure present interface layout with four coordinated regions: a top summary band showing asset health categories, a central topology or service map with affected nodes highlighted, a right-side incident panel showing severity and probable cause, and a bottom trend panel showing recent score movement.

4.6. Comparative Discussion, Limitations, and Research Implications

The overall discussion indicates that the proposed framework performs well when the monitoring problem is treated as an enterprise-wide observability task rather than a set of separate functions. The strongest outcomes appeared in integrated visibility, alert reduction, and more orderly root-cause interpretation. These results are consistent with the methodological choice to combine telemetry normalization, anomaly scoring, and event correlation within one architecture. When those stages operated together, the monitoring output became more useful than any single stage in isolation. The framework also revealed several limitations. Performance depends on telemetry quality, accurate timestamps, and reasonably complete dependency mapping. Weakness in any of those areas reduced the precision of anomaly interpretation and incident grouping. Another limitation appeared in multi-fault scenarios, where close timing and overlapping symptoms made ranking more difficult. The framework still provided structure in such cases, but diagnostic certainty declined. From a research perspective, the findings support future work in three directions. First, dependency mapping should become more adaptive so that service relationships can reflect changes in infrastructure. Second, anomaly models may benefit from workload-aware context for business-critical applications. Third, operator feedback can support refinement of clustering rules after repeated production use. These directions follow directly from the behavior observed in the current results.

Table 2 Summary of major findings from the proposed monitoring framework

Evaluation Area	Main Result	Operational Meaning
Unified Visibility	Network, host, cloud, and security telemetry entered one pipeline	Reduced separation between monitoring domains
Anomaly Detection	Combined threshold and deviation scoring performed better than threshold-only logic	Lower routine-state false alarms and clearer abnormal patterns
Alert Correlation	Raw alerts were compressed into smaller incident groups	Lower alert overload and improved incident readability
Root-Cause Ranking	Initiating faults were often placed above downstream symptoms	Faster movement from symptom review to diagnosis
Dashboard Utility	Operators interpreted incidents more quickly through grouped evidence and health summaries	Better support for prioritization and ticket creation
Limitation Areas	Incomplete dependency data and concurrent faults reduced precision	Further refinement is needed for more complex incident conditions

Taken together, the results show that the proposed framework is suitable for enterprise IT environments that require continuous visibility across devices, services, and infrastructure layers. Its value lies not only in event detection, but also in incident interpretation, reduction of alert noise, and clearer operational context. These outcomes make the framework relevant for both academic study and practical monitoring design.

5. Conclusion

This paper presented a network monitoring framework for enterprise IT infrastructure that combines telemetry collection, preprocessing, anomaly detection, event correlation, and operational visualization within one architecture. The results showed broader visibility across network, system, and application layers, along with lower alert noise and clearer incident grouping. The anomaly scoring method produced stable detection behavior under routine and fault conditions, while the correlation stage reduced redundant alerts and supported more direct identification of initiating faults. The framework also supported operational workflows through dashboard-based interpretation, which allowed administrators to move from service-level summaries to device-level evidence. Taken together, the findings indicate that a unified monitoring structure with multi-source telemetry and dependency-aware analysis can improve monitoring clarity and incident handling in enterprise environments.

Future work will extend the framework in several directions. Adaptive dependency mapping can reflect changes in infrastructure and service relationships over time. Anomaly models can include workload-specific context to improve interpretation in business-critical systems. Integration with automated response modules may reduce recovery time for recurring fault patterns. Operator feedback can also support revision of correlation rules and incident classification after repeated production use. These extensions would broaden the analytical scope of the framework and improve its value for complex enterprise IT environments.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Rahman, M. A., Bristy, I. J., Islam, M. I., & Tabassum, M. (2025, September). Federated learning for secure inter-agency data collaboration in critical infrastructure. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 421–430. https://doi.org/10.36348/sjet.2025.v10i09.005

[2] Bristy, I. J., Tabassum, M., Islam, M. I., & Hasan, M. N. (2025, September). IoT-driven predictive maintenance dashboards in industrial operations. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 457–466. https://doi.org/10.36348/sjet.2025.v10i09.009

[3] Abbasi, M., Shahraki, A., & Taherkordi, A. (2021). Deep learning for network traffic monitoring and analysis (NTMA): A survey. *Computer Communications, 170*, 19–41. https://doi.org/10.1016/j.comcom.2021.01.021

[4] Hasan, M. N., Karim, M. A., Joarder, M. M. I., & Zaman, M. T. (2025, September). IoT-integrated solar energy monitoring and bidirectional DC-DC converters for smart grids. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 467–475. https://doi.org/10.36348/sjet.2025.v10i09.010

[5] Razaq, A., Rahman, M., Karim, M. A., & Hossain, M. T. (2025, September 26). Smart charging infrastructure for EVs using IoT-based load balancing. *Zenodo.* https://doi.org/10.5281/zenodo.17210639

[6] uz Zaman, M. T. (2025). Smart energy metering with IoT and GSM integration for power loss minimization. *Preprints.* https://doi.org/10.20944/preprints202509.1770.v1

[7] Hasan, E. (2025). Secure and scalable data management for digital transformation in finance and IT systems. *Zenodo.* https://doi.org/10.5281/zenodo.17202282

[8] Fathima, A., & Devi, G. S. (2024). Enhancing university network management and security: A real-time monitoring, visualization & cyber attack detection approach using Paessler PRTG and Sophos Firewall. *International Journal of System Assurance Engineering and Management.* https://doi.org/10.1007/s13198-024-02448-y

[9] Joarder, M. M. I. (2025). Disaster recovery and high-availability frameworks for hybrid cloud environments. *Zenodo.* https://doi.org/10.5281/zenodo.17100446

[10] Joarder, M. M. I. (2025). Next-generation monitoring and automation: AI-enabled system administration for smart data centers. *TechRxiv.* https://doi.org/10.36227/techrxiv.175825633.33380552/v1

[11] Joarder, M. M. I. (2025). Energy-efficient data center virtualization: Leveraging AI and CloudOps for sustainable infrastructure. *Zenodo.* https://doi.org/10.5281/zenodo.17113371

[12] M. T. Y., Sharan, S. M. I., Azad, M. A., & Joarder, M. M. I. (2025). Smart maintenance and reliability engineering in manufacturing. *Saudi Journal of Engineering and Technology, 10*(4), 189–199.

[13] Enam, M. M. R., Joarder, M. M. I., Taimun, M. T. Y., & Sharan, S. M. I. (2025). Framework for smart SCADA systems: Integrating cloud computing, IIoT, and cybersecurity for enhanced industrial automation. *Saudi Journal of Engineering and Technology, 10*(4), 152–158.

[14] Farabi, S. A. (2025). AI-augmented OTDR fault localization framework for resilient rural fiber networks in the United States. *arXiv.* https://arxiv.org/abs/2506.03041

[15] Farabi, S. A. (2025). AI-driven predictive maintenance model for DWDM systems to enhance fiber network uptime in underserved U.S. regions. *Preprints.* https://doi.org/10.20944/preprints202506.1152.v1

[16] Shaikat, M. F. B. (2025). Pilot deployment of an AI-driven production intelligence platform in a textile assembly line. *TechRxiv.* https://doi.org/10.36227/techrxiv.175203708.81014137/v1

[17] Tonoy, A. A. R. (2025). Condition monitoring in power transformers using IoT: A model for predictive maintenance. *Preprints.* https://doi.org/10.20944/preprints202507.2379.v1

[18] Rayhan, F. (2025). A hybrid deep learning model for wind and solar power forecasting in smart grids. *Preprints.* https://doi.org/10.20944/preprints202508.0511.v1

[19] Rayhan, F. (2025). AI-powered condition monitoring for solar inverters using embedded edge devices. *Preprints.* https://doi.org/10.20944/preprints202508.0474.v1

[20] Rayhan, F. (2025). AI-enabled energy forecasting and fault detection in off-grid solar networks for rural electrification. *TechRxiv.* https://doi.org/10.36227/techrxiv.175623117.73185204/v1

[21] Hossain, M. T., Nabil, S. H., Razaq, A., & Rahman, M. (2025). Cybersecurity and privacy in IoT-based electric vehicle ecosystems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 921–933. https://doi.org/10.5281/zenodo.17246184

[22] Hossain, M. T., Nabil, S. H., Rahman, M., & Razaq, A. (2025). Data analytics for IoT-driven EV battery health monitoring. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(2), 903–913. https://doi.org/10.5281/zenodo.17246168

[23] Islam, R. (2025). AI and big data for predictive analytics in pharmaceutical quality assurance. *SSRN.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5564319

[24] Haque, S., Al Sany, S. M. A., & Rahman, M. (2025). Circular economy in fashion: MIS-driven digital product passports for apparel traceability. *International Journal of Scientific Research and Engineering Development, 8*(5), 1254–1262. https://doi.org/10.5281/zenodo.17276038

[25] Al Sany, S. M. A., Haque, S., & Rahman, M. (2025). Green apparel logistics: MIS-enabled carbon footprint reduction in fashion supply chains. *International Journal of Scientific Research and Engineering Development, 8*(5), 1263–1272. https://doi.org/10.5281/zenodo.17276049

[26] Hossain, M. T. (2025, October 7). Smart inventory and warehouse automation for fashion retail. *TechRxiv.* https://doi.org/10.36227/techrxiv.175987210.04689809.v1

[27] Karim, M. A. (2025, October 6). AI-driven predictive maintenance for solar inverter systems. *TechRxiv.* https://doi.org/10.36227/techrxiv.175977633.34528041.v1

[28] Akhter, T. (2025, October 6). Algorithmic internal controls for SMEs using MIS event logs. *TechRxiv.* https://doi.org/10.36227/techrxiv.175978941.15848264.v1

[29] Akhter, T. (2025, October 6). MIS-enabled workforce analytics for service quality & retention. *TechRxiv.* https://doi.org/10.36227/techrxiv.175978943.38544757.v1

[30] Saikat, M. H. (2025, October 6). AI-powered flood risk prediction and mapping for urban resilience. *TechRxiv.* https://doi.org/10.36227/techrxiv.175979253.37807272/v1

[31] Karim, M. A., Zaman, M. T. U., Nabil, S. H., & Joarder, M. M. I. (2025, October 6). AI-enabled smart energy meters with DC-DC converter integration for electric vehicle charging systems. *TechRxiv.* https://doi.org/10.36227/techrxiv.175978935.59813154/v1

[32] Al Sany, S. M. A., Rahman, M., & Haque, S. (2025). ERP–MIS integration for intelligent apparel production planning. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 145–156. https://doi.org/10.30574/wjaets.2025.17.1.1387

[33] Rahman, M., Haque, S., & Al Sany, S. M. A. (2025). Federated learning for privacy-preserving apparel supply chain analytics. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 259–270. https://doi.org/10.30574/wjaets.2025.17.1.1386

[34] Rahman, M., Razaq, A., Hossain, M. T., & Zaman, M. T. U. (2025). Machine learning approaches for predictive maintenance in IoT devices. *World Journal of Advanced Engineering Technology and Sciences, 17*(1), 157–170. https://doi.org/10.30574/wjaets.2025.17.1.1388

[35] Akhter, T., Alimozzaman, D. M., Hasan, E., & Islam, R. (2025, October). Explainable predictive analytics for healthcare decision support. *International Journal of Sciences and Innovation Engineering, 2*(10), 921–938. https://doi.org/10.70849/IJSCI02102025105

[36] Rahman, M. (2025, October 15). Integrating IoT and MIS for last-mile connectivity in residential broadband services. *TechRxiv.* https://doi.org/10.36227/techrxiv.176054689.95468219/v1

[37] Islam, R. (2025, October 15). Integration of IIoT and MIS for smart pharmaceutical manufacturing. *TechRxiv.* https://doi.org/10.36227/techrxiv.176049811.10002169

[38] Hasan, E. (2025). Big data-driven business process optimization: Enhancing decision-making through predictive analytics. *TechRxiv.* https://doi.org/10.36227/techrxiv.175987736.61988942/v1

[39] Rahman, M. (2025, October 15). IoT-enabled smart charging systems for electric vehicles. *TechRxiv.* https://doi.org/10.36227/techrxiv.176049766.60280824/v1

[40] Alam, M. S. (2025, October 21). AI-driven sustainable manufacturing for resource optimization. *TechRxiv.* https://doi.org/10.36227/techrxiv.176107759.92503137/v1

[41] Akter, E., Bormon, J. C., Saikat, M. H., & Shoag, M. (2025). AI-enabled structural and façade health monitoring for resilient cities. *International Journal of Science and Innovation Engineering, 2*(10), 1035–1051. https://doi.org/10.70849/IJSCI02102025116

[42] Haque, S., & Al Sany, S. M. A. (2025, October). Impact of consumer behavior analytics on telecom sales strategy. *International Journal of Science and Innovation Engineering, 2*(10), 998–1018. https://doi.org/10.70849/IJSCI02102025114

[43] Islam, K. S. A. (2025). Implementation of safety-integrated SCADA systems for process hazard control in power generation plants. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2321–2331. https://doi.org/10.5281/zenodo.17536369

[44] Afrin, S. (2025). Cloud-integrated network monitoring dashboards using IoT and edge analytics. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2298–2307. https://doi.org/10.5281/zenodo.17536343

[45] Afrin, S. (2025). Cyber-resilient infrastructure for public internet service providers using automated threat detection. *World Journal of Advanced Engineering Technology and Sciences, 17*(02), 127–140. https://doi.org/10.30574/wjaets.2025.17.2.1475

[46] Zaman, S. U. (2025). Vulnerability management and automated incident response in corporate networks. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(5), 2275–2286. https://doi.org/10.5281/zenodo.17536305

[47] Musarrat, R. (2025). AI-driven smart housekeeping and service allocation systems: Enhancing hotel operations through MIS integration. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 898–910. https://doi.org/10.5281/zenodo.17769627

[48] Alam, M. S. (2025). Real-time predictive analytics for factory bottleneck detection using edge-based IIoT sensors and machine learning. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 1053–1064. https://doi.org/10.5281/zenodo.17769890

[49] Zaidi, S. K. A. (2025). Smart sensor integration for energy-efficient avionics maintenance operations. *International Journal of Science and Innovation Engineering, 2*(11), 243–261. https://doi.org/10.70849/IJSCI02112025026

[50] Farooq, H. (2025). Cross-platform backup and disaster recovery automation in hybrid clouds. *International Journal of Science and Innovation Engineering, 2*(11), 220–242. https://doi.org/10.70849/IJSCI02112025025

[51] Farooq, H. (2025). Resource utilization analytics dashboard for cloud infrastructure management. *World Journal of Advanced Engineering Technology and Sciences, 17*(02), 141–154. https://doi.org/10.30574/wjaets.2025.17.2.1458

[52] Zaman, M. T. (2025). Enhancing grid resilience through DMR trunking communication systems. *World Journal of Advanced Engineering Technology and Sciences, 17*(03), 197–212. https://doi.org/10.30574/wjaets.2025.17.3.1551

[53] Nahar, S. (2025). Optimizing HR management in smart pharmaceutical manufacturing through IIoT and MIS integration. *World Journal of Advanced Engineering Technology and Sciences, 17*(03), 240–252. https://doi.org/10.30574/wjaets.2025.17.3.1554

[54] Hasan, E. (2025). Machine learning-based KPI forecasting for finance and operations teams. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 2139–2149. https://doi.org/10.5281/zenodo.17926746

[55] Hasan, E. (2025). SQL-driven data quality optimization in multi-source enterprise dashboards. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 2150–2160. https://doi.org/10.5281/zenodo.17926758

[56] Hasan, E. (2025). Optimizing SAP-centric financial workloads with AI-enhanced CloudOps in virtualized data centers. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 2252–2264. https://doi.org/10.5281/zenodo.17926855

[57] Zaman, S. U. (2025). Enhancing security in cloud-based IAM systems using real-time anomaly detection. *IJSRED - International Journal of Scientific Research and Engineering Development, 8*(6), 2292–2304. https://doi.org/10.5281/zenodo.17926883

[58] Rahman, M. (2025). Predictive maintenance of electric vehicle components using IoT sensors. *World Journal of Advanced Engineering Technology and Sciences, 17*(03), 312–327. https://doi.org/10.30574/wjaets.2025.17.3.1557

[59] Jasem, M. M. H. (2025, December 19). An AI-driven system health dashboard prototype for predictive maintenance and infrastructure resilience. *Authorea.* https://doi.org/10.22541/au.176617579.97570024/v1

[60] Uz Zaman, M. T. (2025). Photonics-based fault detection and monitoring in energy metering systems. *IJSRED – International Journal of Scientific Research and Engineering Development, 8*(6), 2359–2371. https://doi.org/10.5281/zenodo.18074355

[61] Fahim, M. A. I., Sharan, S. M. M. I., & Farooq, H. (2025). AI-enabled cloud-IoT platform for predictive infrastructure automation. *World Journal of Advanced Engineering Technology and Sciences, 17*(03), 431–446. https://doi.org/10.30574/wjaets.2025.17.3.1574

[62] Rahman, T. (2026). Financial risk intelligence: Real-time fraud detection and threat monitoring. *Zenodo.* https://doi.org/10.5281/zenodo.18176490

[63] Rabbi, M. S. (2026). AI-driven SCADA grid intelligence for predictive fault detection, cyber health monitoring, and grid reliability enhancement. *Zenodo.* https://doi.org/10.5281/zenodo.18196487

[64] Zaman, S. U., Afrin, S., Zaidi, S. K. A., & Islam, K. S. A. (2026). Resilient edge computing framework for autonomous, secure, and energy-aware systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(01), 105–121. https://doi.org/10.30574/wjaets.2026.18.1.1577

[65] Mim, M. A., Sharif, M. M., Rahman, F., & Nahar, S. (2026). Smart IoT infrastructure for workplace efficiency and energy savings. *World Journal of Advanced Engineering Technology and Sciences, 18*(01), 140–156. https://doi.org/10.30574/wjaets.2026.18.1.0026

[66] Taimun, M. T. Y., Alam, M. S., & Fareed, S. M. (2026). Digital twin-enabled predictive maintenance for textile and mechanical systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(01), 187–203. https://doi.org/10.30574/wjaets.2026.18.1.0001

[67] Alam, M. S., Fareed, S. M., Fazle, A. B., & Taimun, M. T. Y. (2026). Intelligent material flow optimization using IoT sensors and RFID tracking. *Global Journal of Engineering and Technology Advances, 26*(01), 109–125. https://doi.org/10.30574/gjeta.2026.26.1.0011

[68] Nahar, S., Rahman, F., & Mim, M. A. (2026). AI-integrated renewable energy and data analytics platform for corporate ESG compliance. *World Journal of Advanced Engineering Technology and Sciences, 18*(01), 219–235. https://doi.org/10.30574/wjaets.2026.18.1.0031

[69] Rahman, F., Nahar, S., & Mim, M. A. (2026). Cloud-native enterprise resource management for multi-sector operations. *Global Journal of Engineering and Technology Advances, 26*(01), 126–141. https://doi.org/10.30574/gjeta.2026.26.1.0012

[70] Sharan, S. M. M. I., Fahim, M. A. I., & Farooq, H. (2026). Cloud native fintech analytics platform for IoT enabled retail networks. *World Journal of Advanced Engineering Technology and Sciences, 18*(01), 089–104. https://doi.org/10.30574/wjaets.2026.18.1.1582

[71] Fahim, M. A. I., Farooq, H., & Sharan, S. M. M. I. (2026). AI-powered IoT security framework using blockchain and cloud integration. *Global Journal of Engineering and Technology Advances, 26*(01), 168–185. https://doi.org/10.30574/gjeta.2026.26.1.0003

[72] Islam, R. (2026). AI-integrated management information systems for manufacturing and supply chain risk mitigation. *Zenodo.* https://doi.org/10.5281/zenodo.18349501

[73] Zaidi, S. K. A., Islam, K. S. A., Zaman, S. U., & Afrin, S. (2026). Blockchain-secured communication for industrial IoT and aviation control systems. *IJSRED – International Journal of Scientific Research and Engineering Development, 9*(1), 234–250. https://doi.org/10.5281/zenodo.18278261

[74] Islam, K. S. A., Zaidi, S. K. A., Afrin, S., & Zaman, S. U. (2026). Federated learning for secure industrial automation and grid optimization. *Global Journal of Engineering and Technology Advances, 26*(01), 025–040. https://doi.org/10.30574/gjeta.2026.26.1.0360

[75] Afrin, S., Zaman, S. U., Islam, K. S. A., & Zaidi, S. K. A. (2026). Distributed edge intelligence for energy and transportation systems. *World Journal of Advanced Engineering Technology and Sciences, 18*(1), 280–297. https://doi.org/10.30574/wjaets.2026.18.1.0049

[76] Emon, M. M. H. (2026). An intelligent energy management system for cost optimization and peak demand reduction using battery-integrated smart dispatch. *Zenodo.* https://doi.org/10.5281/zenodo.18444728

[77] Dukkipati, S. S. N. C. (2026, February 9). Design and implementation of scalable AI-driven conversational systems for enterprise-level feedback intelligence and decision support. *SSRN.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6263818

[78] Karim, M. A., uz Zaman, M. T., & Razaq, A. (2026). Integrated renewable energy monitoring and adaptive load optimization using smart grid and intelligent control algorithms. *Zenodo.* https://doi.org/10.5281/zenodo.18748205

[79] Nahar, S., Rahman, M., Alam, M. S., & Al Sany, S. M. A. (2026). Intelligent data governance and ethical AI framework for enterprise information systems. *Zenodo.* https://doi.org/10.5281/zenodo.18839122

[80] Mirza, S. B. (2026). Predictive reliability engineering for cloud scale business intelligence platforms through anomaly detection capacity optimization and proactive support automation. *Zenodo.* https://doi.org/10.5281/zenodo.19474845

[81] Islam, M. A. (2026). Native scalable student information systems and admission test automation with peak load architecture database performance optimization and observability driven reliability. *Zenodo.* https://doi.org/10.5281/zenodo.18987480

[82] Mim, M. A. (2026). Cybersecurity risk mitigation in educational and healthcare IT environments. *Zenodo.* https://doi.org/10.5281/zenodo.18988585

[83] Alam, M. J. (2026). Information systems for legal documentation management and policy analysis in institutional governance. *Figshare.* https://doi.org/10.6084/m9.figshare.31717873

[84] Alam, M. J. (2026). Digital contract lifecycle management systems for corporate governance and regulatory oversight. *Zenodo.* https://doi.org/10.5281/zenodo.19007705

[85] Alam, M. J. (n.d.). Policy monitoring platforms for institutional governance and organizational accountability. *Social Science Research Network.* https://doi.org/10.2139/ssrn.6416238

[86] Alam, M. J. (2026). Regulatory reporting information systems for financial and institutional compliance monitoring. *Preprints.org.* https://doi.org/10.20944/preprints202603.1198.v1

[87] Dukkipati, S. S. N. C. (2026). Cloud-native big data streaming framework for real-time social media intelligence and large-scale public opinion analytics. *Zenodo.* https://doi.org/10.5281/zenodo.19274669

[88] Islam, M. A. (2026). Optimizing project management frameworks to reduce cost overruns in U.S. public infrastructure projects. *Zenodo.* https://doi.org/10.5281/zenodo.19311456

[89] Akter, T. (2026). AI-driven workforce productivity optimization in U.S. service organizations using KPI-based predictive analytics. *Zenodo.* https://doi.org/10.5281/zenodo.19311795

[90] Bhuiyan, M. I. H. (2026). AI-driven customer complaint analytics for systemic risk reduction and consumer protection in the U.S. banking sector. *Zenodo.* https://doi.org/10.5281/zenodo.19344701

[91] Islam, R. (2026). Data-driven sales performance evaluation using business analytics. *Zenodo.* https://doi.org/10.5281/zenodo.19371191

[92] Hossain, M. I. (2026). Enabled digitalization of container vessel navigation and U.S. port operations using real-time AIS and operational data for shipping and supply chain optimization. *Zenodo.* https://doi.org/10.5281/zenodo.19441203

[93] Rashid, M. F. (2026). Management information systems enabled ethical and sustainable apparel sourcing: Supplier compliance and traceability scorecard dashboard. *Zenodo.* https://doi.org/10.5281/zenodo.19441584

[94] Shaik, M. H. (2026). Secure and compliant DevSecOps architecture for automated CI/CD pipelines in regulated cloud environments. *Zenodo.* https://doi.org/10.5281/zenodo.19442346

[95] Uddin, M. N. (2026). AI-driven demand forecasting & inventory optimization for multi-region dealer and retail distribution network. *Zenodo.* https://doi.org/10.5281/zenodo.19473456

[96] Rahman, M. A., Islam, M. I., Tabassum, M., & Bristy, I. J. (2025, September). Climate-aware decision intelligence: Integrating environmental risk into infrastructure and supply chain planning. *Saudi Journal of Engineering and Technology (SJEAT), 10*(9), 431–439. https://doi.org/10.36348/sjet.2025.v10i09.006