iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VIII **Month of publication:** August 2026

DOI: https://doi.org/10.22214/ijraset.2026.84772

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

AI-Driven Root Cause Analysis for Fixed Telecommunications Networks

Mohammad Mustafa[1], Mohammed Hussain Moheet[2], Mohammed Abdul Moheet[3]
[1]*Communications Engineer, Contact Center Company (ccc), Riyadh, Saudi Arabia*
[2]*Computer Science Engineer, Methodist College of Engineering and Technology (MCET), Hyderabad, India*
[3]*Data Center Services Team Leader, Jeraisy Electronic Services, Riyadh, Saudi Arabia*

Abstract: ***Root Cause Analysis (RCA) is a critical component of service assurance in fixed telecommunications networks, where service degradation may originate from multiple interconnected domains, including fixed access infrastructure, Optical Line Terminals (OLTs), Optical Network Terminals (ONTs), IP transport, uplinks, network capacity, Customer Premises Equipment (CPE), and home Wi-Fi environments. Traditional RCA approaches depend largely on predefined thresholds, alarm rules, individual monitoring systems, and manual correlation by network engineers. Although these methods remain effective for known and clearly defined faults, they become less efficient when network problems involve large volumes of operational data, intermittent degradation, multiple simultaneous symptoms, or dependencies across different network domains. This paper examines the application of Artificial Intelligence (AI) to enhance RCA in fixed telecommunications networks. It proposes a practical AI-driven RCA framework that combines network and service data, KPI and alarm monitoring, anomaly detection, multi-source data correlation, AI-based analysis, probable root-cause identification, corrective-action recommendations, and post-action performance validation. The proposed approach aims to transform RCA from a predominantly reactive and manually intensive process into a more intelligent and proactive service-assurance capability. Rather than replacing network engineers, AI-driven RCA is positioned as a decision-support mechanism that accelerates investigation, improves correlation across heterogeneous data sources, and enables more consistent identification of probable causes. The paper concludes that AI-driven RCA represents an important step toward increasingly intelligent and automated fixed telecommunications network operations.***

Keywords: Artificial Intelligence, Root Cause Analysis, Fixed Telecommunications Networks, FTTH, Service Assurance, Network Performance, Anomaly Detection, Fault Management, Customer Experience.

I. INTRODUCTION

Fixed telecommunications networks have evolved into complex service environments combining fiber access infrastructure, Optical Line Terminals (OLTs), Optical Network Terminals (ONTs), IP transport networks, aggregation and uplink resources, Customer Premises Equipment (CPE), and home Wi-Fi environments. Maintaining consistent service quality across these interconnected domains requires continuous monitoring of network performance, faults, alarms, capacity, availability, and customer-experience indicators. As network complexity increases, identifying the actual cause of service degradation becomes increasingly challenging because a customer-visible problem may originate from several different network layers.

Root Cause Analysis (RCA) is therefore an essential component of fixed-network service assurance. Conventional RCA generally relies on KPI thresholds, alarm monitoring, predefined correlation rules, troubleshooting procedures, and the experience of network engineers. These approaches remain valuable for known and deterministic problems; however, they can become inefficient when operational data is distributed across multiple systems or when several network events occur simultaneously. In such situations, engineers may need to manually correlate alarms, performance trends, topology, utilization, fault records, and customer-experience information before determining the most probable cause.

Artificial Intelligence (AI) provides an opportunity to enhance this process by identifying abnormal network behavior, recognizing patterns in operational data, correlating information from multiple sources, and ranking probable causes. The ITU-T framework for AI-enhanced telecommunication operation and management recognizes capabilities such as anomaly detection and fault prediction as part of AI-supported quality assurance [1]. Similarly, current industry frameworks increasingly position AI and analytics as important enablers of network observability and service assurance [2].

This paper examines the application of AI-driven RCA specifically within fixed telecommunications networks. It proposes a practical framework integrating network and service data, KPI and alarm monitoring, anomaly detection, multi-source correlation, AI-driven analysis, probable root-cause identification, corrective-action recommendations, and subsequent performance validation.

The objective is not to replace engineering expertise, but to demonstrate how AI can improve decision support, reduce manual correlation effort, and enable faster and more proactive fixed-network service assurance.

II. ROOT CAUSE ANALYSIS IN FIXED TELECOMMUNICATIONS NETWORKS

Root Cause Analysis (RCA) is the systematic process of identifying the underlying condition responsible for a network fault, performance degradation, or service-quality problem. In telecommunications management, fault localization involves examining available operational information to determine the origin of a detected problem [3]. In fixed telecommunications networks, this process is particularly important because an observed service issue may be the result of problems occurring at different points across the end-to-end service path. A typical fixed broadband service involves several interconnected components, including the Optical Line Terminal (OLT), optical distribution and fiber infrastructure, Optical Network Terminal (ONT), aggregation and IP transport networks, uplinks, Customer Premises Equipment (CPE), and the customer's home Wi-Fi environment. Consequently, a symptom such as low download speed does not by itself identify the actual root cause. Similar degradation may result from access-network congestion, uplink saturation, optical impairment, incorrect service configuration, transport-network degradation, CPE limitations, or poor Wi-Fi conditions. Effective RCA therefore requires correlation of multiple categories of operational information. These may include network alarms and fault events, availability indicators, traffic and utilization measurements, throughput and latency KPIs, interface statistics, topology and configuration information, historical incidents, CPE measurements, and customer-experience indicators. The purpose of correlation is to distinguish the primary cause from secondary symptoms and unrelated events occurring during the same period. For example, an increase in customer throughput degradation accompanied by high OLT uplink utilization may indicate a shared capacity constraint. In contrast, poor throughput affecting only a limited number of customers while network-side KPIs remain normal may indicate CPE or home Wi-Fi limitations. Similarly, multiple alarms generated across dependent network elements may originate from a single upstream failure rather than independent faults.

RCA in fixed telecommunications networks should therefore be considered an end-to-end analytical process rather than simple alarm identification. Previous work on AI-driven fixed-network performance and service assurance has similarly emphasized the importance of combining network performance, operational, and customer-experience information to improve network analysis [4], [5]. The effectiveness of RCA ultimately depends on identifying meaningful relationships among these heterogeneous data sources and converting them into an evidence-based explanation of the probable cause.

III.LIMITATIONS OF TRADITIONAL RCA

Traditional Root Cause Analysis in telecommunications networks relies primarily on alarm monitoring, predefined KPI thresholds, static correlation rules, troubleshooting procedures, and the experience of network engineers. These approaches remain effective for well-understood and deterministic faults, particularly when a clear relationship exists between an alarm and the affected network element. However, their effectiveness decreases when service degradation involves multiple network domains, large volumes of operational data, or complex dependencies between network elements.

One major limitation is the dependence on manual correlation. Fixed-network performance information is often distributed across different monitoring and operational systems. An engineer investigating a service degradation may need to examine alarms, KPI trends, utilization, topology, configuration, fault history, and customer-experience information separately before establishing a probable cause. This increases investigation effort and can result in inconsistent conclusions depending on the available information and individual engineering experience.

Another limitation is the reliance on static thresholds and predefined rules. Threshold-based monitoring is effective when abnormal behavior is already known, but it may not identify gradual degradation or unusual patterns that remain within configured limits. Similarly, predefined alarm-correlation rules may become difficult to maintain as network topology, configurations, services, and dependencies change. Communication networks can also generate large numbers of correlated or redundant alarms following a common failure, making it difficult to distinguish the originating event from secondary symptoms [6], [7].

Traditional RCA is also predominantly reactive. Analysis generally begins after an alarm, KPI violation, service degradation, or customer complaint has already occurred. This limits the ability of service-assurance teams to identify developing problems before significant customer impact is observed.

These limitations do not make conventional RCA obsolete. Rules, thresholds, and engineering expertise remain important for known network conditions. However, the increasing volume and diversity of fixed-network operational data create a need for complementary analytical capabilities that can automatically identify anomalies, correlate events across multiple data sources, recognize recurring patterns, and prioritize probable causes. This provides the operational basis for introducing AI-driven RCA.

TABLE I
COMPARISON OF TRADITIONAL AND AI-DRIVEN RCA

Aspect	Traditional RCA	AI-Driven RCA
Data analysis	Often performed across individual tools and data sources	Integrates and analyzes multiple operational data sources
Problem detec-tion	Primarily alarms and predefined KPI thresholds	Thresholds combined with anomaly and pattern detection
Correlation	Manual or predefined rules	Automated multi-source and temporal correlation
Historical learning	Depends largely on engineer knowledge and documented rules	Can learn recurring relationships from historical incidents and data
Complex alarm handling	May require manual filtering and investigation	Can group correlated events and prioritize probable root causes
Scalability	Investigation effort increases with network and data complexity	Designed to process larger volumes of heterogeneous data
Root-cause identification	Engineer-driven diagnosis	AI-generated probable causes supported by engineering validation
Operational approach	Predominantly reactive	Supports reactive and increasingly proactive analysis
Engineer role	Performs most data collection, correlation, and diagnosis	Validates AI findings and focuses on decisions and corrective actions
Data analysis	Often performed across individual tools and data sources	Integrates and analyzes multiple operational data sources

IV. ROLE OF AI IN ROOT CAUSE ANALYSIS

Artificial Intelligence can enhance Root Cause Analysis by transforming large volumes of network and service data into actionable information. Rather than relying exclusively on predefined thresholds and static correlation rules, AI-driven RCA can analyze historical and real-time data to detect abnormal behavior, identify relationships among network events, recognize recurring patterns, and determine the most probable causes of service degradation. ITU-T M.3390 specifically identifies AI-supported anomaly detection, multi-indicator correlation, alarm relationship analysis, and root-cause analysis as capabilities applicable to telecommunications service-quality assurance [8].

Anomaly detection represents an important first step in AI-driven RCA. Traditional monitoring typically generates an alert when a KPI crosses a configured threshold. AI-based analysis can additionally establish normal behavioral patterns from historical network data and identify deviations that may indicate emerging degradation. For example, an uplink may remain below its configured congestion threshold but exhibit an unusual increase in utilization, packet loss, or latency compared with its normal operating pattern.

The second major capability is multi-source data correlation. Fixed-network problems may generate related symptoms across OLTs, ONTs, interfaces, transport links, CPEs, and customer-experience monitoring systems. AI can correlate these observations using factors such as time, topology, service dependency, location, and historical relationships. This helps separate independent events from symptoms originating from a common network condition.

AI can also support pattern recognition and probable-cause identification. Historical incidents and their confirmed resolutions can provide useful evidence for recognizing similar conditions. If a particular combination of increasing uplink utilization, throughput degradation, latency deterioration, and affected customers has previously been associated with capacity congestion, an AI-driven RCA system can identify the similarity and rank congestion as a probable cause. Importantly, the result should be treated as a probability-based recommendation rather than an unquestionable diagnosis.

Another important capability is decision support. Once probable causes have been identified, the system can associate them with relevant corrective actions, previous resolutions, or engineering procedures. Network engineers can then validate the available evidence and determine the appropriate intervention. This human-in-the-loop approach is particularly important where configuration changes or corrective actions may affect live customer services.

AI-driven RCA should therefore be viewed as an enhancement to engineering expertise rather than its replacement. Previous research on AI-supported fixed-network operations has similarly positioned intelligent analytics and service assurance as progressive steps toward more autonomous network management [9]. By automating data correlation and assisting probable-cause identification, AI enables engineers to focus more effectively on validation, decision-making, and preventive improvement.

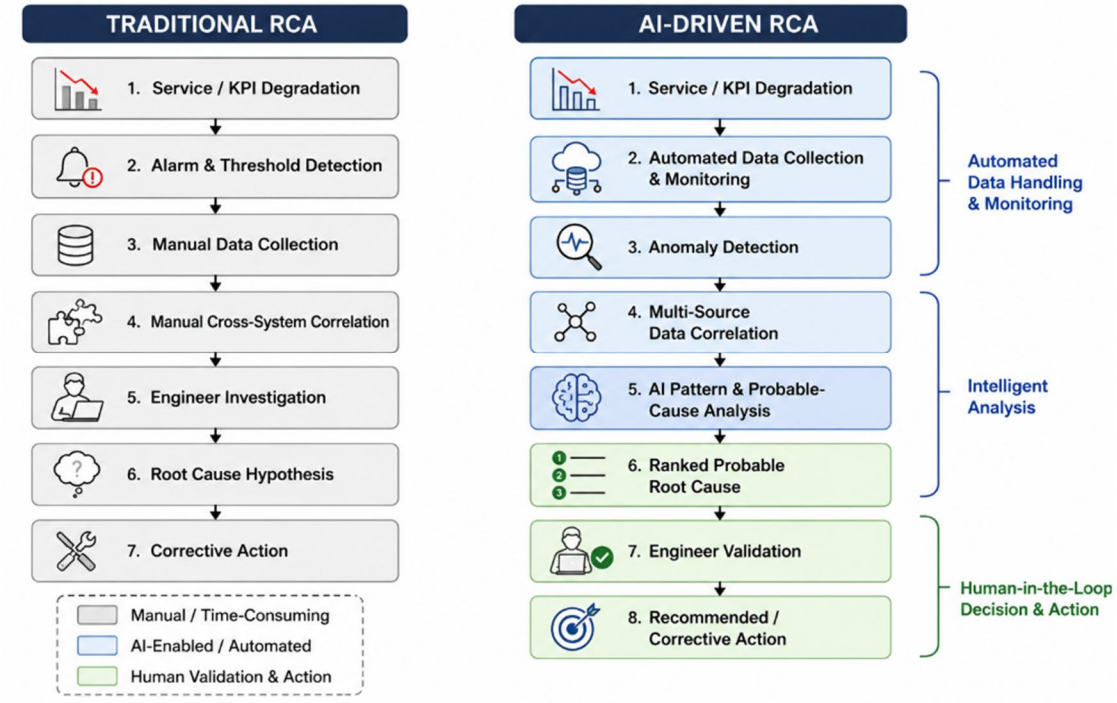


Fig. 1 Traditional vs. AI-Driven RCA Process

V. PROPOSED AI-DRIVEN RCA FRAMEWORK

This paper proposes a practical AI-driven Root Cause Analysis framework for fixed telecommunications networks. The framework is designed to transform heterogeneous network and service information into an evidence-based identification of probable root causes and appropriate corrective actions. It consists of eight sequential stages: Network and Service Data, KPI/Alarm Monitoring, Anomaly Detection, Multi-Source Data Correlation, AI-Driven Analysis, Probable Root Cause Identification, Recommended Corrective Action, and Performance Validation. The framework is aligned with the broader concept of AI-enhanced telecommunications service assurance, where operational data, anomaly detection, correlation, RCA, and assurance strategies are progressively integrated [8].

A. Network and Service Data

The first stage establishes a unified data foundation. Relevant information may originate from OLTs, ONTs, access infrastructure, IP transport interfaces, uplinks, CPEs, home Wi-Fi systems, fault-management platforms, and customer-experience monitoring systems. The collected information can include throughput, latency, packet loss, utilization, availability, optical indicators, alarms, traffic statistics, topology, configuration, historical incidents, and customer-experience KPIs. Combining these sources provides the end-to-end visibility required to determine whether degradation originates from the access network, transport layer, capacity constraint, customer equipment, or another service component.

B. KPI and Alarm Monitoring

The second stage continuously monitors performance KPIs, faults, and alarms. Conventional thresholds remain useful for detecting known conditions such as interface unavailability or excessive utilization. However, the monitoring layer should also preserve historical behavior and contextual information. This allows subsequent analytical stages to evaluate not only whether a threshold has been exceeded but also whether current network behavior differs significantly from expected operating

C. Anomaly Detection

Anomaly detection identifies unusual changes in network or service behavior. AI and machine-learning techniques can complement static thresholds by learning normal patterns from historical data and identifying deviations [8]. For example, an uplink operating at 70% utilization may not exceed a conventional congestion threshold, but a rapid increase from its normal 30–40% range accompanied by increasing latency and declining throughput may indicate developing degradation. This stage therefore enables earlier identification of conditions that might otherwise remain undetected until customer impact becomes significant.

D. Multi-Source Data Correlation

Detected anomalies must then be correlated across different data sources. Correlation can consider time, network topology, shared resources, service relationships, location, affected customers, and historical events. For example, simultaneous throughput degradation across multiple ONTs connected to the same OLT, combined with increasing uplink utilization, provides stronger evidence of a shared network constraint than an isolated customer measurement. This stage is critical because individual alarms or KPIs frequently represent symptoms rather than the underlying cause.

E. AI-Driven Analysis

The correlated information is analyzed to identify meaningful patterns and relationships. Depending on data availability and operational maturity, the analytical capability may combine classification, clustering, pattern recognition, historical incident matching, knowledge-based reasoning, and other machine-learning techniques. AI-supported telecommunications analysis can use historical information and topology relationships to improve fault and service-quality analysis [8]. The objective is not necessarily to apply highly complex algorithms, but to determine which combination of observed conditions best explains the detected degradation.

F. Probable Root Cause Identification

Instead of producing only another alarm, the system should generate one or more ranked probable root causes together with supporting evidence. For example, a low-throughput condition could be classified as most likely associated with uplink congestion, while alternative causes such as access degradation or CPE limitations receive lower confidence. Providing ranked causes is important because operational network conditions may be ambiguous, and a single symptom can have multiple possible explanations.

G. Recommended Corrective Action

Once a probable cause has been identified, the framework associates the diagnosis with an appropriate corrective action or engineering recommendation. Depending on the problem, this may include capacity augmentation, traffic redistribution, interface investigation, configuration correction, optical-path inspection, CPE troubleshooting, or Wi-Fi optimization. Initially, these recommendations should support engineers rather than automatically execute high-impact network changes. As confidence and operational maturity increase, selected low-risk actions may progressively become automated [9].

H. Performance Validation

The final stage verifies whether the corrective action has resolved the original degradation. Relevant KPIs, alarms, customer-experience indicators, and affected network elements are monitored after intervention and compared with their pre-action condition. Successful outcomes can be retained as historical RCA knowledge, while unsuccessful outcomes trigger further analysis. This creates a feedback mechanism through which confirmed incidents, causes, and corrective actions can progressively improve future RCA decisions.

Overall, the proposed framework converts RCA from a sequence of largely manual troubleshooting activities into a structured intelligence cycle. AI is applied primarily where conventional operations face the greatest difficulty: detecting non-obvious abnormalities, correlating heterogeneous information, identifying patterns, and prioritizing probable causes. Engineering expertise remains essential for validating complex diagnoses and determining appropriate corrective actions.

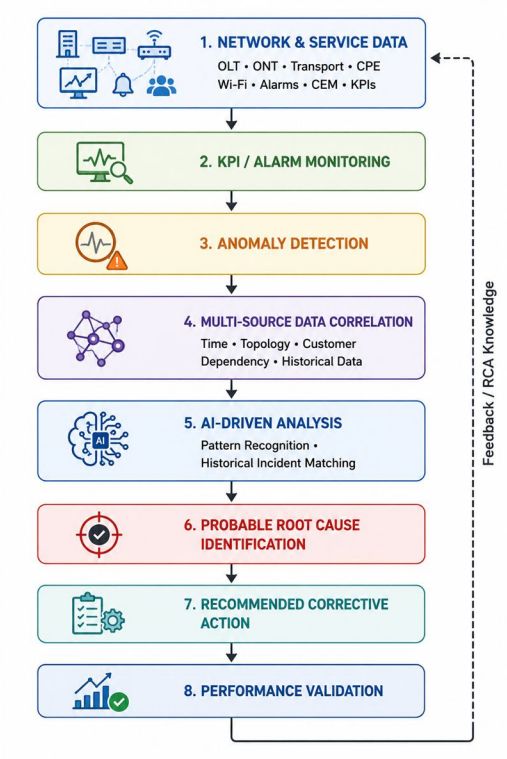


Fig. 2. Proposed AI-driven root cause analysis framework for fixed telecommunications networks.

VI. KEY FIXED NETWORK RCA USE CASES

The value of AI-driven RCA becomes more apparent when applied to practical fixed-network service-assurance scenarios. Fixed broadband degradation can originate from the access, transport, capacity, CPE, or home-network domain, while the customer may experience similar symptoms regardless of the actual source. Multi-source correlation is therefore essential for distinguishing between these conditions.

A. FTTH Access and OLT/ONT Degradation

In an FTTH network, service degradation may be associated with the OLT, ONT, optical path, access capacity, configuration, or a shared network resource. An AI-driven RCA system can correlate OLT and ONT performance, optical indicators, alarms, availability, throughput, topology, and affected-customer information. If several ONTs connected through a common access element exhibit degradation during the same period, the system can prioritize a shared access-network condition over isolated customer-side faults.

B. Uplink and IP Transport Congestion

Low customer throughput may occur even when the FTTH access layer is functioning normally. The underlying cause may instead be congestion or degradation in an OLT uplink, aggregation interface, or IP transport path. By correlating interface utilization, traffic trends, latency, packet loss, throughput, and the number of affected customers, AI-driven RCA can identify whether service deterioration is associated with a shared transport bottleneck. Temporal analysis is particularly useful for recognizing recurring peak-hour congestion patterns.

C. Network Capacity Degradation

Capacity-related problems often develop gradually and may initially remain below static congestion thresholds. Anomaly detection can identify unusual growth in utilization or changes in the relationship between traffic and service performance. When rising utilization repeatedly coincides with throughput reduction or latency deterioration, the RCA system can increase the probability of a capacity constraint and recommend further capacity assessment or augmentation.

D. Intermittent Network Faults

Intermittent faults can be difficult to diagnose because network elements may return to normal operation before an engineer begins investigation. AI-driven RCA can correlate historical alarms, interface availability, traffic interruptions, error indicators, and recurring temporal patterns to identify repeated degradation associated with a particular link or network element. Historical pattern recognition is therefore valuable for problems that cannot be reproduced during manual troubleshooting.

E. CPE and Home Wi-Fi Performance

Not every fixed broadband performance problem originates within the operator network. Customer throughput and experience may also be affected by CPE capability, Wi-Fi technology, signal conditions, channel interference, frequency band, connected-device load, or the customer's indoor environment. Previous research has highlighted the importance of combining network-side and customer-side information when analyzing fixed-broadband customer experience [5]. If access and transport KPIs remain healthy while degradation is concentrated among particular CPE or Wi-Fi conditions, the AI-driven RCA system can prioritize the customer environment as the probable source rather than incorrectly initiating network-side remediation.

F. Customer Experience and Service Degradation

Customer-experience indicators can provide an additional service-level view of network performance. When deterioration is detected, AI-driven RCA can correlate affected customers with their OLT, access resources, uplinks, CPE characteristics, alarms, and performance KPIs. A geographically or topologically concentrated group of affected customers may indicate a shared network issue, whereas isolated degradation across otherwise healthy network resources may point toward individual customer environments. This correlation enables RCA to move beyond individual network alarms toward an end-to-end service perspective.

These use cases demonstrate that the primary strength of AI-driven RCA is not simply detecting more alarms, but establishing relationships among multiple symptoms and determining the most plausible explanation. Research on communication-network alarm analysis has similarly demonstrated the value of historical relationships and association-based approaches for reducing redundant alarms and supporting root-cause inference [6], [7].

TABLE II
EXAMPLE FIXED TELECOMMUNICATIONS RCA USE CASES

Use Case / Observed Symptom	Data Correlated	Example Probable Root Cause	Potential Action
Multiple FTTH customers show low throughput	OLT/ONT KPIs, topology, optical indicators, alarms, utilization	Shared access or OLT-related degradation	Investigate affected access element and capacity
Peak-hour throughput degradation	Uplink utilization, traffic, latency, packet loss, throughput	Uplink or transport congestion	Capacity assessment or traffic optimization
Gradual performance deterioration	Historical utilization, throughput, latency, traffic growth	Developing capacity constraint	Capacity augmentation planning
Repeated short service interruptions	Availability, alarms, interface errors, traffic history	Intermittent link/interface instability	Link/interface investigation
Individual customer has low Wi-Fi speed	CPE, Wi-Fi band/technology, signal indicators, network-side KPIs	CPE or home Wi-Fi limitation	CPE/Wi-Fi optimization
Multiple alarms occur simultaneously	Alarm timestamps, topology, dependency relationships	Common upstream fault	Prioritize originating network element
Customer-experience KPI degradation	CEM indicators, OLT/ONT, transport, utilization, alarms, CPE	Access, transport, capacity, or customer-environment issue	Action based on highest-ranked probable cause

The examples illustrate probable RCA relationships; the actual diagnosis depends on network topology, available data, and operational context.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VIII Aug 2026- Available at www.ijraset.com

VII. BENEFITS AND OPERATIONAL IMPACT

The primary operational benefit of AI-driven RCA is the ability to accelerate the transformation of network data into actionable diagnostic information. Traditional investigations may require engineers to manually navigate multiple monitoring systems and correlate alarms, KPIs, topology, utilization, historical faults, and customer-experience information. By automating part of this correlation process, AI-driven RCA can reduce the time and effort required to identify the most probable source of degradation.

A second benefit is improved consistency of analysis. Manual RCA can depend significantly on individual experience and familiarity with particular network domains. An AI-driven system can apply common analytical logic across incidents while using historical patterns and previously validated cases as additional evidence. This does not eliminate the need for engineering expertise; rather, it provides engineers with a more consistent starting point for investigation and decision-making.

AI-driven RCA can also support a transition from reactive toward proactive service assurance. Anomaly detection may identify unusual behavior before a conventional alarm threshold is crossed or significant customer impact becomes visible. When such anomalies are correlated with capacity, traffic, topology, and historical performance, service-assurance teams can investigate developing conditions such as congestion, intermittent instability, or gradual performance deterioration at an earlier stage. AI-enhanced telecommunications management frameworks similarly recognize anomaly detection, fault analysis, and intelligent service-quality assurance as important capabilities for improving network operations [1], [8].

Another operational advantage is improved prioritization of engineering effort. Instead of presenting engineers with large numbers of individual alarms or KPI deviations, an AI-driven RCA system can group related symptoms, identify affected services or customers, and rank probable causes according to available evidence. Engineers can therefore focus on validating high-probability causes and implementing appropriate corrective measures.

At the service level, faster and more accurate identification of degradation can support improved customer experience by reducing unnecessary troubleshooting and directing corrective actions toward the appropriate network or customer domain. Previous work on AI-driven fixed-network performance and customer-experience optimization has similarly emphasized the value of combining network analytics with service and customer indicators [4], [5].

Overall, the operational value of AI-driven RCA lies not in replacing existing assurance processes, but in making them more efficient, evidence-based, consistent, and increasingly proactive.

VIII. CHALLENGES AND LIMITATIONS

Despite its potential benefits, implementing AI-driven RCA in fixed telecommunications networks presents several technical and operational challenges. The effectiveness of an AI-based RCA system depends not only on the analytical model but also on the quality, completeness, consistency, and availability of the underlying network data.

A primary challenge is data quality and integration. RCA requires information from multiple sources, including performance-management systems, fault-management platforms, network inventory, topology, OLT/ONT management systems, IP transport monitoring, CPE platforms, and customer-experience systems. These sources may use different identifiers, timestamps, measurement intervals, data models, and aggregation methods. Missing measurements, incorrect topology relationships, inconsistent naming, or time synchronization problems can result in inaccurate correlations and consequently misleading probable-cause recommendations. Effective data governance is therefore a prerequisite for reliable AI-driven RCA.

A second challenge concerns the availability of historical and validated RCA information. Supervised AI approaches may require previous incidents with accurately identified causes and resolutions. However, operational incident records may contain incomplete descriptions or inconsistent root-cause classifications. Historical data may therefore require significant preparation before it can be used reliably for model development or validation. Explainability and confidence are also important. Network engineers need to understand why a particular cause has been prioritized. An RCA system that provides only a predicted root cause without supporting evidence may be difficult to trust in operational environments. The system should therefore provide relevant indicators, correlated alarms, affected resources, historical similarities, and confidence information alongside its recommendation. AI-enhanced telecommunications management consequently requires appropriate governance and operational controls [1], [8].

Another limitation is changing network behavior. Traffic patterns, topology, software versions, configurations, customer usage, and capacity can change over time. Models trained on historical conditions may become less accurate as the network evolves, creating a requirement for continuous monitoring, validation, and periodic model updates.

False positives and incorrect correlations must also be considered. Events occurring at similar times are not necessarily causally related, and an abnormal KPI does not always indicate a network fault. For this reason, AI-generated outputs should generally be treated as probable causes rather than absolute conclusions.

Finally, integration with existing OSS, service-assurance processes, and operational workflows can require significant effort. Human oversight remains particularly important for complex incidents and high-impact corrective actions. AI-driven RCA should therefore be introduced progressively, with measurable validation of its recommendations before greater levels of automated decision-making are adopted.

IX. FUTURE SCOPE

Future development of AI-driven RCA is expected to move beyond the analysis of existing faults toward increasingly predictive and adaptive fixed-network service assurance. As historical operational data and validated incident records accumulate, AI models can improve their ability to recognize early patterns associated with congestion, intermittent failures, access degradation, and customer-experience deterioration. This could allow probable causes to be investigated before conventional alarms or significant service impact occur.

Another important direction is the development of continuous RCA learning. Confirmed relationships between symptoms, root causes, corrective actions, and subsequent performance can be retained as operational knowledge and reused during future incidents. This feedback mechanism can progressively improve probable-cause ranking and recommendation quality while reducing dependence on manually maintained troubleshooting rules.

Future RCA platforms may also integrate richer network context, including dynamic topology, service dependencies, CPE characteristics, customer-experience indicators, and historical operational actions. This would enable more accurate end-to-end reasoning across the access, transport, capacity, and customer domains.

As confidence in AI recommendations improves, selected low-risk corrective actions could progressively be integrated with closed-loop assurance mechanisms, while high-impact actions continue to require engineering approval. Previous research on Agentic AI and autonomous fixed-network operations has identified this progression from intelligent analysis toward increasingly autonomous assurance and decision-making [9], [10]. AI-driven RCA can therefore serve as an important enabling capability for the gradual evolution toward more intelligent and autonomous fixed telecommunications networks.

X. CONCLUSION

Root Cause Analysis is a fundamental component of fixed telecommunications service assurance, yet increasing network complexity and the growing volume of operational information make traditional manual and rule-based approaches increasingly difficult to scale. A single customer-visible symptom may originate from the FTTH access network, OLT/ONT infrastructure, IP transport, uplink capacity, CPE, or home Wi-Fi environment. Effective RCA therefore requires correlation across multiple network and service domains rather than analysis of individual alarms or KPIs in isolation.

This paper proposed an AI-driven RCA framework that integrates network and service data, KPI and alarm monitoring, anomaly detection, multi-source data correlation, AI-driven analysis, probable root-cause identification, corrective-action recommendations, and performance validation. Such an approach can complement conventional thresholds and engineering procedures by identifying abnormal patterns, correlating heterogeneous operational information, and prioritizing probable causes for further investigation. These capabilities are consistent with the broader evolution of AI-enhanced telecommunications operation and service assurance [1], [8].

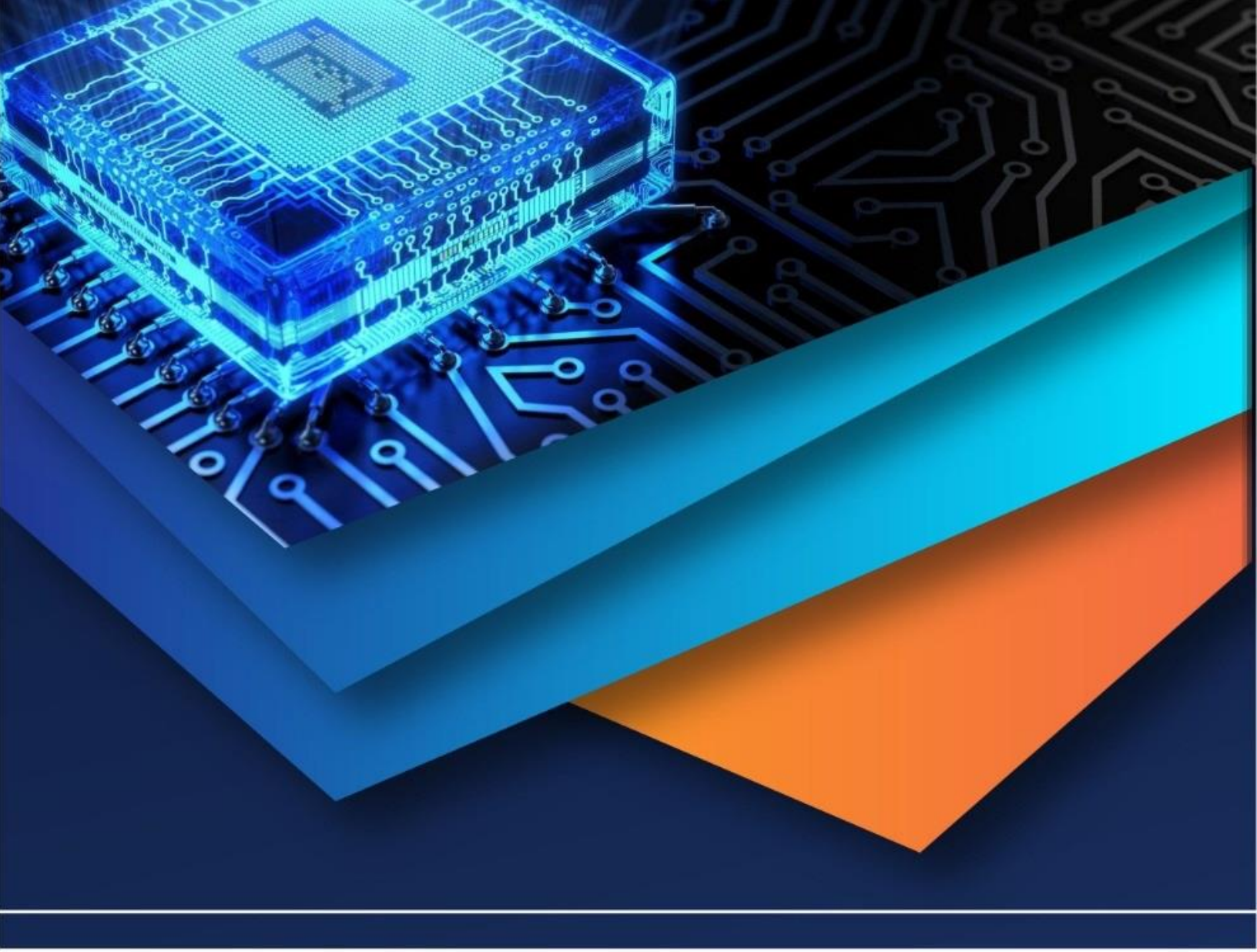
AI-driven RCA should not, however, be considered a replacement for network engineering expertise. Data quality, model accuracy, explainability, changing network conditions, and incorrect correlations remain important limitations. A practical implementation should therefore maintain engineering validation while progressively automating suitable analytical and low-risk operational activities.

Overall, AI-driven RCA represents an important step toward faster, more consistent, proactive, and increasingly intelligent fixed telecommunications network operations. Its greatest value lies in converting fragmented operational data into actionable evidence that enables engineers to identify and address service degradation more effectively.

REFERENCES

[1] ITU-T, Framework of Artificial Intelligence Enhanced Telecommunication Operation and Management (AITOM), Recommendation ITU-T M.3080, International Telecommunication Union, Geneva, Switzerland, Mar. 2026.
[2] TM Forum, AI for Observability & Service Assurance in Autonomous Networks, IG1343, Version 2.3.0, TM Forum, 2026.
[3] ITU-T, TMN Management Functions, Recommendation ITU-T M.3400, International Telecommunication Union, Geneva, Switzerland, Feb. 2000.
[4] M. Mustafa et al., “Optimizing Fixed Network Performance Through AI-Driven Operations and Analytics,” International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2026, doi: 10.22214/IJRASET.2026.83286.

[5] M. Mustafa et al., "AI-Driven Customer Experience Optimization in Fixed Broadband Networks," International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2026, doi: 10.22214/IJRASET.2026.83484.
[6] M. Liu, X. Qi, L. Liu, and H. Pan, "Roots-tracing of communication network alarm: A real-time processing framework," Computer Networks, vol. 192, Art. no. 108037, 2021, doi: 10.1016/j.comnet.2021.108037.
[7] M. Li, M. Yang, and P. Chen, "Alarm reduction and root cause inference based on association mining in communication network," Frontiers in Computer Science, vol. 5, Art. no. 1211739, 2023, doi: 10.3389/fcomp.2023.1211739.
[8] ITU-T, Requirements for Smart Comprehensive Analysis within Artificial Intelligence Enhanced Telecom Operation and Management (AITOM), Recommendation ITU-T M.3390, International Telecommunication Union, Geneva, Switzerland, Mar. 2025.
[9] M. Mustafa et al., "Agentic AI for Service Assurance in Fixed Broadband Networks: Conceptual Framework for Intelligent NOC," International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2026, doi: 10.22214/IJRASET.2026.83601.
[10] M. Mustafa et al., "From AI Analytics to Agentic AI: Framework for Autonomous Fixed Broadband Operations," International Journal for Research in Applied Science & Engineering Technology (IJRASET), 2026, doi: 10.22214/IJRASET.2026.83844.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY