International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

NEXORA: An Intelligent Network Incident Diagnosis and Automated Service Response System for Internet Service Providers

P P Rajeshwari
III MSC.SS
Department of Software Systems
Sri Krishna Arts and Science College
Coimbatore, India

Raveena R, Om Prakassh S, Pavish S, Pavithran S
III MSC.SS
Department of Software Systems
Sri Krishna Arts and Science College
Coimbatore, India

Abstract - Rapid growth in Internet Service Providers (ISPs) significantly increased the complexity of network operations and customer support. Network faults such as fibre link failures, Optical Line Terminal (OLT) issues, router connectivity problems, and service interruptions often require manual diagnosis and coordination among technical teams, resulting in delayed issue resolution and reduced customer satisfaction. To address these challenges, this paper proposes NEXORA – An Intelligent Network Incident Diagnosis and Automated Service Response System, a software-based solution designed to streamline network incident management and improve operational efficiency.

NEXORA continuously processes network event information obtained from network monitoring systems, operational logs, and incident reports to identify the probable cause of network faults. The proposed system classifies incidents based on their severity and automatically recommends appropriate actions. For minor issues, it provides guided troubleshooting instructions that help users resolve common connectivity problems. For major incidents, the system automatically generates support tickets, prioritizes the incident, notifies the technical team and customer support representatives, and maintains complete incident tracking until resolution. In addition, NEXORA records historical fault information and generates analytical reports to support network maintenance and operational decision-making.

The proposed architecture is developed using Python, Flask, MySQL, and Visual Studio Code, providing a scalable and modular framework that can be integrated with existing ISP operational workflows. By reducing manual intervention, improving incident response time, and centralizing network fault management, NEXORA has the potential to enhance service reliability, increase operational efficiency, and improve the overall customer experience. The proposed system offers a practical foundation for future intelligent network operation platforms that support automation and data-driven decision-making within modern Internet Service Providers.

Keywords: Network Fault Diagnosis, Internet Service Provider (ISP), Network Incident Management, Intelligent Network Operations, Automated Service Response, Network Monitoring, OLT, Fiber Optic Networks, Python, Flask

1. INTRODUCTION

The Internet has become an essential part of modern communication, supporting businesses, educational institutions, healthcare services, government organizations, and millions of residential users. As the demand for high-speed and uninterrupted internet connectivity continues to increase, Internet Service Providers (ISPs) are required to maintain highly reliable and efficient network infrastructures. These infrastructures consist of various networking components such as Optical Line Terminals (OLTs), fiber optic cables, routers, switches, Point of Presence (POP) stations, and customer premises equipment, all of which must operate continuously to ensure quality service.

Despite advancements in networking technologies, ISPs continue to face numerous operational challenges. Network failures caused by fibre cable damage, equipment malfunction, power outages, configuration errors, or signal degradation can lead to service interruptions affecting a large number of customers. In many organizations, the process of identifying the root cause of these failures still depends on manual monitoring, technician experience, and customer complaints. This manual approach often increases fault diagnosis time, delays service restoration, and places additional workload on Network Operations Centre (NOC) engineers and customer support teams.

Existing network management solutions primarily focus on monitoring network devices and generating alarms whenever

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

abnormal conditions occur. However, these systems generally provide limited assistance in identifying the actual cause of the problem, determining its severity, recommending corrective actions, or coordinating communication among technical teams and customers. As a result, engineers spend significant time analyzing alarms, creating support tickets manually, assigning technicians, and updating customers regarding service restoration.

To address these limitations, this research proposes **NEXORA – An Intelligent Network Incident Diagnosis and Automated Service Response System**. The proposed system is designed to improve network incident management by automatically analysing network events, identifying the probable cause of faults, classifying incidents based on severity, and initiating appropriate response mechanisms. For minor issues, NEXORA provides guided troubleshooting instructions that enable users to resolve common problems independently. For critical incidents requiring technical intervention, the system automatically generates service tickets, notifies technical personnel, informs customer support teams, and tracks the incident until successful resolution.

The proposed solution is implemented using Python, Flask, MySQL, and Visual Studio Code, providing a modular and scalable architecture suitable for deployment in ISP environments. By integrating intelligent fault diagnosis with automated incident response, NEXORA aims to reduce manual intervention, improve operational efficiency, minimize service downtime, and enhance the overall customer experience. The system also establishes a foundation for future intelligent network operations by supporting data-driven decision-making and automated service management.

2. PROBLEM STATEMENT

Internet Service Providers (ISPs) are responsible for delivering reliable and uninterrupted internet connectivity to residential, commercial, and enterprise customers. The number of subscribers and network devices grows, managing and maintaining the network infrastructure becomes increasingly complex. Network failures such as fiber cable cuts, Optical Line Terminal (OLT) faults, router malfunctions, power failures, configuration errors, and signal degradation can disrupt internet services and affect a large number of customers.

In many ISP environments, fault identification and incident management are still highly dependent on manual processes. Network engineers monitor alarms generated by network devices, analyse network logs, identify the root cause of the issue, create support tickets, assign field technicians, and communicate with customer support teams. This process often requires significant time and technical expertise, resulting in delayed fault diagnosis, slower service restoration, increased operational costs, and reduced customer satisfaction.

Another major challenge is the lack of an integrated system that not only detects network incidents but also analyzes their severity and coordinates the complete response process. Existing monitoring systems primarily generate alerts without providing intelligent fault diagnosis, automated troubleshooting recommendations, incident prioritization, or centralized communication between technical teams and customer support. Consequently, engineers must perform repetitive manual tasks before initiating corrective actions.

The absence of intelligent automation also increases the possibility of human error during incident handling and limits the organization's ability to respond proactively to network failures. Customers frequently experience delays in receiving service updates, while technical teams spend valuable time coordinating incident response instead of focusing on network restoration.

To overcome these challenges, there is a need for an intelligent software solution capable of automatically analysing network incidents, identifying probable fault causes, classifying issues based on severity, generating troubleshooting recommendations, automating ticket creation, notifying technical personnel, and maintaining complete incident tracking. Such a system can significantly improve operational efficiency, reduce response time, enhance service reliability, and improve the overall quality of customer support provided by Internet Service Providers.

3. OBJECTIVES OF PROPOSED SYSTEM

Primary objective of research is developing **NEXORA**, an intelligent software

solution for automated network incident diagnosis and service response in Internet Service Provider (ISP) environments. The proposed system is designed to enhance network operations by reducing manual intervention during fault detection, incident analysis, and service management.

NEXORA aims to intelligently analyse network events, identify the probable root cause of network failures, and classify incidents based on their severity. The system is intended to support technical teams by providing automated troubleshooting recommendations for minor faults while initiating an efficient incident response workflow for critical network failures. Furthermore, the proposed solution seeks to automate ticket generation, facilitate real-time notifications to technical personnel and customer support teams, and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

maintain complete incident lifecycle management from detection to resolution.

Another important objective in research is to establish the centralized platform for monitoring network incidents, maintaining historical fault records, and generating analytical reports that assist engineers and management in making informed operational decisions. The modular architecture of the proposed system also provides scalability, allowing future integration with live network monitoring infrastructures, intelligent analytics, and advanced automation technologies.

Ultimately, this research aims to improve service reliability, minimize network downtime, optimize operational efficiency, and enhance the overall quality of customer support through an intelligent and systematic approach to network incident management.

4. EXISTING SYSTEM

Modern Internet Service Providers (ISPs) employ various Network Management Systems (NMS), monitoring tools, and operational support platforms to supervise the performance and availability of their network infrastructure. These systems continuously monitor network devices such as Optical Line Terminals (OLTs), routers, switches, Point of Presence (POP) stations, and fiber links by generating alarms and event logs whenever abnormal network conditions are detected.

These monitoring solutions provided real-time visibility for network performing, the overall incident management process remains largely dependent on manual intervention. Network engineers are responsible for interpreting alarms, analysing multiple network parameters, identifying the root cause of faults, prioritizing incidents, creating service tickets, assigning field technicians, and coordinating with customer support teams. This manual workflow increases the complexity of network operations and often results in delayed fault diagnosis and prolonged service restoration.

In addition, existing systems primarily focus on event monitoring rather than intelligent decision-making. They generate numerous alarms without correlating related events or identifying the actual source of the problem. As a result, engineers must spend considerable time investigating incidents before initiating corrective actions. Furthermore, customer communication and service updates are generally performed manually, increasing operational workload and reducing overall service efficiency.

Another limitation of conventional network management systems is the absence of an integrated incident response mechanism that combines intelligent fault diagnosis, automated troubleshooting guidance, ticket generation, notification management, and incident lifecycle tracking within a unified platform. This lack of automation limits the ability of Internet Service Providers to respond quickly and efficiently to network failures, especially in large-scale network environments.

There is growing need for intelligent and automating network incident management capable of improving operational efficiency, reducing manual effort, minimizing service downtime, and enhancing the quality of customer support.

5. PROPOSED SYSTEM

To overcome the limitations of existing network management and incident handling systems, this research proposes **NEXORA – An Intelligent Network Incident Diagnosis and Automated Service Response System**. NEXORA is designed as an integrated software solution that automates the complete lifecycle of network incident management within Internet Service Provider (ISP) environments. The system combines intelligent fault diagnosis, automated decision-making, incident management, and notification services into a unified platform, thereby reducing manual intervention and improving operational efficiency.

The proposed system continuously processes network events obtained from monitoring systems, operational logs, and network devices. Instead of simply displaying alarms, NEXORA performs intelligent analysis to identify the probable root cause of each incident by evaluating network conditions and predefined diagnostic rules. Based on the diagnosis, the system categorizes the incident according to its severity and determines the most appropriate response mechanism.

For minor network issues that can be resolved without technical intervention, NEXORA automatically generates troubleshooting recommendations to assist support personnel or customers in restoring connectivity. For critical incidents requiring engineering support, the system automatically creates service tickets, assigns incident priorities, records all relevant fault information, and notifies the appropriate technical teams and customer support representatives. Throughout the incident lifecycle, NEXORA maintains complete tracking of the issue until successful resolution and closure.

The proposed system also incorporates centralized incident management, historical fault recording, and analytical reporting, enabling network administrators to monitor operational performance, identify recurring network problems, and support data-driven maintenance planning. The modular architecture ensures scalability, maintainability, and compatibility with existing ISP operational workflows, allowing future integration with live network monitoring infrastructures and intelligent network analytics.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

Compared with conventional network management systems, NEXORA provides a more intelligent and systematic approach to incident handling by integrating fault diagnosis, severity classification, automated response, ticket management, notification services, and resolution tracking within a single platform.

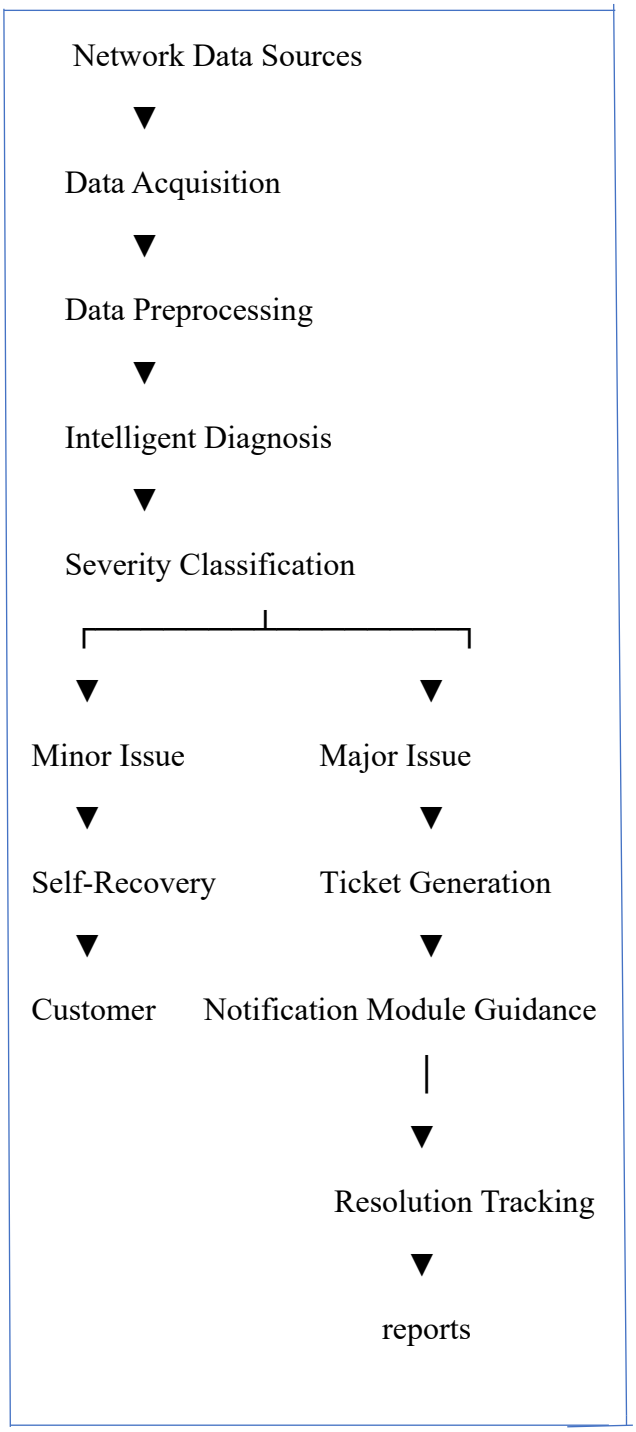

Figure 1. Overall System Architecture

6. SYSTEM ARCHITECTURE

The architecture of **NEXORA** is designed to provide an intelligent and automated approach to network incident management. The system consists of multiple interconnected modules that work together to detect network issues, analyze fault conditions, classify incident severity, generate appropriate responses, and manage the complete incident lifecycle.

Initially, network events are collected from monitoring systems and operational logs. The collected data is then analyzed by the Intelligent Diagnosis Engine to identify the probable cause of the network fault. Based on the diagnosis, the Severity Classification Module categorizes the incident as either minor or major. Minor issues are handled through automated troubleshooting recommendations, while major incidents trigger automatic ticket generation and notifications to the technical team and customer support. Finally, the Resolution Tracking Module monitors the progress of the incident until successful closure.

The modular architecture ensures scalability, maintainability, and efficient communication between all system components, enabling faster fault resolution and improved operational efficiency.

7. METHODOLOGY

The proposed NEXORA system follows a systematic approach to automate network incident management. Initially, network events are collected from monitoring systems and operational logs. The collected data is pre-processed and analysed to identify abnormal network conditions. An intelligent diagnosis mechanism determines the probable cause of the incident and classifies its severity.

Based on the severity level, the system either generates troubleshooting recommendations for minor issues or initiates an automated incident response for major faults. The incident response includes ticket generation, notification to technical personnel and customer support teams, and continuous tracking of the incident until successful resolution. Finally, all incident information stored for future analysis, reporting, the performance evaluation.

8. SYSTEM MODULES

8.1 Data Acquisition Module

This responsible in collecting network-related informing various sources, including network monitoring systems, operational logs, customer complaints, and simulated network events. It acts as the input layer of the proposed system by gathering all relevant network data required for further analysis. The collected information is validated,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

standardized, and forwarded to the Intelligent Diagnosis Engine for fault analysis. This module ensures the system receive accurate consistent data, enables reliable incident detection with effective network management.

8.2 Data Preprocessing Module

This Data preprocessing module prepares the collected network data for accurate analysis by removing duplicate records, validating input values, and organizing the data into a standardized format. It ensures data consistency and reliability before forwarding the processed information to the Intelligent Diagnosis Module. This preprocessing step minimizes errors during fault analysis and improves the overall efficiency and accuracy of the proposed system.

8.3 Intelligent Diagnosis Module

The intelligent diagnosis module is the core component of this proposed systems. It analyses pre-processed network data to identify the probable cause of network incidents using predefined diagnostic rules and network parameters. The module accurately determines the type of fault and forwards the diagnosis result to the Severity Classification Module for further processing.

8.4 Severity Classification Module

The Severity Classification Module categorizes the identified network incident based on its impact and urgency. The detected fault is classified into minor or major severity levels, enabling the system to determine the most appropriate response strategy. This classification ensures that critical incidents receive immediate attention while minor issues are handled through automated guidance.

8.5 Self-Recovery Recommendation Module

The Self-Recovery Recommendation Module provides automated troubleshooting instructions for minor network issues that can be resolved without technical intervention. Based on the diagnosed fault, the system generates appropriate corrective actions to assist users or support personnel in restoring network connectivity efficiently, thereby reducing unnecessary service requests.

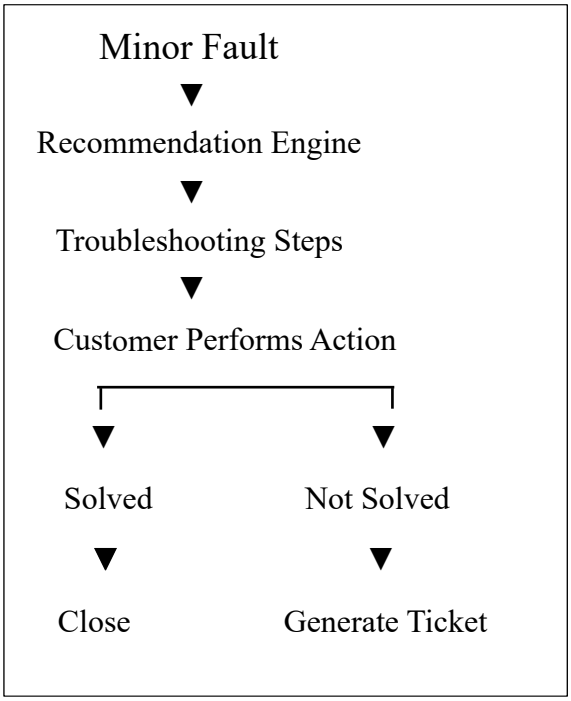

Figure:2 Self-Recovery Recommendation

8.6 Incident Response Module

The Incident Response Module initiates the appropriate actions for major network incidents. It coordinates the complete response process by triggering ticket generation, assigning incident priority, and activating the notification mechanism for the concerned technical teams. This module ensures a structured and timely response to critical network failures.

8.7 Ticket Generation Module

The Ticket Generation Module automatically creates a unique service ticket for every major network incident. Each ticket contains essential information such as incident details, customer information, fault description, severity level, timestamp, and current status. The generated ticket serves as the primary record for tracking and managing the incident until resolution.

8.8 Notification Management Module

The Notification Management Module automatically communicates network incidents to the respective stakeholders. It sends alerts to technical engineers, Network Operations Centre (NOC) personnel, customer support teams, and customers whenever necessary. This module ensures timely communication and improves coordination throughout the incident management process.

8.9 Resolution Tracking Module

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

The Resolution Tracking Module continuously monitors the progress of each incident from ticket creation to final closure. It records every stage of the resolution process, including engineer assignment, repair updates, verification, and completion status. This module provides complete visibility into the incident lifecycle and supports effective service management.

8.10 Analytics and Reporting Module

The Analytics and Reporting Module generates comprehensive reports based on historical network incidents and operational data. It provides insights into fault trends, incident frequency, resolution time, engineer performance, and overall network reliability. These reports assist network administrators and management in making informed decisions to improve operational efficiency and service quality.

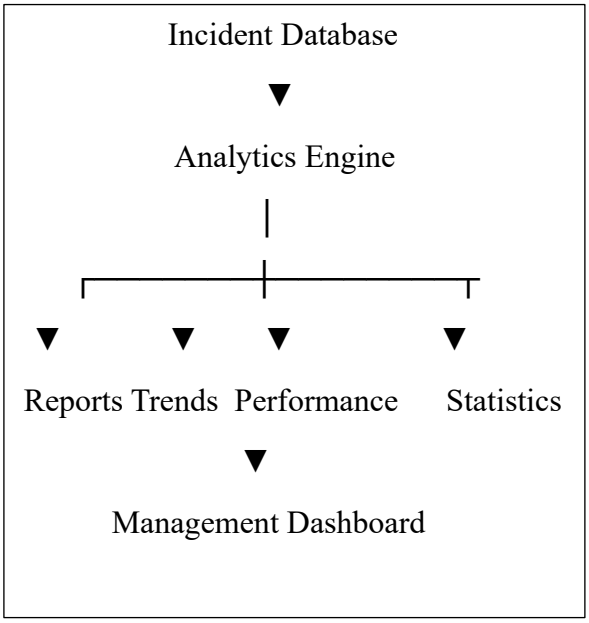

Figure 3: Analytics & Reporting

9. SYSTEM DESIGN

The system design of **NEXORA** defines the overall structure and interaction between various functional modules. It illustrates how network events are processed from data collection to incident resolution through a systematic and modular workflow. The proposed design emphasizes scalability, reliability, and automation, ensuring efficient fault diagnosis and service management. The system architecture includes multiple design components such as system architectural diagram, activity diagram, sequence diagrams, entity relationship diagram, and database design, which collectively represent the complete functionality of the proposed system.

9.1 System Architectural Diagram

The System Architecture Diagram illustrates this overall workflow of NEXORA by showing interaction between the major functional modules. It represents the flow of network data from acquisition to intelligent diagnosis, severity classification, automated incident response, notification management, and resolution tracking. This architecture provide a clear understand how proposed system processes network incidents and coordinates automated service responses.

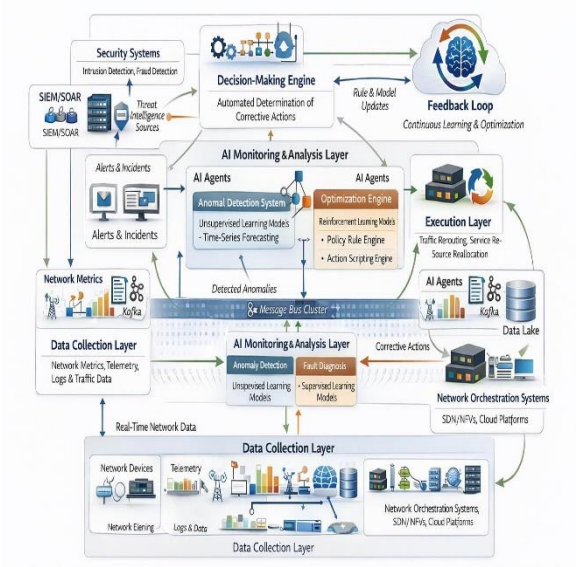

Figure 4: System Architecture Diagram

9.2 Use Case Diagram

This use case diagram represents the interacting different users and NEXORA systems. This primary actors include the Administrator, Network Operations Centre (NOC) Engineer, Technical Engineer, Customer Care Executive, and Customer. Each actor performs specific operations such as monitoring incidents, diagnosing faults, managing tickets, tracking resolution status, and viewing reports.

9.3 Activity Diagram

The Activity Diagram illustrates the sequence of activities performed by the proposed system during network incident management. It begins with network data collection, followed by fault detection, intelligent diagnosis, severity classification, automated response generation, ticket creation, notification, incident resolution, and finally ticket closure.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

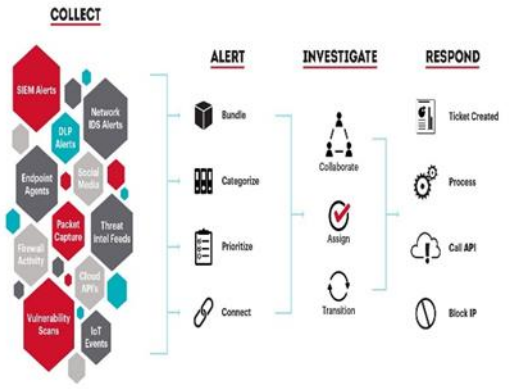

Figure 4.1 : Activity Diagram

9.4 Sequence Diagram

The Sequence Diagram describes the interaction between system components during the execution of a network incident. It shows the communication flow among the user, system modules, database, notification service, and technical team, ensuring proper coordination throughout the incident lifecycle.

9.5 ER Diagram

The entity relationship diagram represents this logical structure of the database used in NEXORA. It defines the relationships between entities such as Customer, Network Device, Incident, Ticket, Engineer, Notification, and Resolution History, ensuring efficient storage and retrieval of operational data alone with records, service tickets, notifications, and historical data.

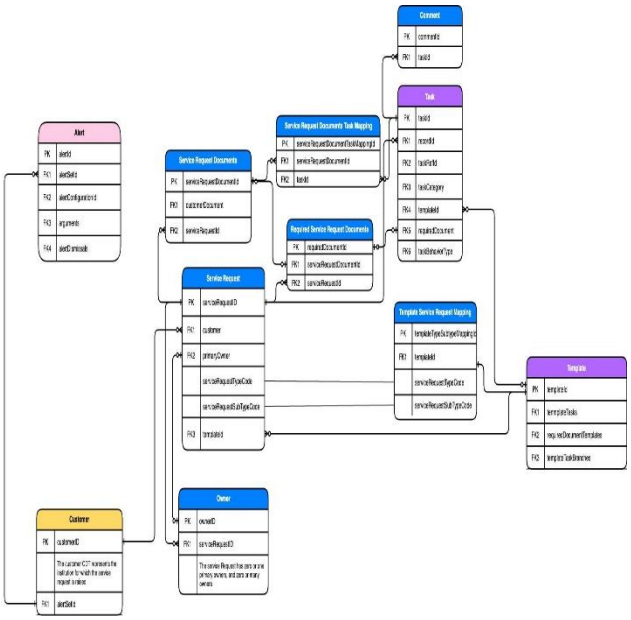

Figure 4.2: ER Diagram

9.6 Database Design

The database design provides a structured mechanism for storing and managing network incident information. It consists of multiple relational tables that maintain customer details, device information, incident records, support tickets, notification logs, engineer assignments, and resolution history. The database ensures data integrity, consistency, and efficient access to operational information required by the proposed system.

10. IMPLEMENTATION

The proposed NEXORA system implemented as web-based applications that automate process network incident diagnosis and service response. The system is developed using a modular architecture to ensure scalability, maintainability, and efficient integration of all functional components. Each module performs a specific task, enabling seamless communication throughout the incident management process.

The frontend of the application is designed using HTML, CSS, and Bootstrap to provide an interactive and user-friendly interface. The backend is developed using Python and the Flask framework, which manages business logic, module interactions, and database communication. MySQL is used as the relational database for storing customer information, incident records, service tickets, notifications, and historical data.

The implementation begins with collecting network event information, followed by preprocessing and intelligent fault diagnosis. Based on the identified fault severity, the system either generates troubleshooting recommendations or initiates an automated incident response by creating service tickets and notifying the concerned personnel. All incident activities are recorded in the database, enabling continuous monitoring, resolution tracking, and analytical reporting.

The modular implementation approach simplifies future enhancements and allows the proposed system to be integrated with real-time network monitoring platforms and advanced intelligent technologies.

11. RESULTS AND DISCUSSION

This proposed NEXORA systems were successfully developed and tested to automate the process of network incident diagnosis and service response. The system effectively processes network event information, identifies the probable cause of network incidents, classifies their severity, and initiates appropriate response mechanisms. Minor issues are addressed through automated troubleshooting recommendations, while major incidents

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

trigger ticket generation, notification services, and incident tracking.

This experiments result demonstrates the proposed systems significantly reduces manual intervention during network fault management by integrating multiple operational tasks into a single platform. The modular architecture ensures efficient communication between different system components, resulting in faster incident processing and improved coordination among technical teams.

The generated reports and historical incident records provide valuable insights into network performance, fault trends, and resolution activities. The proposed solution also improves the efficiency of technical support operations by maintaining complete visibility throughout the incident lifecycle.

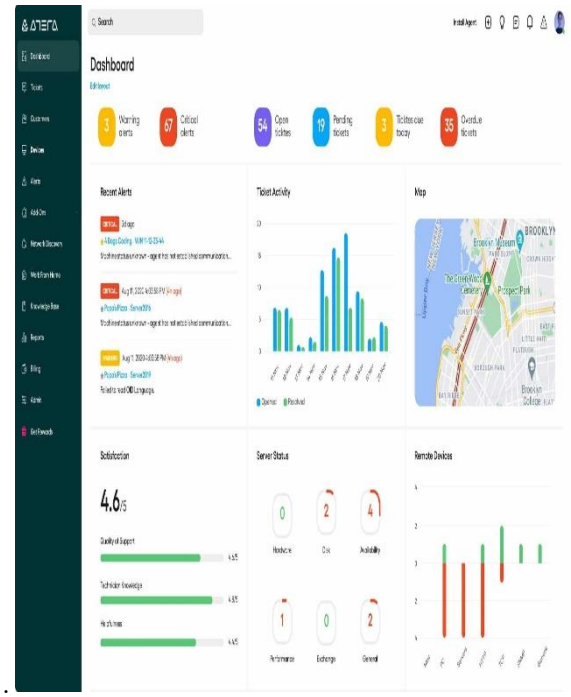

Figure 5 : NEXORA

12. CONCLUSION

This research presented **NEXORA**, an intelligent network incident diagnosis and automated service response system designed to improve network fault management in Internet Service Provider (ISP) environments. The proposed system integrates network event analysis, intelligent fault diagnosis, severity classification, automated ticket generation, notification management, and incident tracking into a unified platform. By reducing manual intervention and streamlining the incident management process, NEXORA enhances operational efficiency, minimizes service downtime, and improves coordination among technical teams and customer support. The modular architecture of the system ensures scalability, reliability, and ease of future integration with advanced network monitoring technologies. Overall, the proposed solution provides an effective approach for intelligent network operations and contributes to improved service quality and customer satisfaction.

Figure 6: Network Incident Analytics

13. FUTURE SCOPE

The proposed NEXORA system provides a strong foundation for intelligent network incident management and can be enhancing with advance technology. This improvements may include integration with real-time network monitoring systems such as OLTs, routers, and Network Management Systems (NMS) for live fault detection. Artificial Intelligence and ML algorithm can incorporated that enable predictive fault analysis and proactive maintenance. The system can also be extended with cloud-based deployment, mobile application support, geospatial visualization of network infrastructure, and advanced analytics for capacity planning and performance optimization. These enhancements will further improve automation, scalability, and operational efficiency, making NEXORA a comprehensive solution for modern Internet Service Provider environments.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 09 , September - 2026

14. REFERENCES

[1] H. Yan, A. Flavel, Z. Ge, A. Gerber, D. Massey, and C. Papadopoulos, "Argus: End-to-End Service Anomaly Detection and Localization from an ISP's Point of View," Proceedings of IEEE INFOCOM, 2012.

[2] "Design of Network Monitoring System for IoT and Autonomous Network Using Python," IEEE Conference Publication, 2023.

[3] J. Steinberger, B. Kuhnert, A. Serotta, H. Baier, and A. Pras, "Collaborative DDoS Défense Using Flow-Based Security Event Information," IEEE/IFIP Network Operations and Management Symposium (NOMS), 2016.

[4] B. H. Oh, S. Vural, and N. Wang, "A Lightweight Scheme of Active-Port Aware Monitoring in Software-Defined Networks," IEEE Transactions on Network and Service Management, vol. 18, no. 1, 2021.

[5] "NetEye: Network Monitoring for a Software Defined Network-Based Virtualized Network Functions Platform," IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE), 2021.

[6] A. Messager et al., "Network Events in a Large Commercial Network: What Can We Learn?," IEEE/IFIP Workshop on Analytics for Network and Service Management (Anet), 2018.

[7] H. Mostafaei and S. Afridi, "P4Flow: Monitoring Traffic Flows With Programmable Networks," IEEE Communications Letters, vol. 25, no. 11, 2021.

[8] R. Sadre, A. Sperotto, and A. Pras, "The Effects of DDoS Attacks on Flow Monitoring Applications," IEEE Network Operations and Management Symposium (NOMS), 2012.

[9] J. Haxhibeqiri, P. H. Isolani, J. M. Marquez-Barja, I. Moerman, and J. Hoebeke, "In-Band Network Monitoring Technique to Support SDN-Based Wireless Networks," IEEE Transactions on Network and Service Management, vol. 18, no. 1, 2021.

[10] Python Software Foundation, Python Documentation. Available: https://docs.python.org/

[11] Flask Development Team, Flask Documentation. Available: https://flask.palletsprojects.com/

[12] Oracle Corporation, MySQL 8.0 Reference Manual. Available: https://dev.mysql.com/doc/