Automating Network Log Analysis for Telecom Outage

Document

By

TEAM MYSTIQUE

VIT Chennai.

#DATASET24- a 36-hour national-level hackathon hosted by ECDS

at Vellore Institute of Technology, Chennai.

1. INTRODUCTION

In the rapidly evolving telecommunications industry, network reliability and uptime are paramount for maintaining customer satisfaction and operational efficiency. Nevertheless, network outages persist as significant challenges, frequently resulting in extended downtime and disrupted services.

Telecommunications operators traditionally allocate substantial time and effort to manually analyse logs and network traces in order to pinpoint the root cause of these outages. This process is not only time-consuming but also susceptible to errors due to the complexity and scale of the data involved.

#Problem Statement:

Telecom operators spend significant time analysing logs and network traces to determine the cause of network outages. How can automation improve the speed and accuracy of this process without compromising reliability?

To address the challenges of analysing network logs and traces, **we propose an automated, multi-layered solution that integrates advanced AI models, anomaly detection techniques, and an intuitive visualization system**. The proposed solution aims *to improve the speed, accuracy, and reliability of root cause analysis for network outages.*

By employing advanced tools such as *Large Language Models (LLMs)* and *anomaly detection frameworks*, the proposed solution endeavours to:

1. Accelerate the identification of root causes.
2. Enhance the precision and reliability of the analysis.
3. Reduce the reliance on manual intervention.

Through automation, the system seeks to streamline outage resolution, thereby expediting recovery times and enhancing network reliability.

Key Considerations:

Scalability: The solution must *efficiently handle large datasets*.

Flexibility: *Adaptable* to various log formats and network trace types.

User-Friendliness: *Provides actionable insights* in a clear and digestible format.

2. Proposed Solutions

To address the challenges of analysing network logs and traces, we propose an automated, multi-layered solution that integrates advanced artificial intelligence models, anomaly detection techniques, and an intuitive visualization system. The proposed solution aims to enhance the speed, accuracy, and reliability of root cause analysis for network outages.

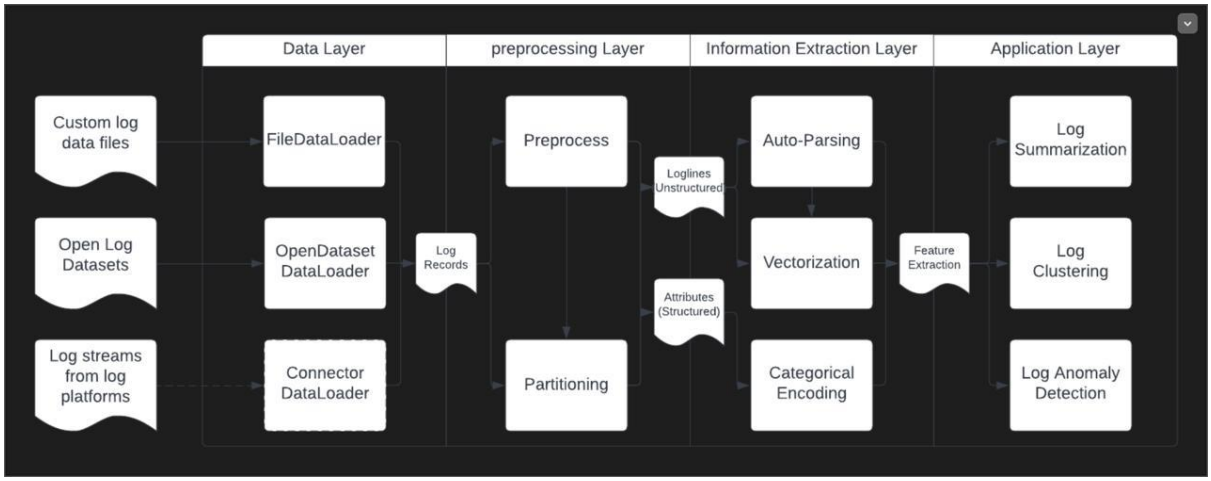
1. Log Parsing and Analysis Automation

Objective: Automate parsing and structuring of logs for easier analysis.

Approach:

1. Use automation tools to parse unstructured data into structured formats.
2. Apply machine learning to identify recurring patterns and anomalies in logs.
3. Correlate log entries across systems and timeframes to pinpoint outage sources.

Example Tools: Elasticsearch, Logstash, Kibana (ELK stack), Splunk.



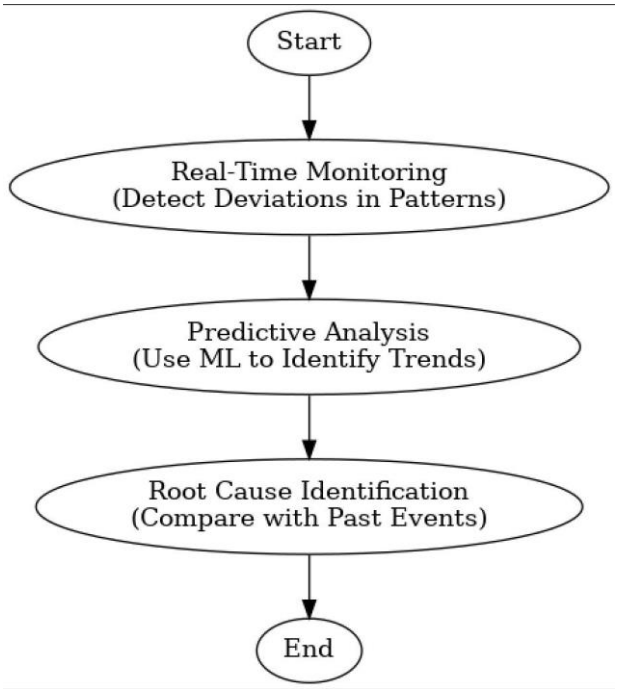
2. Anomaly Detection with AI and ML

Objective: Identify *anomalies or irregularities in network behaviour* that may indicate the root cause of an outage.

Approach:

1. Continuously monitor *network data streams for deviations* from normal patterns.
2. Analyse trends and historical data to *predict potential issues proactively.*
3. Identify *probable failure causes by comparing anomalies* with past events.

Recommended Techniques: Supervised learning for classification, unsupervised learning for anomaly detection.



Anomaly Detection Procedure

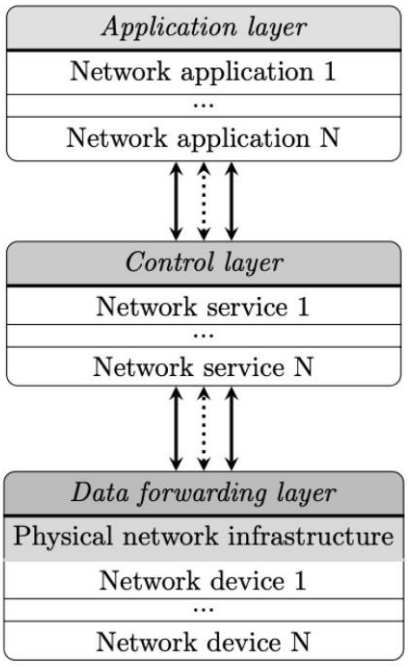
3. Automated Playbooks for Incident Response

Objective: Automate troubleshooting procedures and incident management processes.

Approach:

1. Implement *predefined workflows* that execute scripts for detected issues.
2. Execute *dynamic diagnostics* based on the outage type to gather pertinent data.
3. Integrate with *ticketing systems for automated creation and prioritization of tickets.*

Recommended Tools: ServiceNow, PagerDuty, Ansible.



Automated Playbooks Practice

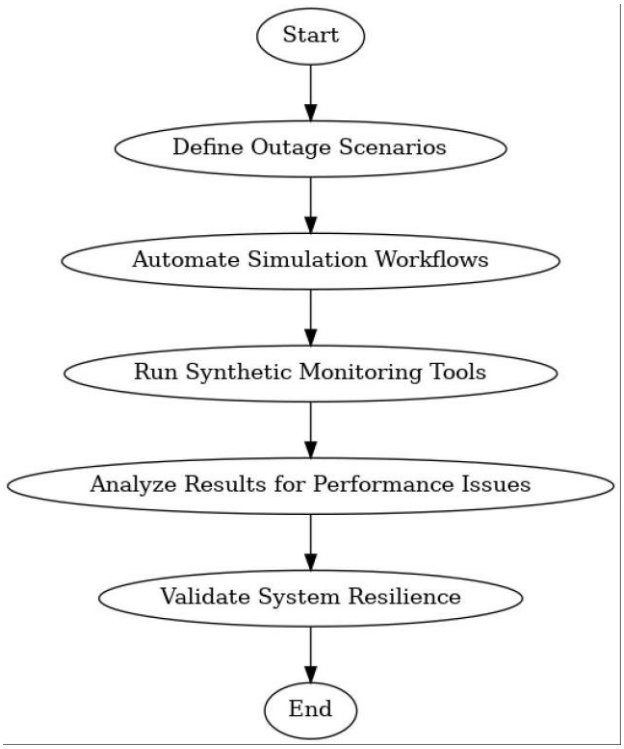
4. Network Simulation and Testing

Objective: *Simulate and test outage scenarios* to validate workflows.

Approach:

1. *Automate simulations of outage* scenarios to test system resilience.
2. Utilize *synthetic monitoring* tools to simulate user behaviour and *identify performance anomalies.*

Recommended Tools: NetBrain, ThousandEyes.



Network Simulation

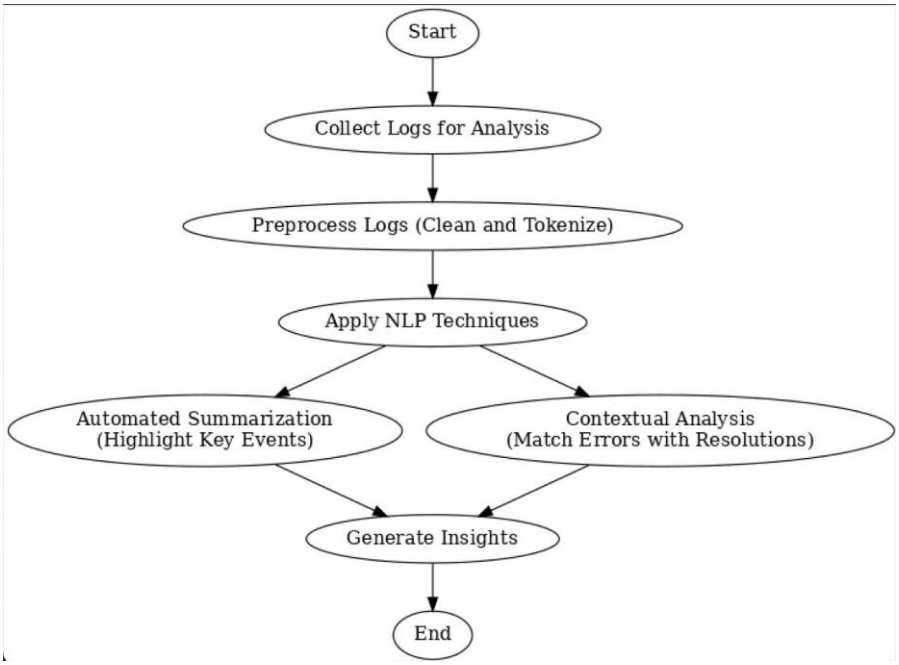
5. Natural Language Processing (NLP) for Log Analysis

Objective: Extract insights and summarize lengthy logs using NLP.

Approach:

1. Use NLP to summarize logs and highlight key events or anomalies.
2. Match error descriptions with known resolutions from knowledge bases.

Recommended Tools: OpenAI, Google Cloud NLP.



NLP for Logs Analysis

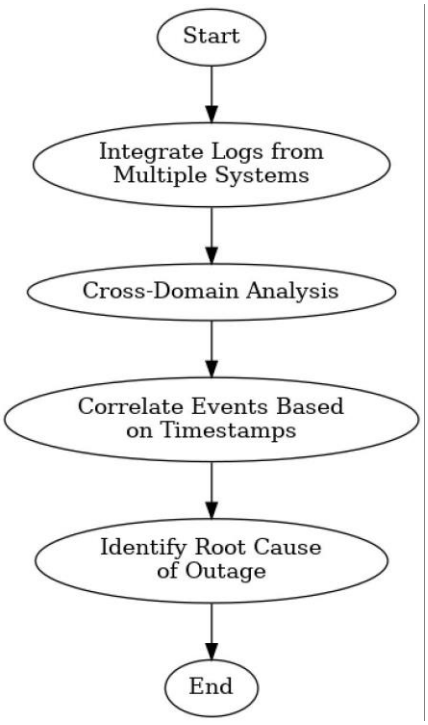
6. Corelation Across Systems

Objective: Integrate and *analyse logs from multiple systems holistically.*

Approach:

1. Perform *cross-domain analysis* by integrating logs from routers, switches, and servers.
2. Use *time-series analysis to correlate events* across systems based on timestamps.

Recommended Tools: Prometheus, Grafana, Splunk.



Systems Corelations

7. Proactive Alerting and Visualizations

Objective: Provide *real-time visualizations and proactive alerts* for quick responses.

Approach:

1. Automate the creation of *dashboards for real-time network health metrics*.
2. Set *thresholds for metrics* and *generate alerts* when limits are breached.

Recommended Tools: Zabbix, Nagios, Datadog.

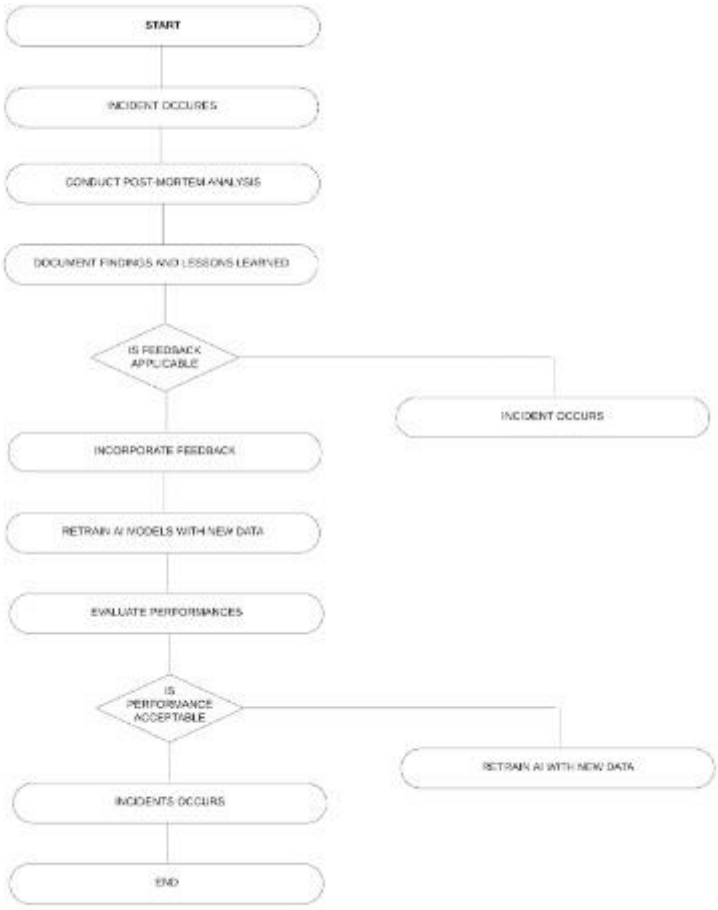
Proactive Alerting

8. Continuous Learning and Improvements

Objective: Continuously *enhance automation pipelines* through feedback and retraining.

Approach:

1. Incorporate *post-mortem analyses into workflows* to improve processes.
2. Retrain *AI models with new data* to adapt to evolving network behaviours.
3. Use *incident reports to refine anomaly detection models* for greater accuracy.



Continuous Learning and Improvements