Automated Network Monitoring & Alerting System

TEAM M58

Abdalrhman Owaida, Kureym Alzarea , Abdulaziz Hakami, Hussain Bin Hashim, Mohammed Alharthy, Abdalrahman Isleem

Coach: Uthman Baroudi

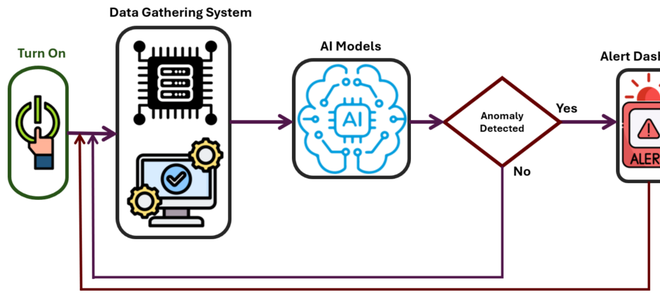
COE ICS 3 ISE

PROPLEM STATEMENT

The campus network at KFUPM lacks intelligent, real-time monitoring and automated threat detection capabilities, making it difficult for network administrators to quickly identify performance degradation, abnormal traffic behavior, and potential security intrusions, which can delay incident response, reduce network reliability, and increase the risk of undetected cyberattacks.

Prototype design

- Backend: Python, FastAPI, Postgres.
- Frontend: React.
- AI/ML: Symbolic AI for anomalies in availability and performance. Random Forest model for cyberattacks.
- Hardware: Cisco Network Devices
- Protocols: SNMP, ICMP, HTTP, DNS, NetFlow, and ARP.



An **Anomaly** is lack of availability, significant degradation in performance, or cyberattacks.

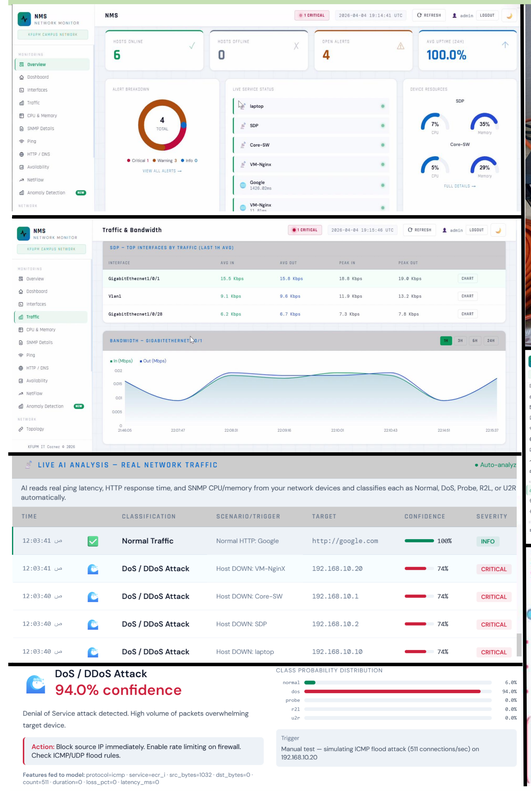
Specifications and Constraints

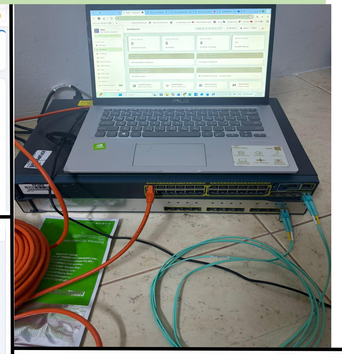
Specifications
UI load time: < 2 seconds.
Root cause: per anomaly.
SNMP collected: ≤ 60s intervals.
availability < 15 seconds.
Anomaly filter recall ≥ 75%.
functions executable in ≤ 4 clicks.
Maximum 30 unique operations.
Preprocessing completes in ≤ 10s per cycle.
Anomaly filter precision ≥ 80%.

Constrains
Sole data source: KDD Cup knowledge base.
Read-only telemetry; no write operations.
Dashboard info accessible in ≤ 2 clicks.
No university datasets for AI training.
Node deployment time < 5 minutes.

Integrated Specifications
90-second max latency for node data delivery to AI.
Alerts must update within 30 seconds of data arrival.
Generate diagnostic hypotheses within 15 seconds of detection.

Testing & Validation





Conclusion

- The ML AI achieved 99.98% recall and 99.99 precision. The Symbolic AI achieved 94.76% recall and 87.17% precision.
- The system met all 17 specified requirements.
- Deployment can be completed within 3 minutes.
- Demonstrates a scalable, high-performance system for detecting and identifying root causes of network availability issues, performance degradation, and cyberattacks.