Scammers 25

Anushka Harale

Shravani Kale

Shruti Deshmukh

Siddhi Chavhan

MKSSS's Cummins College Of Engineering,Pune

PROBLEM STATEMENT :

Application logs are critical for debugging and monitoring, but their volume and complexity often overwhelm teams. The challenge is to create an **AI-driven log analyzer that processes logs across multiple sources**, extracts actionable insights, and automates log analysis.

Agenda

1. Introduction
2. Proposed Solution
3. Methodology
4. Results and Outcomes
5. Impact and Applications
6. Future Scope
7. Conclusion

Introduction

Problem: Application logs are critical for debugging and monitoring, but their volume and complexity often overwhelm teams. The challenge is to create an AI-driven log analyzer that processes logs across multiple sources, extracts actionable insights, and automates log analysis.

Automated Log Parsing & Aggregation.

AI-Powered Analysis Converts

Interactive Dashboard

Role Based Access Control

Predictive Insights

Log Summary Statistics

Visualization of logs summary

User Management

1. **Log Parsing and Aggregation :**
   - Collect logs from servers, databases, and web services.
   - Support JSON, XML, and Plain Text formats.

2. **AI-Based Analysis :**
   - Use pretrained NLP (DistilBERT) to classify log entries into categories.
   - Zero-shot classification using facebook’s BART model.
   - Clustering algorithms to group similar errors.

3. **Advanced Analytics**
   - TF-IDF + K-Means clustering to group similar logs
   - Trend analysis with linear regression for error prediction

4. **Visualization and Reporting :**
   - Interactive dashboards for real-time insights.

5. **Role Based Access:**
   - User roles: Admin, Developer, Manager, Viewer
   - Permissions:
     - view_all, configure, alerts, predictions, remedies.

6. **Security Features**
   - SHA-256 password hashing

Technologies

Backend: Python

Libraries & Tools: Pandas, NumPy, Matplotlib, Scikit-learn

AI Models: DistilBERT (Transformer) for NLP.

Findings from previous work.

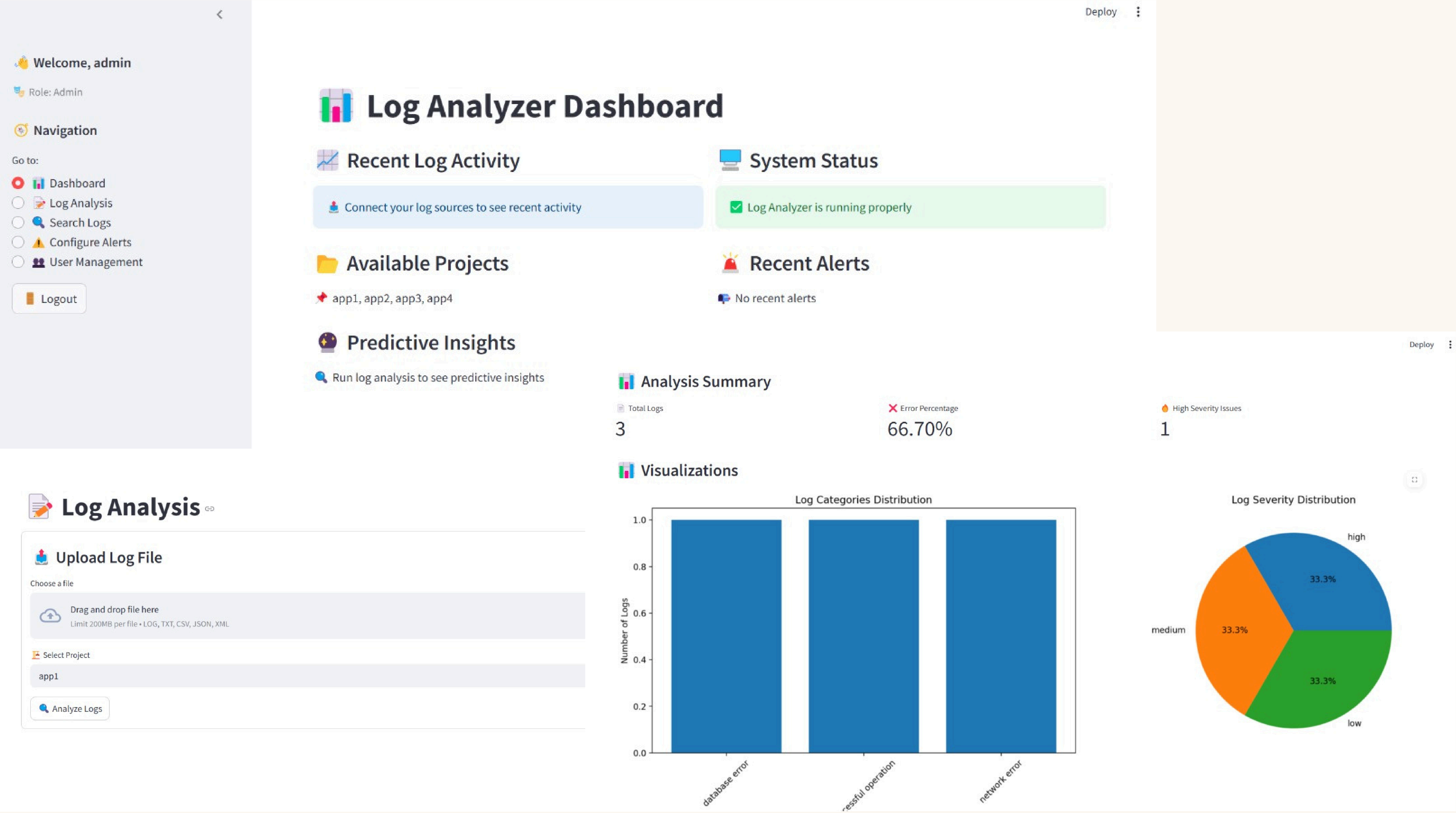
1. Manual Analysis Dominance:
2. Limited Context Awareness:
3. Poor Handling of Unstructured Logs:
4. Lacking unified dashboards:

Gap Identified in existing solutions

Lack of AI/ML Adoption:
Few tools leverage zero-shot classification or sentiment analysis for dynamic log categorization.

Limited Remediation Guidance:
Identifies errors but fails to suggest actionable fixes.

Weak Access Control:
No role-based permissions for team collaboration (e.g., devs vs. admins)



Deploy

Welcome, admin

Role: Admin

Navigation

Go to:

- ● Dashboard
- ○ Log Analysis
- ○ Search Logs
- ○ Configure Alerts
- ○ User Management

Logout

Log Analyzer Dashboard

Recent Log Activity

Connect your log sources to see recent activity

System Status

✓ Log Analyzer is running properly

Available Projects

app1, app2, app3, app4

Recent Alerts

No recent alerts

Predictive Insights

Run log analysis to see predictive insights

Log Analysis

Upload Log File

Choose a file

Drag and drop file here
Limit 200MB per file • LOG, TXT, CSV, JSON, XML

Select Project

app1

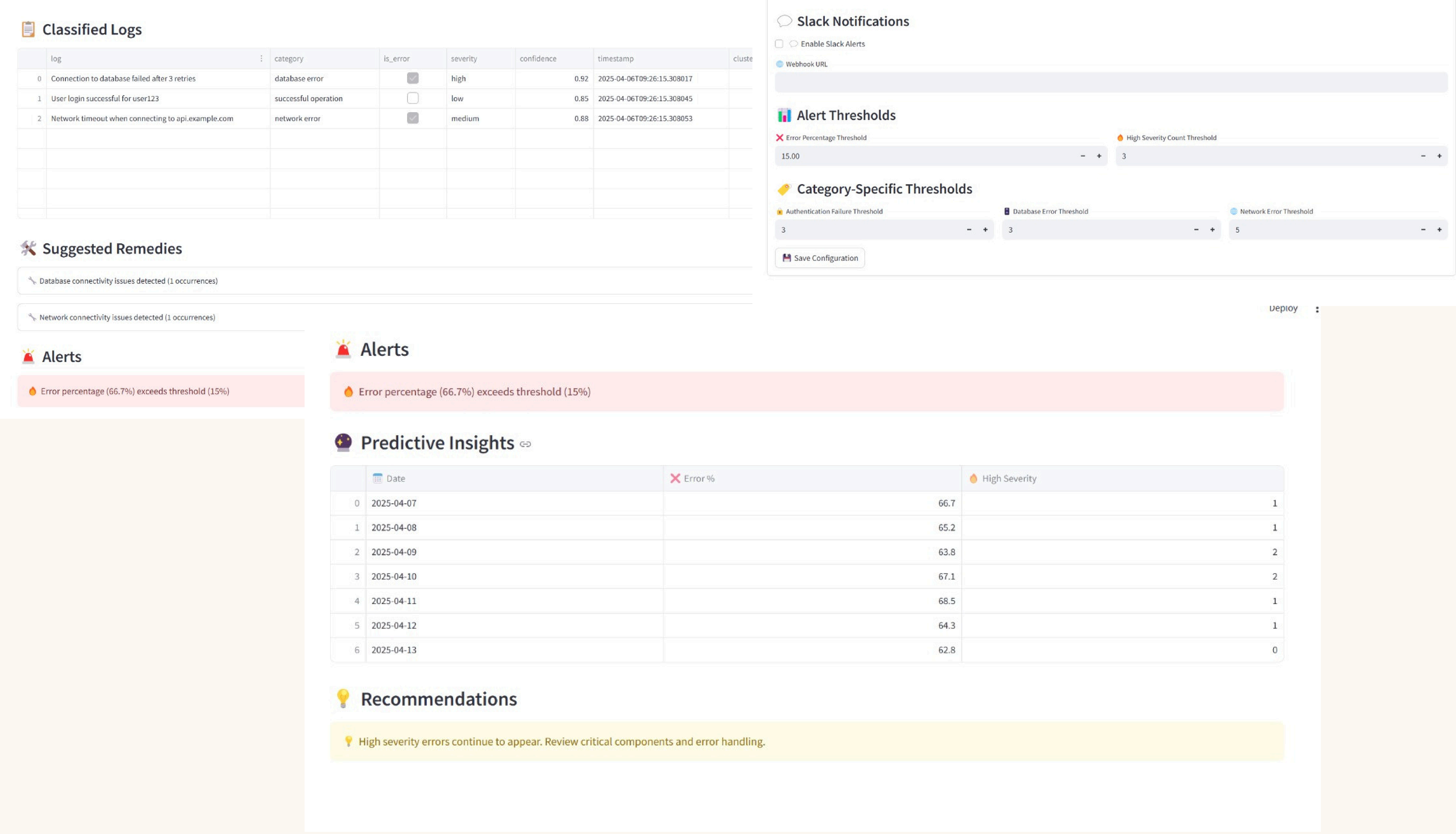
Analyze Logs

Deploy

Analysis Summary

Total Logs	Error Percentage	High Severity Issues
3	66.70%	1

Visualizations



📋 Classified Logs

	log	category	is_error	severity	confidence	timestamp	cluste
0	Connection to database failed after 3 retries	database error	☑	high	0.92	2025-04-06T09:26:15.308017	
1	User login successful for user123	successful operation	☐	low	0.85	2025-04-06T09:26:15.308045	
2	Network timeout when connecting to api.example.com	network error	☑	medium	0.88	2025-04-06T09:26:15.308053	

🛠 Suggested Remedies

🔧 Database connectivity issues detected (1 occurrences)

🔧 Network connectivity issues detected (1 occurrences)

🚨 Alerts

🔥 Error percentage (66.7%) exceeds threshold (15%)

💬 Slack Notifications

☐ 💬 Enable Slack Alerts

🌐 Webhook URL

📊 Alert Thresholds

❌ Error Percentage Threshold: 15.00 − +

🔥 High Severity Count Threshold: 3 − +

🏷 Category-Specific Thresholds

🔒 Authentication Failure Threshold: 3 − +

🗄 Database Error Threshold: 3 − +

🌐 Network Error Threshold: 5 − +

💾 Save Configuration

🚨 Alerts

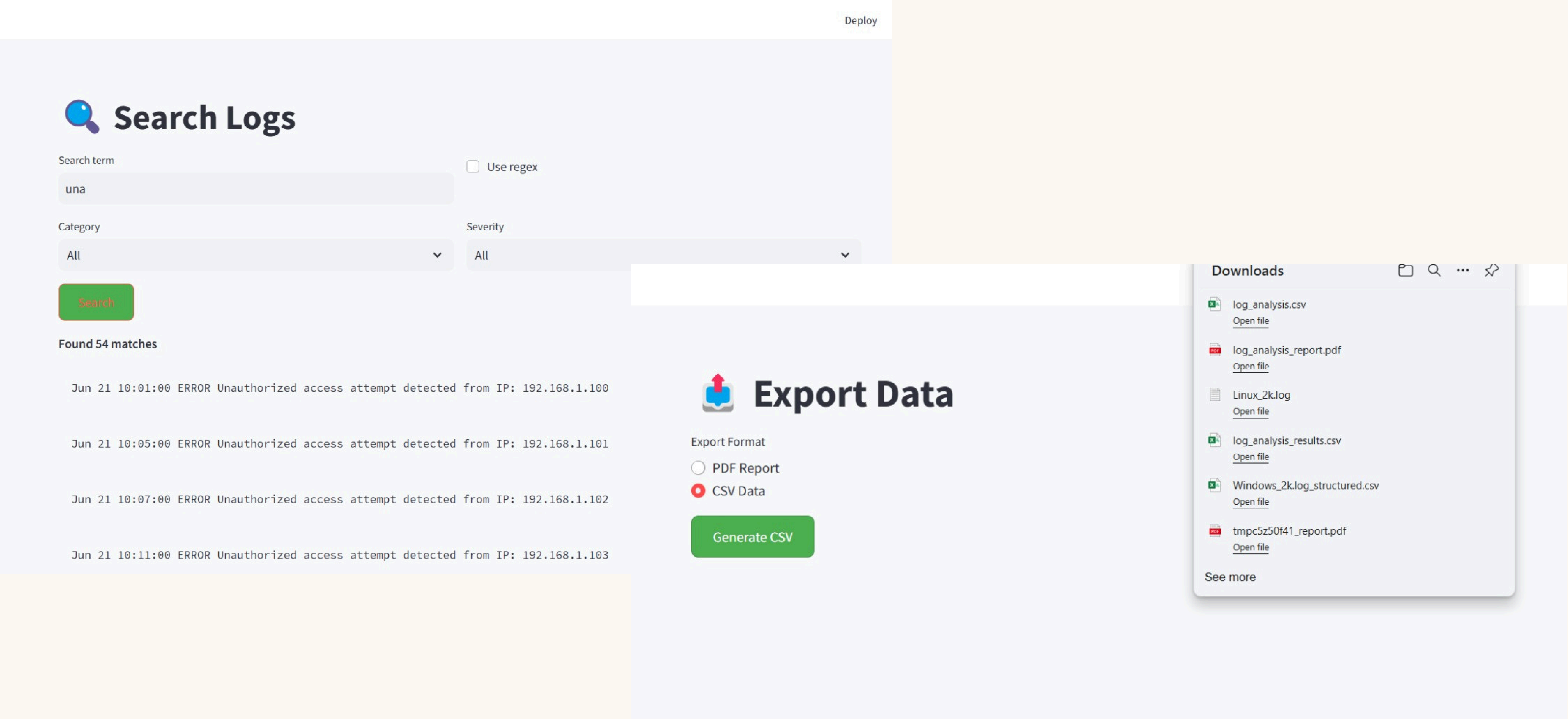
🔥 Error percentage (66.7%) exceeds threshold (15%)

🔮 Predictive Insights

	📅 Date	❌ Error %	🔥 High Severity
0	2025-04-07	66.7	1
1	2025-04-08	65.2	1
2	2025-04-09	63.8	2
3	2025-04-10	67.1	2
4	2025-04-11	68.5	1
5	2025-04-12	64.3	1
6	2025-04-13	62.8	0

💡 Recommendations

💡 High severity errors continue to appear. Review critical components and error handling.



Search Logs

Search term: una

□ Use regex

Category: All

Severity: All

Found 54 matches

```
Jun 21 10:01:00 ERROR Unauthorized access attempt detected from IP: 192.168.1.100

Jun 21 10:05:00 ERROR Unauthorized access attempt detected from IP: 192.168.1.101

Jun 21 10:07:00 ERROR Unauthorized access attempt detected from IP: 192.168.1.102

Jun 21 10:11:00 ERROR Unauthorized access attempt detected from IP: 192.168.1.103
```

Export Data

Export Format

○ PDF Report

● CSV Data

Downloads

log_analysis.csv
Open file

log_analysis_report.pdf
Open file

Linux_2k.log
Open file

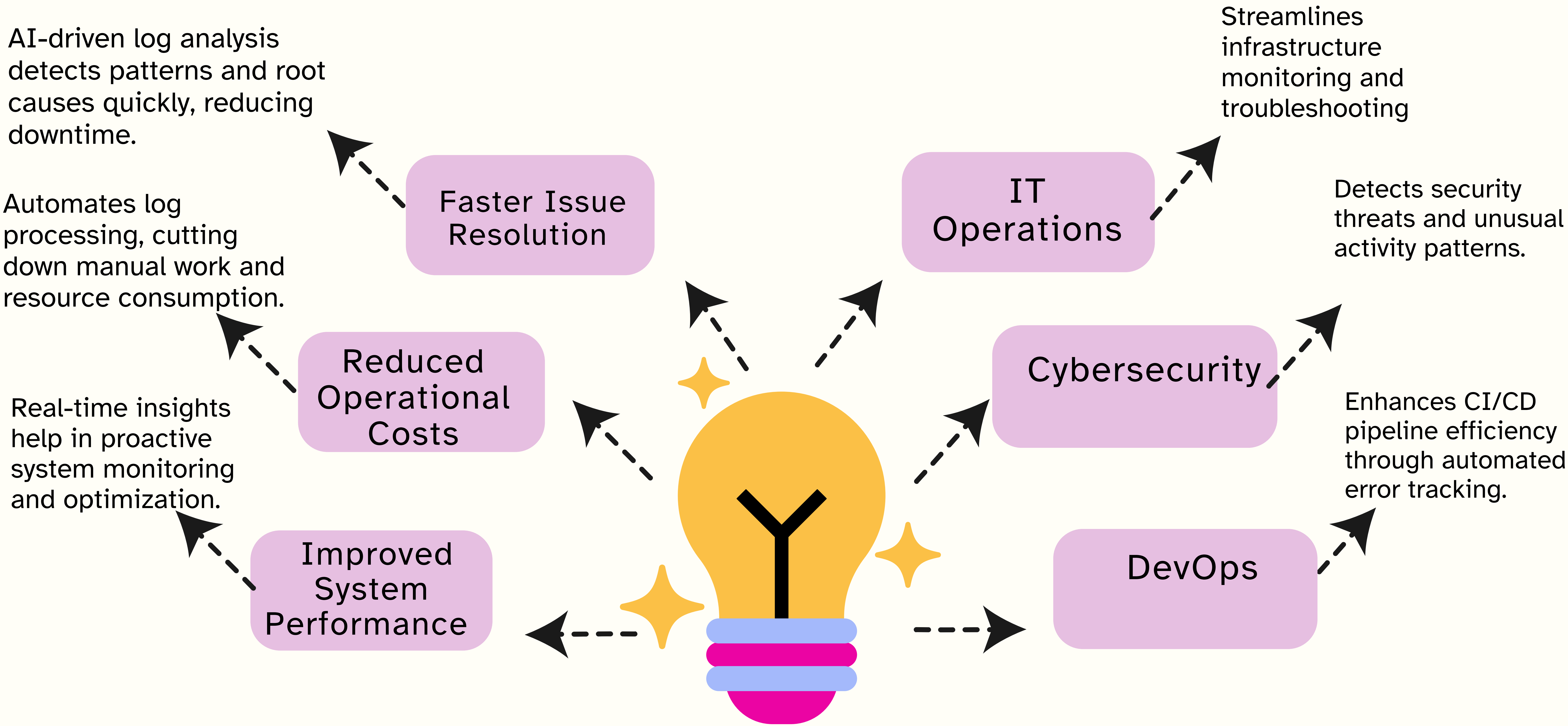
log_analysis_results.csv
Open file

Windows_2k.log_structured.csv
Open file

tmpc5z50f41_report.pdf
Open file

IMPACTS :

APPLICATIONS :



Faster Issue Resolution

AI-driven log analysis detects patterns and root causes quickly, reducing downtime.

Reduced Operational Costs

Automates log processing, cutting down manual work and resource consumption.

Improved System Performance

Real-time insights help in proactive system monitoring and optimization.

IT Operations

Streamlines infrastructure monitoring and troubleshooting

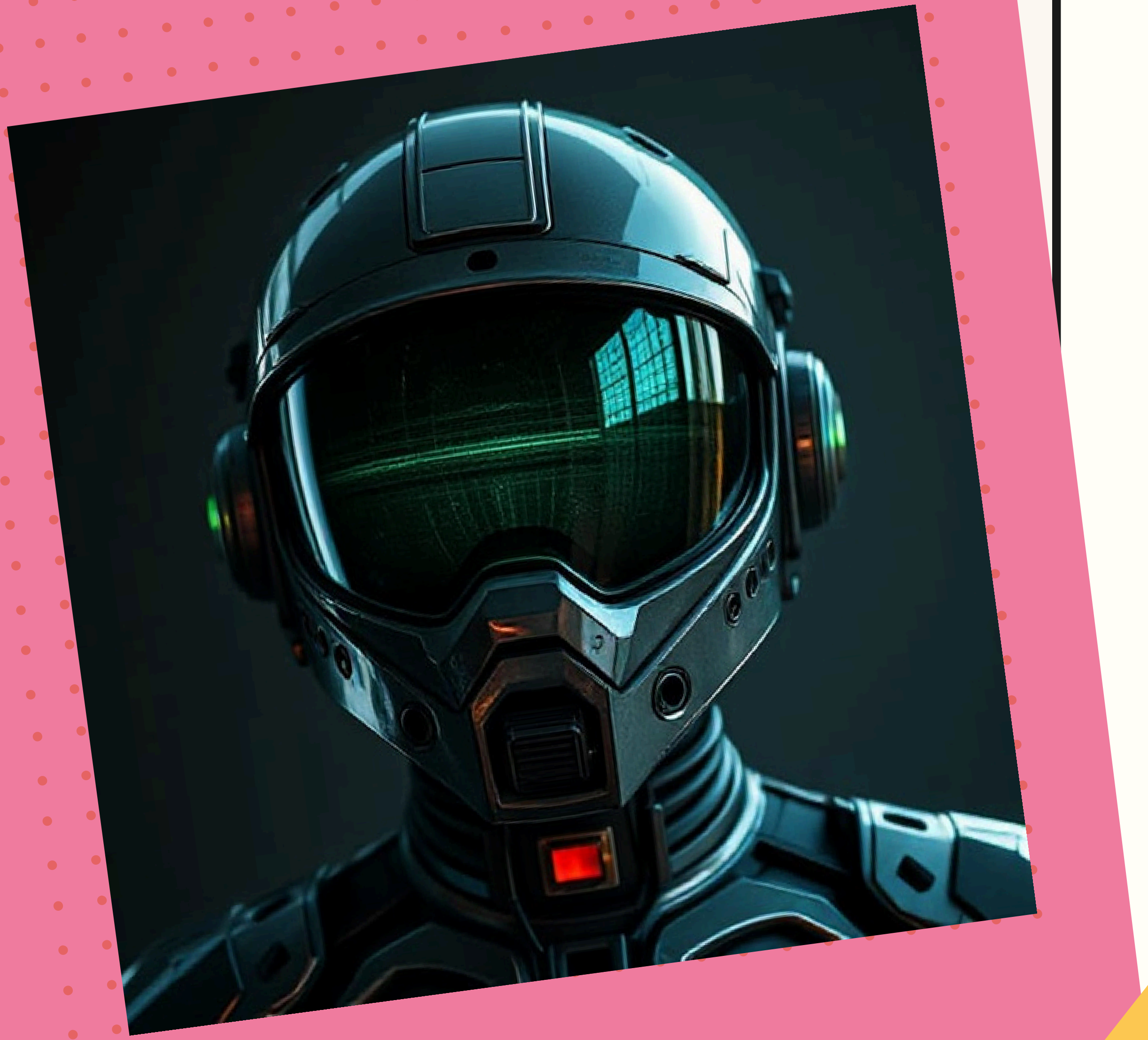
Cybersecurity

Detects security threats and unusual activity patterns.

DevOps

Enhances CI/CD pipeline efficiency through automated error tracking.

FUTURE SCOPE



- **ADVANCED AI MODELS**

Integration of more sophisticated AI models for better pattern recognition and anomaly detection.

- **REAL-TIME THREAT MITIGATION**

Implement AI-powered auto-response mechanisms to prevent failures and security breaches.

- **CROSS-PLATFORM COMPATIBILITY**

Develop a mobile and web-based version for on-the-go log analysis.

- **INTEGRATION WITH CLOUD PLATFORMS**

Enable seamless log aggregation and analysis across multiple cloud services..

CONCLUSION

- LogAI is an AI-powered tool that automates and enhances log analysis.
- It integrates multiple technologies to identify patterns and detect anomalies in real-time.
- The project contributes to a more secure and efficient system monitoring future.

THANK YOU!