NIRF-2024
Engineering Rank Band (151-200)
Pharmacy Rank - 77
Innovation Rank Band (11-50)

www.kiet.edu
Delhi-NCR, Ghaziabad

KIET GROUP OF INSTITUTIONS
Connecting Life with Learning

Accredited by
NAAC with Grade "A+"

DEPARTMENT OF COMPUTER SCIENCE

Project Presentation (BCS 554)
(IT SYSTEM LOG ANALYZER)

Guide Name With Designation

Project Members Name with Roll Number & Section

Mridul sharma (2300290129007) C

Vikas Yadav (2300290129015) C

Mayank (2300290129006) B

NIRF-2024
Engineering Rank Band (151-200)
Pharmacy Rank - 77
Innovation Rank Band (11-50)

www.kiet.edu
Delhi-NCR, Ghaziabad

KIET GROUP OF INSTITUTIONS
Connecting Life with Learning

Accredited by
NAAC with Grade "A+"

Table of content

Problem Statement

- Modern IT systems generate vast amounts of log data from servers, applications, network devices, databases, and security appliances.
- These logs contain critical information about the operation, performance, errors, and security events occurring within the system.
- However, due to the sheer volume and complexity of logs, manual log analysis is impractical, leading to missed alerts, unidentified performance issues, and undetected security threats.

Objectives

- The IT System Log Analyzer aims to automate the collection, parsing, storage, and analysis of logs from various sources in real-time. This tool will enable system administrators, security personnel, and DevOps teams to:
- Identify critical errors and performance bottlenecks.
- Detect security incidents like unauthorized access, DDoS attacks, and data breaches.
- Generate insights into system usage patterns, performance trends, and resource consumption.
- Provide visual reports, alerts, and dashboards for better decision-making.

Technology Used

Domain Overview

The IT System Log Analyzer domain revolves around analyzing log data generated by IT infrastructure .Logs contain time-stamped records of system activities, errors, performance metrics, and security events.

Front-End: User Interaction and Visualization

The front-end of the IT System Log Analyzer refers to the user-facing components that allow administrators, security teams, and engineers to interact with the system, configure alerts, and visualize log data.

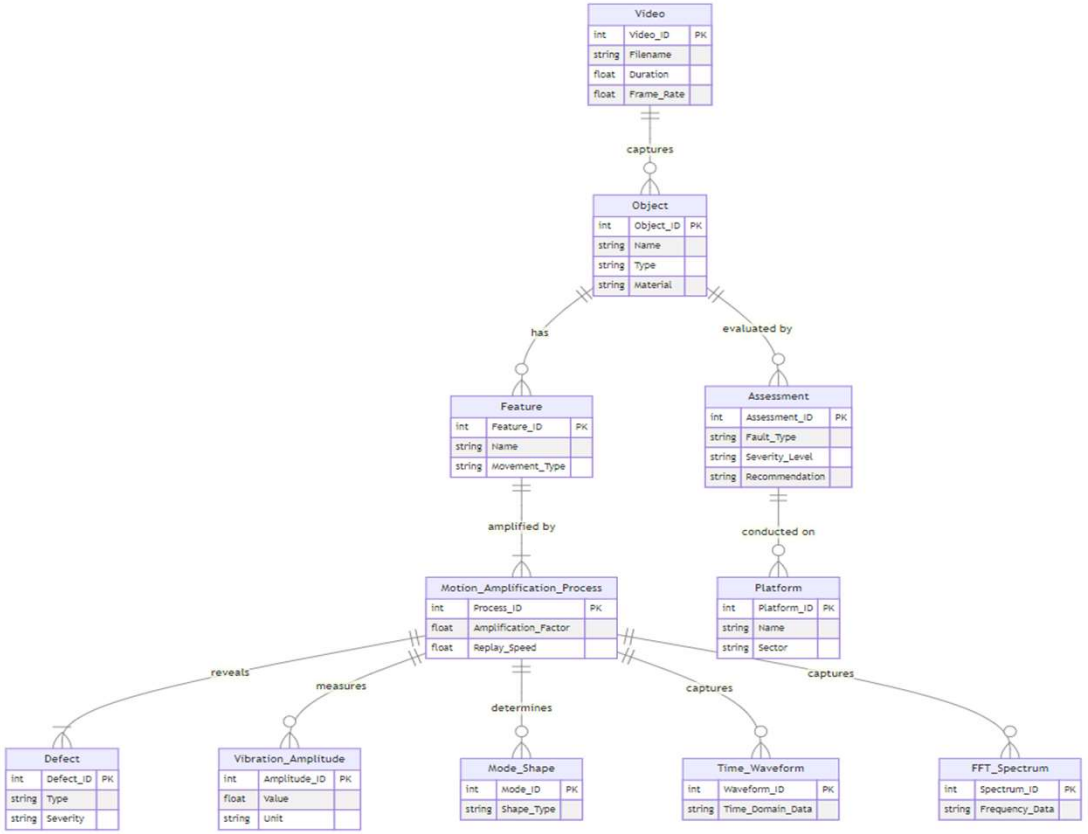
Back-End: Data Processing and Log Analysis

The **back-end** of the IT System Log Analyzer handles data ingestion, processing, storage, and the application of rules for log analysis. It is responsible for scalability, ensuring that even large volumes of logs can be processed efficiently.

Literature Survey

- Early approaches to log management focused on simple text-based logs and manual analysis.
- As systems became more complex and the volume of log data increased, automated tools and techniques were developed to handle larger datasets.
- Sutton (1990) explored early methods of log file management and analysis, emphasizing the importance of log data for troubleshooting and system monitoring.
- Eckhardt and Lee (1995) discussed the evolution of look management practices as systems grew in scale, highlighting the need for more sophisticated tools to manage increasing log volumes

Diagrams


Video
int Video_ID PK
string Filename
float Duration
float Frame_Rate
captures
Object
int Object_ID PK
string Name
string Type
string Material
has
evaluated by
Feature
int Feature_ID PK
string Name
string Movement_Type
Assessment
int Assessment_ID PK
string Fault_Type
string Severity_Level
string Recommendation
amplified by
conducted on
Motion_Amplification_Process
int Process_ID PK
float Amplification_Factor
float Replay_Speed
Platform
int Platform_ID PK
string Name
string Sector
reveals
measures
determines
captures
captures
Defect
int Defect_ID PK
string Type
string Severity
Vibration_Amplitude
int Amplitude_ID PK
float Value
string Unit
Mode_Shape
int Mode_ID PK
string Shape_Type
Time_Waveform
int Waveform_ID PK
string Time_Domain_Data
FFT_Spectrum
int Spectrum_ID PK
string Frequency_Data

NIRF-2024
Engineering Rank Band (151-200)
Pharmacy Rank - 77
Innovation Rank Band (11-50)

www.kiet.edu
Delhi-NCR, Ghaziabad

KIET GROUP OF INSTITUTIONS
Connecting Life with Learning

Accredited by
NAAC with Grade "A+"

Patent Status

NIL

Research Paper Status

- NIL

NIRF-2024
Engineering Rank Band (151-200)
Pharmacy Rank - 77
Innovation Rank Band (11-50)

www.kiet.edu
Delhi-NCR, Ghaziabad

KIET GROUP OF INSTITUTIONS
Connecting Life with Learning

Accredited by
NAAC with Grade "A+"

Project Status

Github Link.

git@github.com:mridulsharma2226/IT-System-Log-Analyzer.git

References

- A. Oliner, A. Ganapathi, and W. Xu, "Advances and Challenges in Log Analysis," *Communications of the ACM*, vol. 55, no. 2, pp. 55-61, Feb. 2012, doi: 10.1145/2076450.2076466.
- Lou, L. Zhang, Q. Lin, Z. Zheng, P. He, and M. R. Lyu, "Log Efficient: A Log Analysis Platform for Large-Scale Log Data," *2017 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, Prague, Czech Republic, 2017, pp. 458-465, doi: 10.1109/QRS.2017.57.