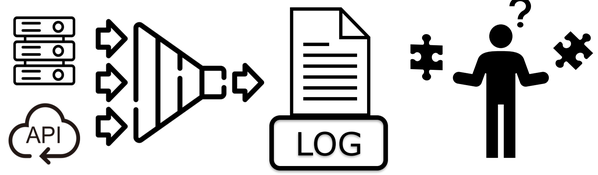
Log Anomaly Analytics Platform (LAAP): Structure, Pinpoint, Explain, Explore

Authors: Suhani Chaudhary[1], Ethan Shanbaum[2], Athanasios Tassiadamis[3]
Advisors: Elke Rundensteiner[2], Lei Ma[2], Peter VanNostrand[2]
[1]University of California, Riverside, [2]Worcester Polytechnic Institute, [3]University of Nevada, Las Vegas

Motivation

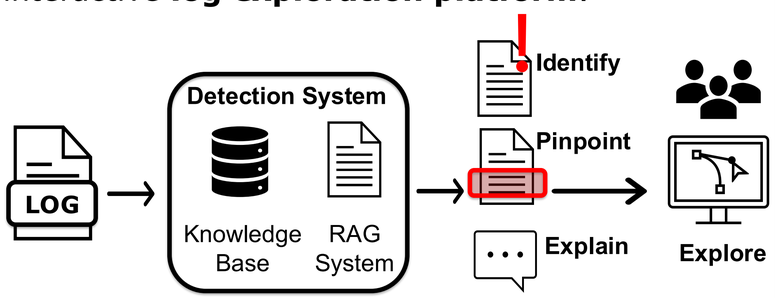
Log anomaly detection is vital for identifying critical system failures, such as data breaches, which cost organizations an average of **$4.9 million per incident** [2].

Dense log files and system complexity make root cause analysis and anomaly detection challenging



Proposed Solution

Utilize an **LLM-based** detection system to identify, pinpoint, and explain log anomalies for an interactive **log exploration platform**.



Structure Log Data

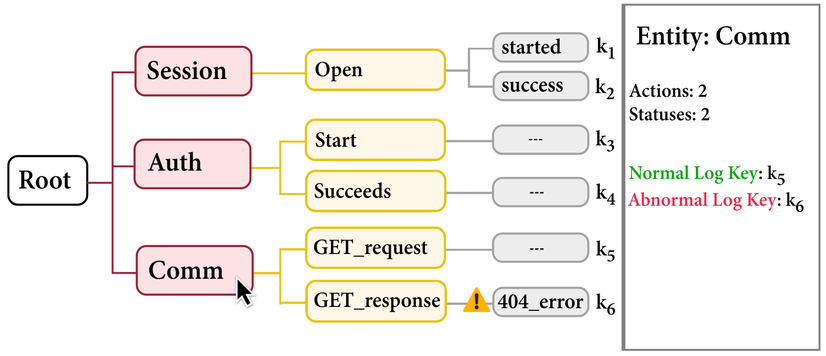
Extract clear hierarchical structure from flat logs

Flat Log File
1. Open session id=1243 started
2. Session opened successfully
3. Auth start pwd=******
4. Auth succeeds
5. Comm: GET_request at URL="/api/v1/d3"
6. Comm: GET_response error 404 at URL="api/v1/d3"
7. Comm: POST_request at URL="/api/v1/f2/edit"
...
9586. Auth logout successful
9587. Session end id=1243

Entity	Action	Status	Key
Session	open	started	k_1
Session	open	success	k_2
Auth	start	-	k_3
Auth	succeed	-	k_4
Comm	GET request	-	k_5

Pinpoint Underlying Hierarchy

Understand **underlying structure** in the log data to determine which templates are **abnormal**



Entity: a software component or resource

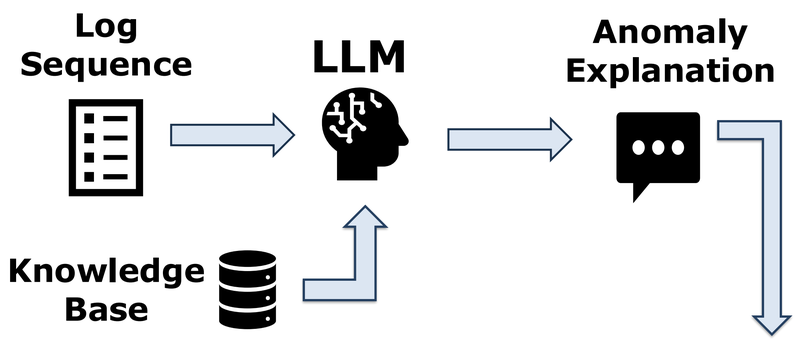
Action: an operation performed by or on the entity

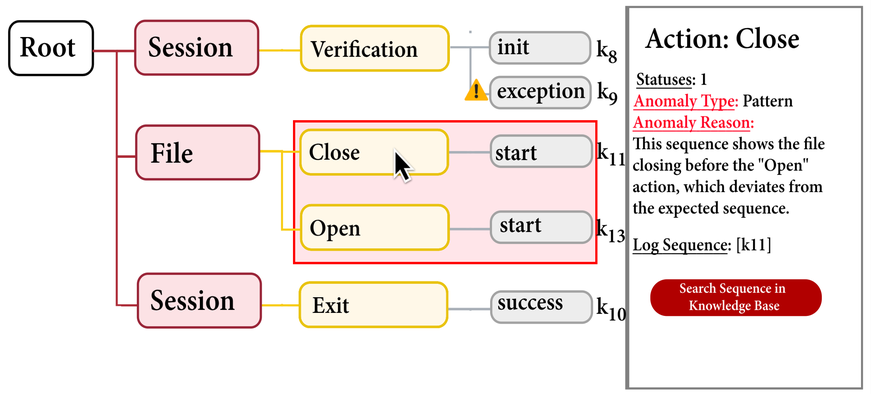
Status: the outcome or condition of the action

⚠ : an anomalous log template

Explain Log Anomalies

LLM uses **archived sequences** in the knowledge base to explain **detected anomalies** in a sequence

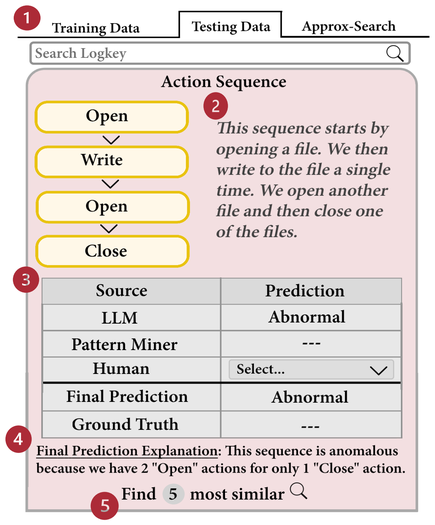




Explore Sequence Patterns

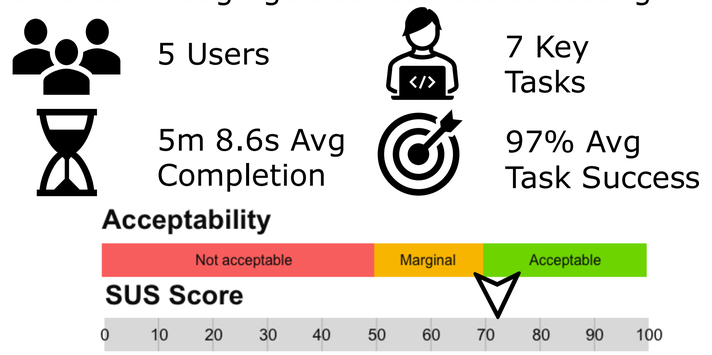
Query **similar log sequences** from the knowledge base with **LLM explanations**

1. Stores training and testing data
2. Anomaly Explanation
3. Manipulation analytics
4. Prediction explanation
5. Similarity search



User Evaluation

Evaluated ease of use and user success in identifying anomalies through guided task-based testing



Impact Statement

Our technology provides **powerful** LLM-driven log **analytics capabilities.**

Acknowledgements & GitHub

Thanks to:
NSF for funding (#2349370)

QR code:
Demo website, citations, and testing setup