KYUNGPOOK NATIONAL UNIVERSITY

Intelligent Software Systems Lab
KYUNGPOOK NATIONAL UNIVERSITY

주요 연구 발표

시스템 이상징후 탐지를 위한 모니터링 및 로그 기반 이상징후 탐지 기술 소개

권영우

ywkwon@knu.ac.kr

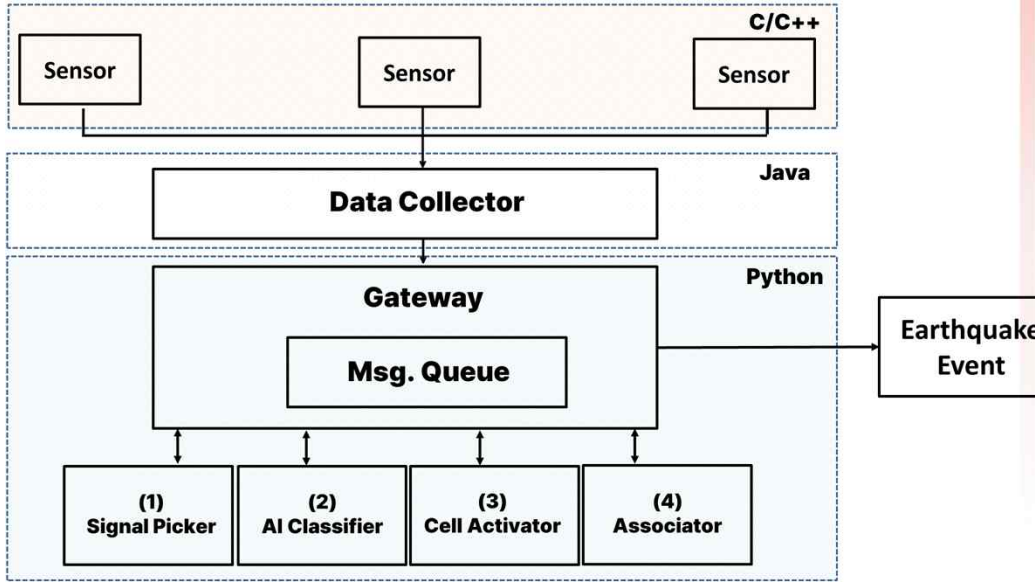
http://sslab.knu.ac.kr

주요 연구 내용

- 테스트베드 구축 및 활용 지원
- 이상징후 탐지 연구
  - 산학협력연구
  - 로그 기반 이상징후 탐지 연구
- 테스트베드 대상 PySTAAR 적용 연구 (센터내 공동연구)

테스트베드- 지진조기경보체계

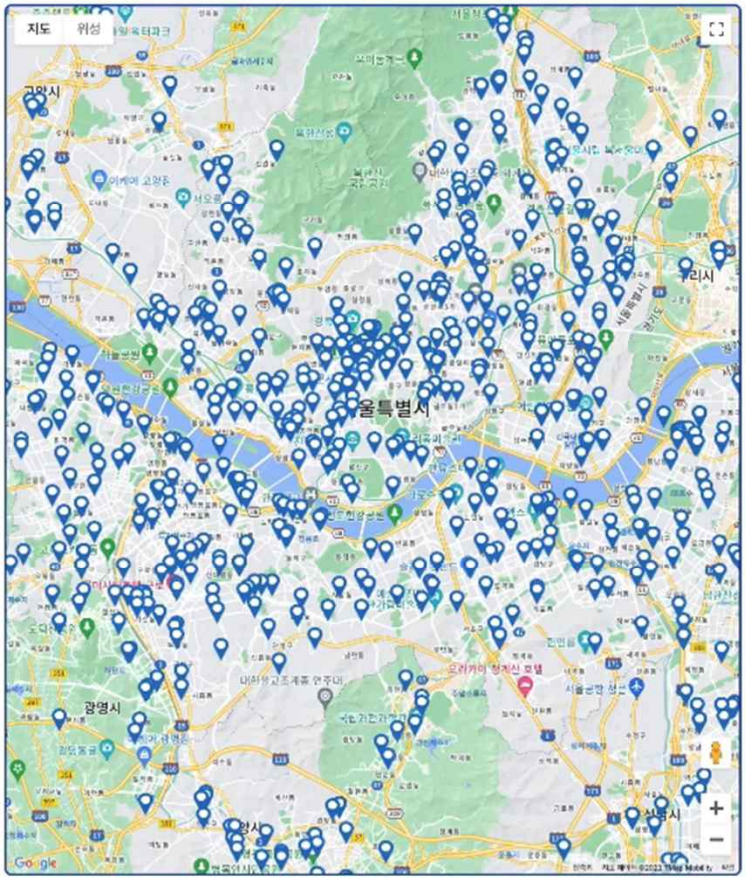
- 개발기간: 2018년 ~현재
- 개발언어: C/C++ (센서), Java (수집서버), Python (백엔드)
- 규모
  - 센서 수: 8,000
  - 백엔드 서버 수: 5대
  - 컨테이너 수: 상시 45개, On-demand 35개
    - 지진 감지 및 경보 관련 45개
    - 지진 데이터 사후 분석용 35개
  - 코드: 248개의 파이썬 파일, 16,316 LoC
    - 센서와 수집서버는 SKT 및 외주 개발
    - 백엔드는 학부~대학원생 위주의 개발



admin 님, 환영합니다. LogOut

전국 센서 현황 대시보드 과거 지진 사례 센서 현황 관리 EMS 관리

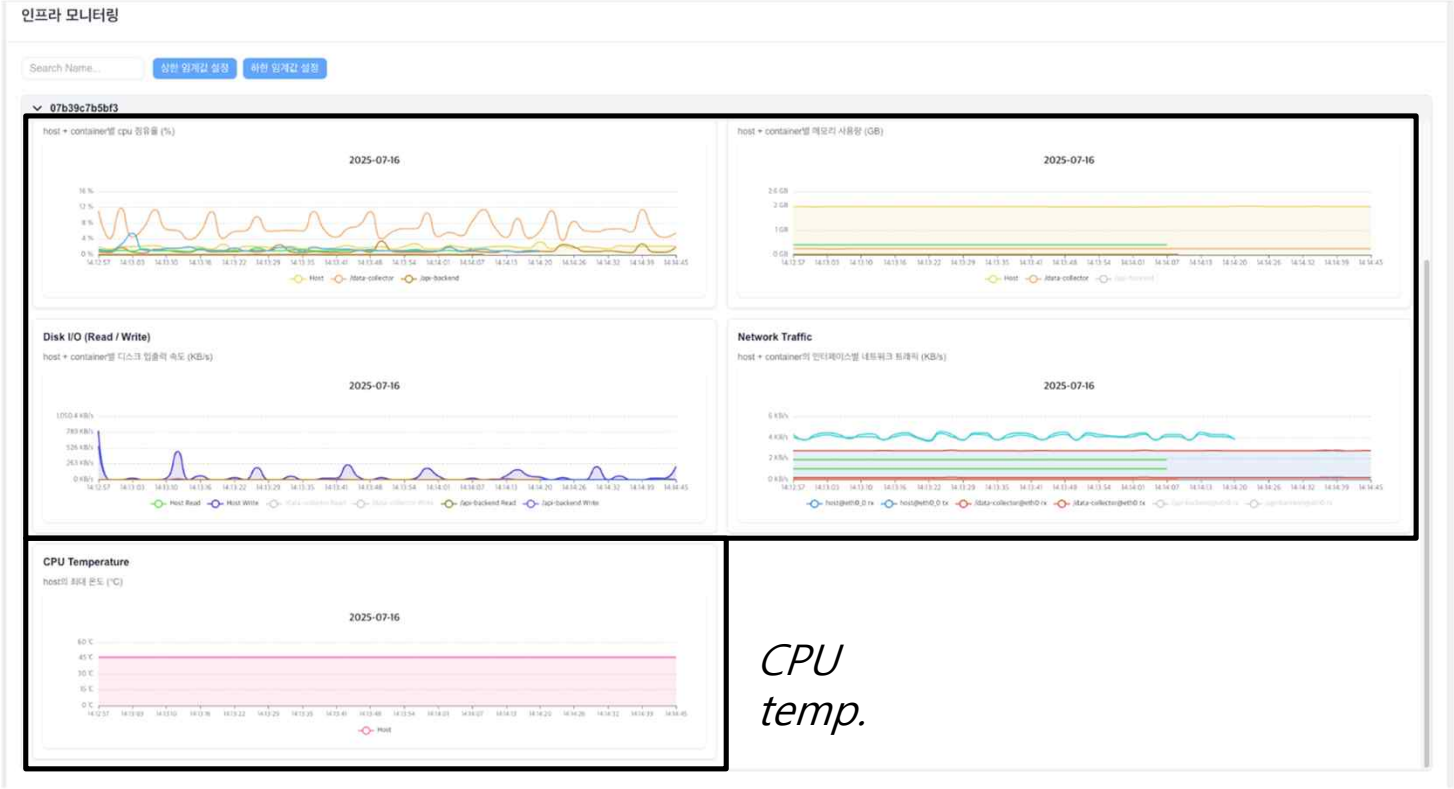
대시보드



KNU KYUNGPOOK NATIONAL UNIVERSITY

CrowdQuake 모니터링 및 로그 수집

- 시스템 모니터링
  - 기기 자원 사용량 추적 (CPU, Memory, Disk, Network I/O) 및 CPU 온도 확인
  - 서버 내 실행중인 작업자(Container)에 대한 자원 사용량 추적



Resource Usages

CPU temp.

CrowdQuake 모니터링 및 로그 수집

- 메트릭 기반 이상징후 탐지
  - 서버/컨테이너 종료, 재실행 등에 대한 알림 기능

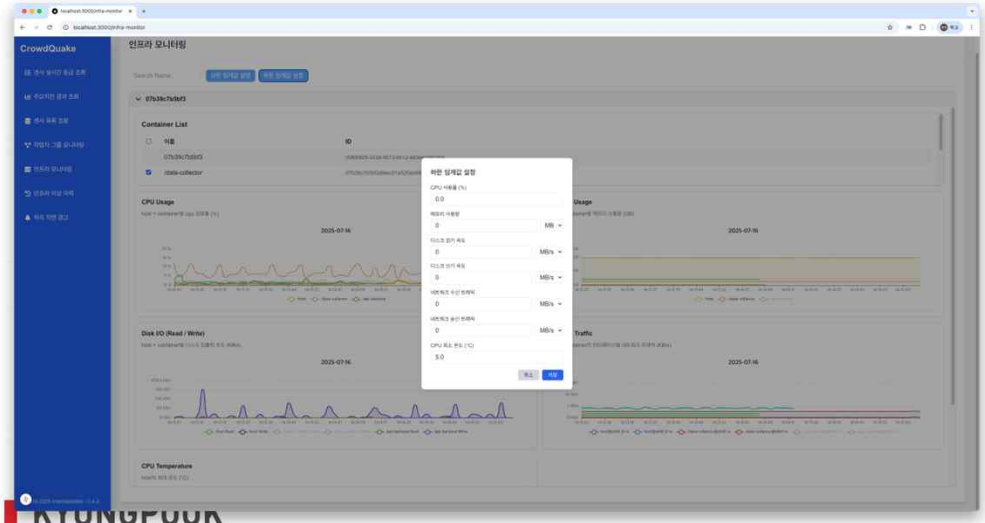
특정 작업자 미응답으로 인한 경보 이력

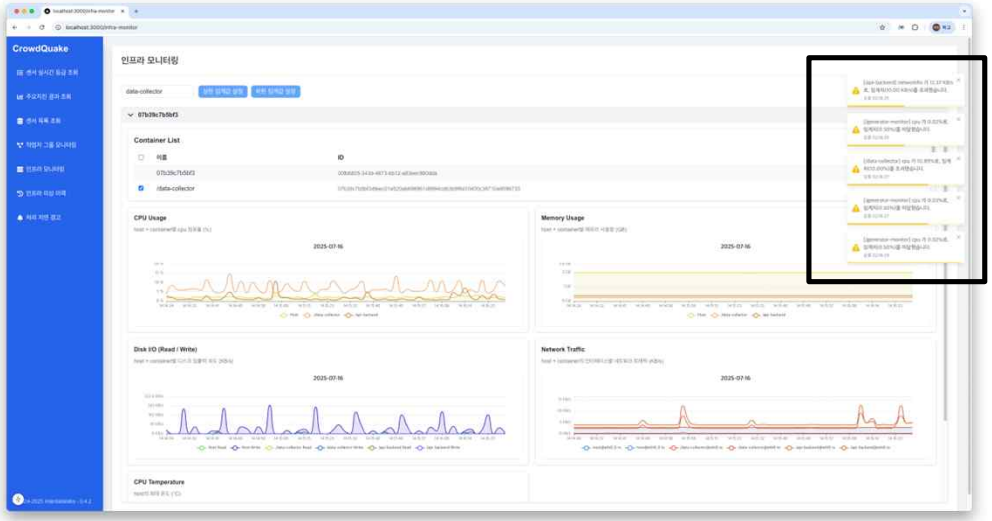
인프라 이상 이력

마지막 업데이트: 2025. 7. 16. 오후 2:12:07

발생 시각	머신 유형	Host 이름	머신 이름	ID	발생 원인	항목	임계값	실제값
2025. 7. 16. 오후 2:11:53	container	07b39c7b5bf3	/generator-monitor	354834079ab3fb1f28bb632080c90202d6...	연결 끊김	-	-	-
2025. 7. 16. 오후 2:10:14	container	07b39c7b5bf3	/generator-monitor	354834079ab3fb1f28bb632080c90202d6...	재연결	-	-	-
2025. 7. 16. 오후 2:10:11	container	07b39c7b5bf3	/generator-monitor	354834079ab3fb1f28bb632080c90202d6...	임계값 미달	diskWriteDelta	0	-569344
2025. 7. 16. 오후 2:09:50	container	07b39c7b5bf3	/consumer	b267b9538bb1c6057349d7c879bfacd3fca...	임계값 초과	cpu	1	2.5612979817965966
2025. 7. 16. 오후 2:09:50	container	07b39c7b5bf3	/mysql-db	7e42cff71a1acfeb5814255c0d96557f55c3...	임계값 초과	cpu	1	1.4774912891986063

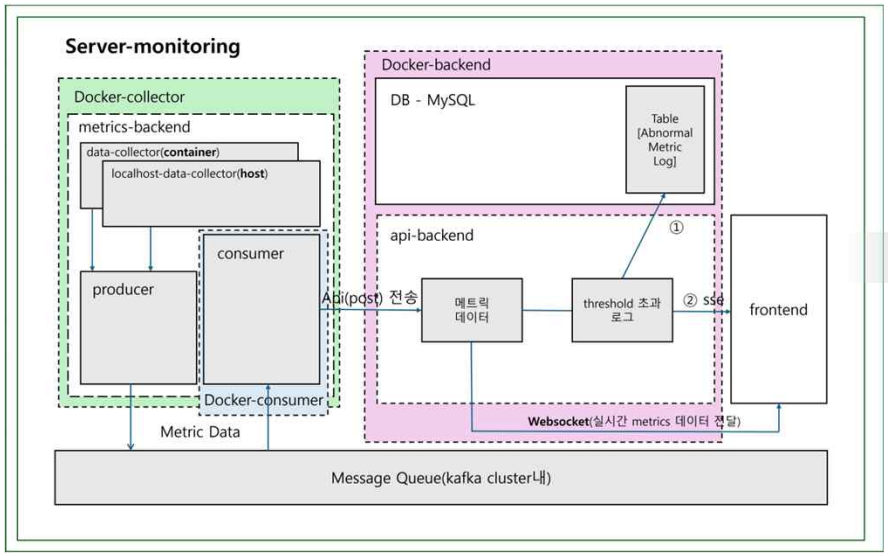
  - 자원 사용에 대한 이상징후 발생 시 알림 기능

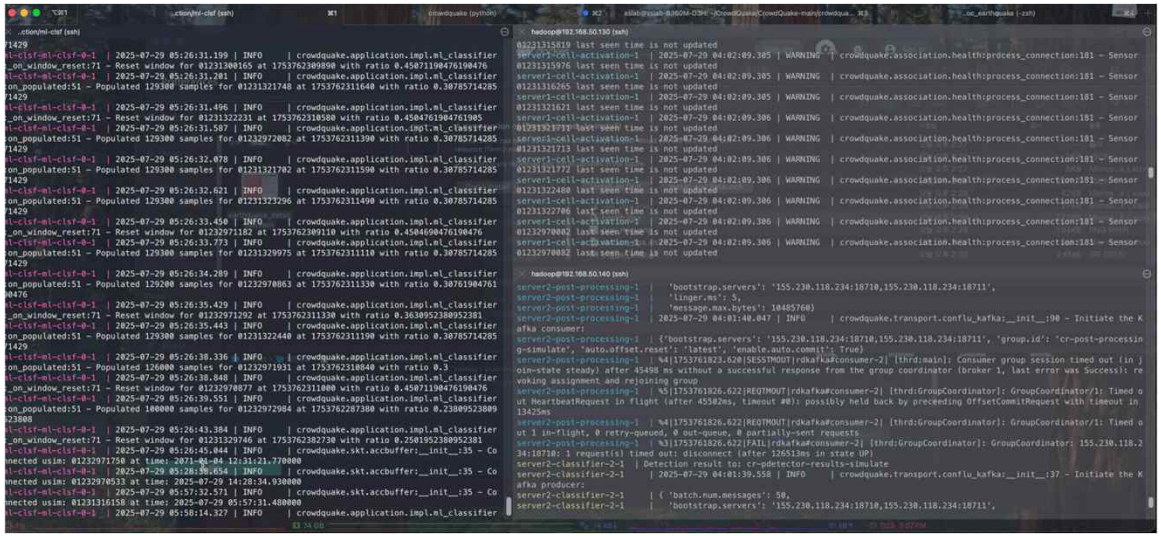




CrowdQuake 모니터링 및 로그 수집

- 로그 수집 대상 및 종류
  - 대상: CrowdQuake 백엔드 시스템
  - 종류
    - 응용프로그램 로그, 도커 컨테이너 로그, 프레임워크 (Kafka) 및 인프라 (DB, HDFS) 로그, OS 로그 등





시스템 이상징후 탐지 (산학협력 연구)

❖ 말레이시아 홍수 모니터링 시스템을 운영하며 자동화 운영 지원 시스템의 필요성 체감
컨테이너에서 발생하는 로그를 실시간으로 분석하기 어려움
스파이크성 트래픽의 Auto-scaling 대응력이 부족함

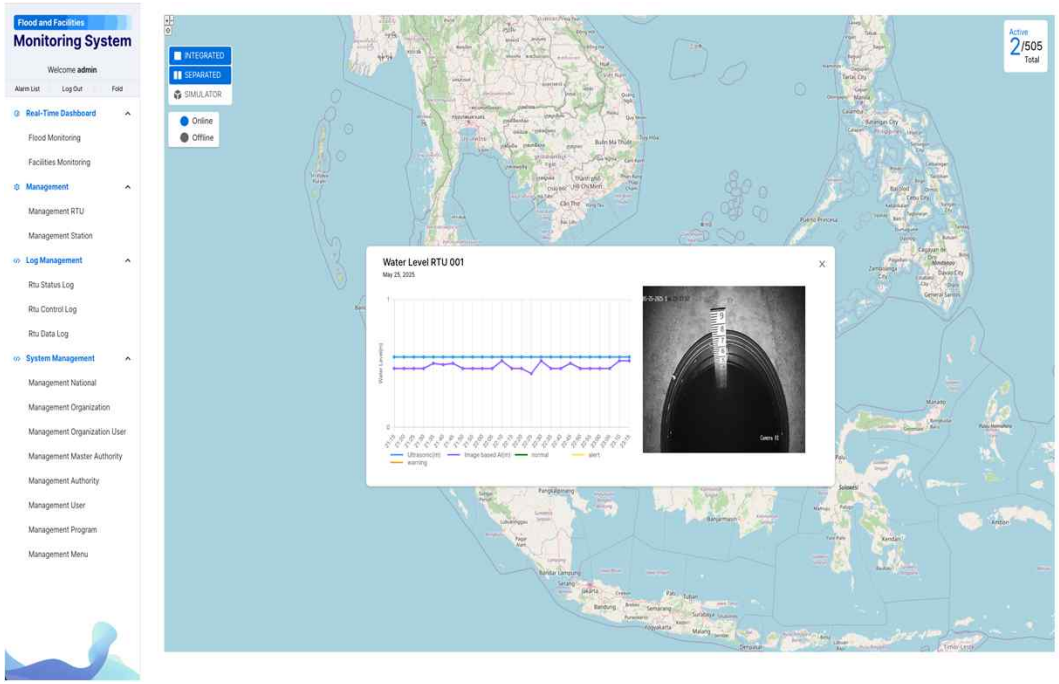


그림 –Flood and Facility Monitoring System화면

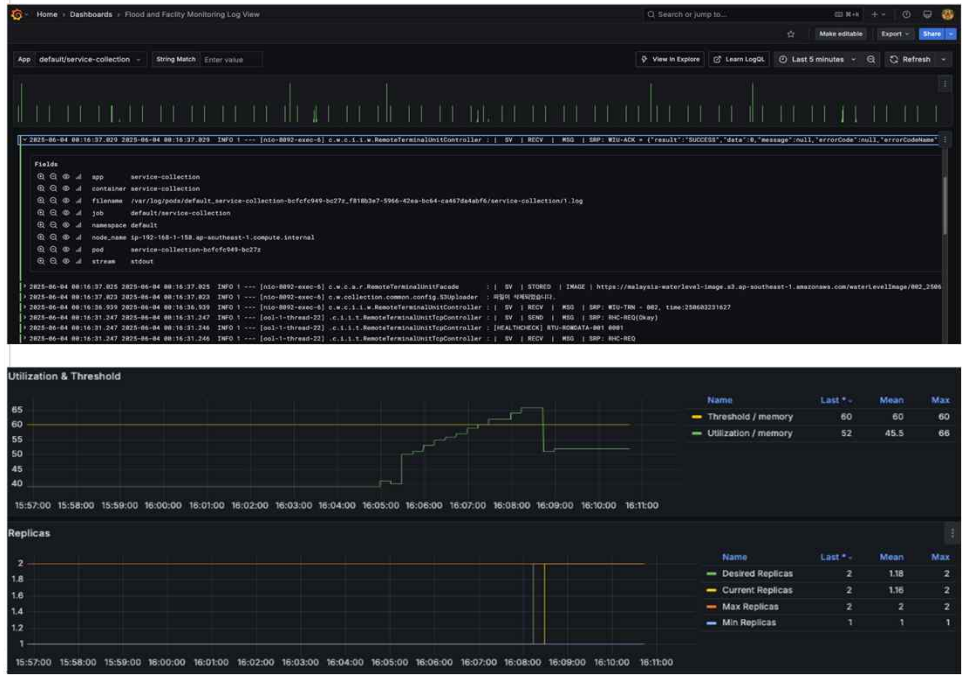


그림 – 홍수 모니터링 시스템 모니터링 도구

시스템 이상징후 탐지 (산학협력 연구)

WINITECH (주)위니텍

❖ 세 가지 기능을 조합하여 컨테이너 오케스트레이션 환경을 지원 하는 시스템 제안

1. 로그 분석을 통한 이상감지: 정적 프롬프트 + 실시간 로그 → sLLM(로컬) → 재실행/스케일아웃/유지 판단

2. 매트릭 예측을 통한 이상감지: 실시간 매트릭 → 학습된 Informer 모델(로컬) → 스케일아웃 여부 판단

3. 적정 리소스 산정 기법: 재실행 및 스케일 아웃시 필요한 컨테이너 적정 리소스 제공

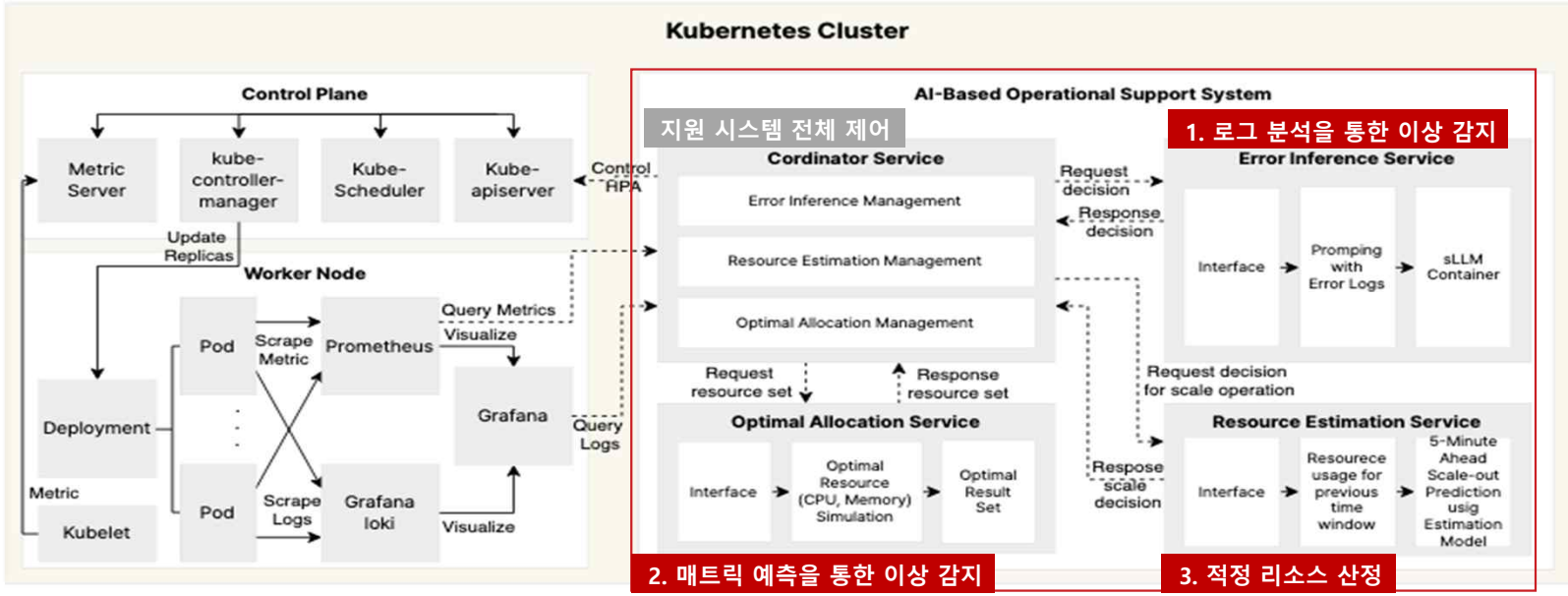


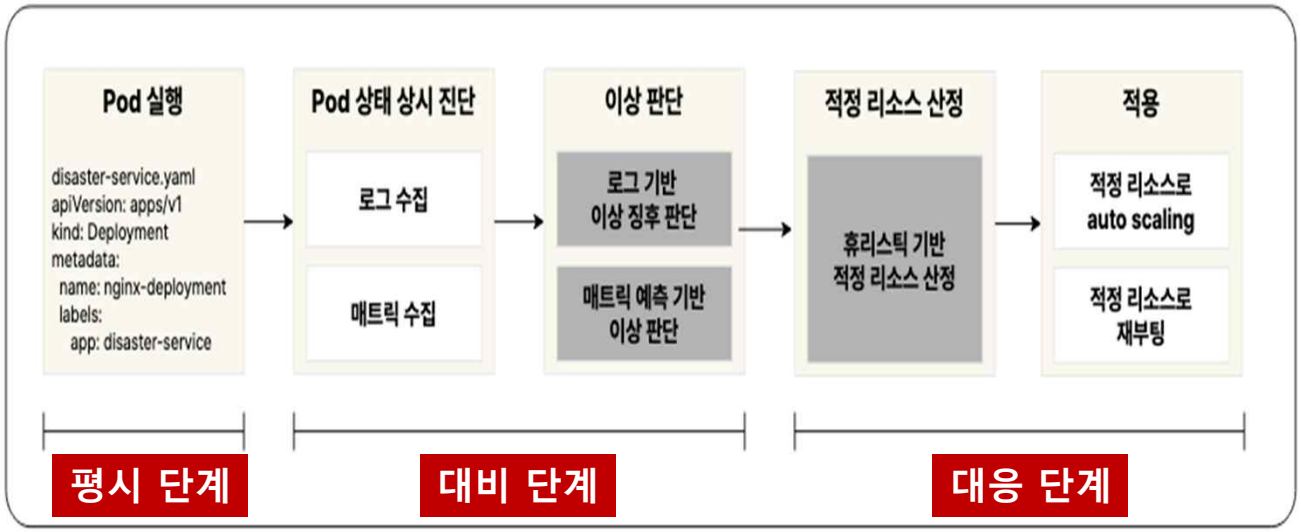
그림 – 제안 시스템 아키텍처

시스템 이상징후 탐지 (산학협력 연구)

WINITECH (주)위니텍

❖ 세 가지 기능을 조합하여 컨테이너 오케스트레이션 환경을 지원 하는 시스템 제안

1. **로그 분석을 통한 이상감지:** 정적 프롬프트 + 실시간 로그 → sLLM(로컬) → 재실행/스케일아웃/유지 판단
2. **매트릭 예측을 통한 이상감지:** 실시간 매트릭 → 학습된 Informer 모델(로컬) → 스케일아웃 여부 판단
3. **적정 리소스 산정 기법:** 재실행 및 스케일 아웃시 필요한 컨테이너 적정 리소스 제공



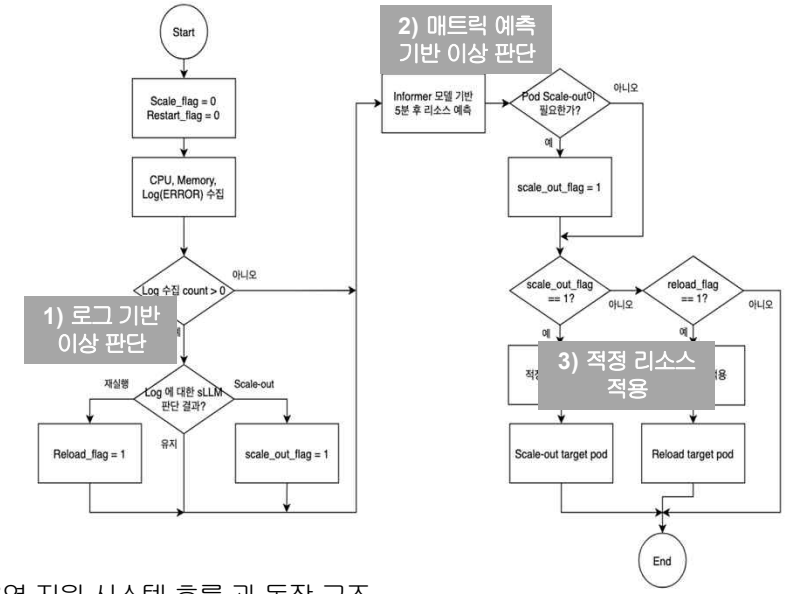


그림 – Cloud-Native 환경을 위한 AI 기반 이상상황 대응 및 자원 예측 운영 지원 시스템 흐름 과 동작 구조

시스템 이상징후 탐지 (산학협력 연구)

WINITECH (주)위니텍

- ❖ 운영 환경에서 수집한 로그 데이터를 기반으로 실험 데이터 셋 구축
- ❖ sLLM(Gemma 3) 모델을 이용하여 프롬프팅 기법을 통해 Pod 재시작 / Scale-out / 유지 판단

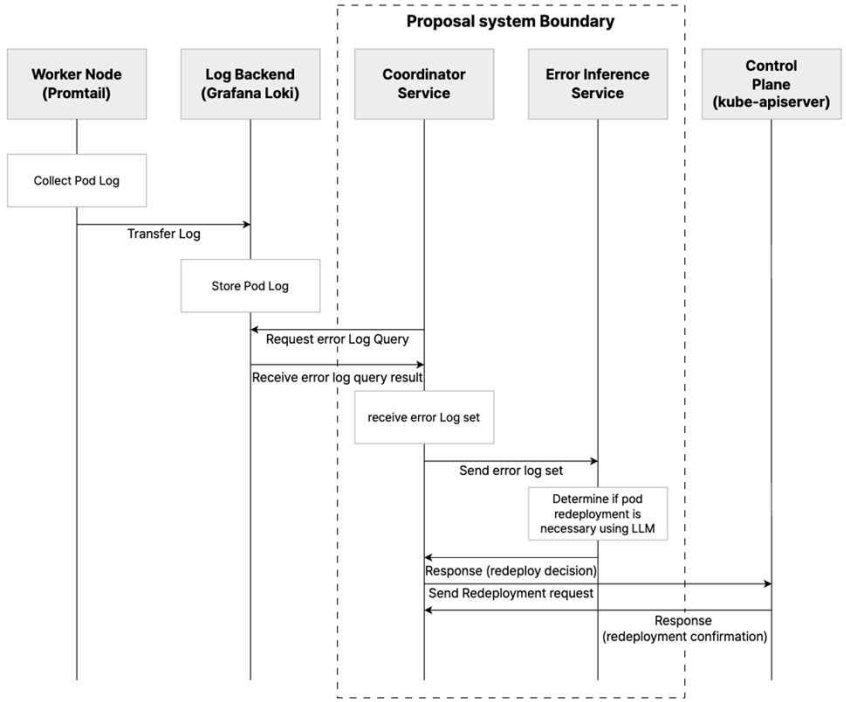


그림 – 에러 로그 탐지 절차

프롬프트 (지시)

당신은 Java Spring Boot 기반 컨테이너 로그를 분석하여 운영 정책에 따라 적절한 조치를 판단하는 시스템입니다.

[로그 메시지]

${log} // 운영환경 최근 1분 로그 데이터삽입

다음 기준에 따라 판단하세요:

- OutOfMemoryError, GC Overhead Limit → 재시작 필요
- Connection refused, SocketTimeoutException → 재시작 또는 점검 필요
- Too many open files, Unable to create native thread → 스케일링 필요
- Database connection pool exhausted, JDBC Connection is closed → 재시작 권장
- Thread deadlock detected → 재시작 또는 스레드 풀 초기화 필요

아래와 같은 형식으로 결과를 출력하세요:
{"action": "restart" | "scale" | "ignore", "reason": "설명 요약" }

sLLM(Gemma3)

출력

{"action": “restart”, “reason”: “GC overhead는 가비지 컬렉션이 과도하게 실행되고 있음을 나타냅니다. 이는 시스템 성능 저하의 원인이 될 수 있으며, 특히 메모리 부족 상황에서 더욱 심각해질 수 있습니다. 즉시 애플리케이션을 재시작하여 가비지 컬렉션을 초기화하고 잠재적인 문제를 해결하는 것이 좋습니다."}

그림 – 로그 분석 기반 이상 판단 예시

시스템 이상징후 탐지 (산학협력 연구)

WINITECH (주)위니텍

- **Informer** 모델 기반 매트릭 예측으로 이상 판단
- 사후 대응: Kubernetes HPA, VPA < 사전 예방: 예측 기반 **Scale- out**
- **"Informer: Beyond Efficient Transformer for Long Sequence Time- Series Forecasting (AAAI'21 Best Paper)"** 의 하이퍼 파라메터 수정 및 다변량 입력 다변량 출력 구조 → 다변량 입력 단변량 출력(Scale-out 필요 여부) 변경

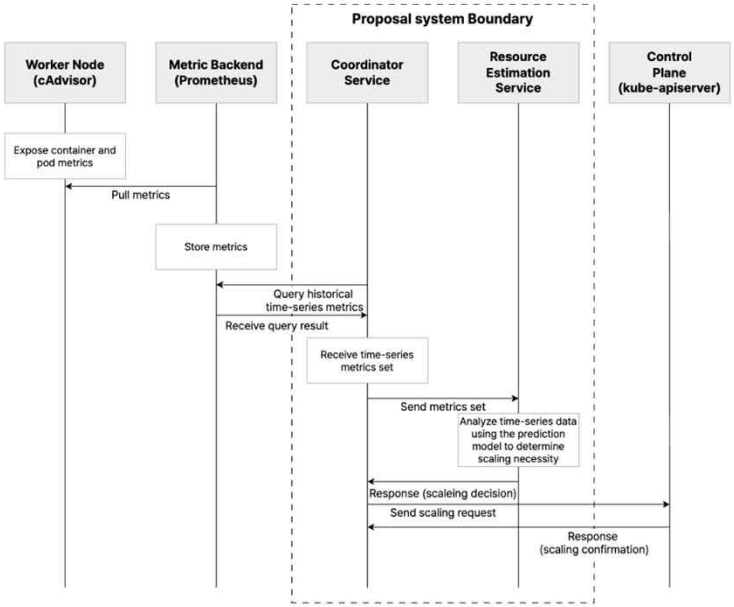


그림 – 리소스 예측 절차

학습 데이터

```
date,cpu_usage,memory_usage, scale
2025-03-11T08:54:39.000Z,1.032,39.612, 0
2025-03-11T08:54:44.000Z,0.976,39.616, 0
…
2025-03-11T09:15:09.000Z,22.334,74.624,1
2025-03-11T09:15:14.000Z,23.132,75.001,1
```

시퀀스 전달 (5초간격 20분)

```
date,cpu_usage,memory_usage
2025-05-18T08:54:39.000Z,,39.612
2025-05-18T08:54:44.000Z,0.976,39.616
2025-05-18T08:54:49.000Z,,39.616
2025-05-18T08:54:54.000Z,,39.616
…
2025-05-18T09:15:09.000Z,,39.624
2025-05-18T09:15:14.000Z,0.491,39.626
```

단변량 출력으로 튜닝 후 모델 사전 학습

다변량 입력

Informer Model

단변량 출력

Scale- out

or

유지

그림 – Informer 기반 매트릭 예측 흐름

시스템 이상징후 탐지 (산학협력 연구) WINITECH (주)위니텍

- ❖ Flood and Facility Monitoring System(Malaysia, 2025) 운영환경에서 검증
- ❖ K6 시뮬레이터를 이용하여 **5분** 동안 **단일 컨테이너**에 **초당 400건**의 Http Request 부하 유발
- ❖ HPA 기준 scale-out 동작 속도 **1분 45초** 절감, 통신 실패율 **6%** 감소 → **안정성 증가, Cold Start** 문제 해결

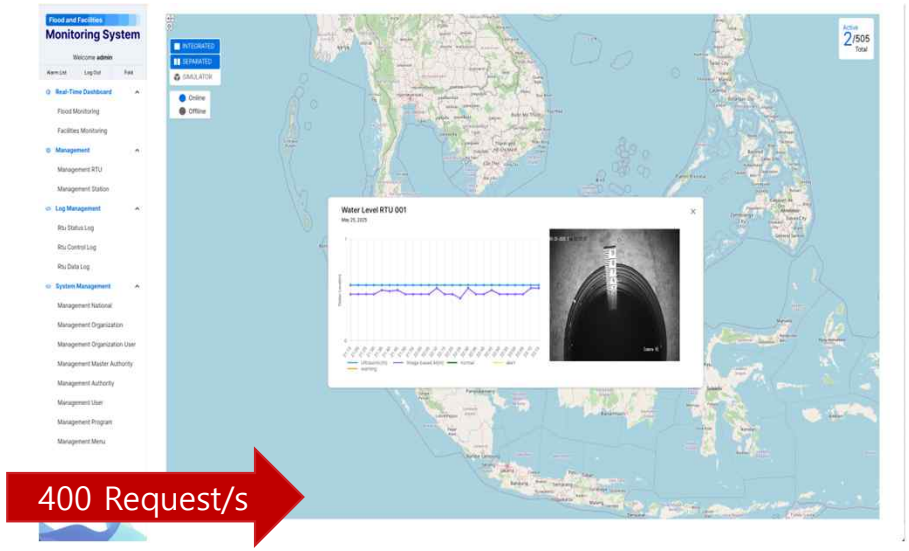


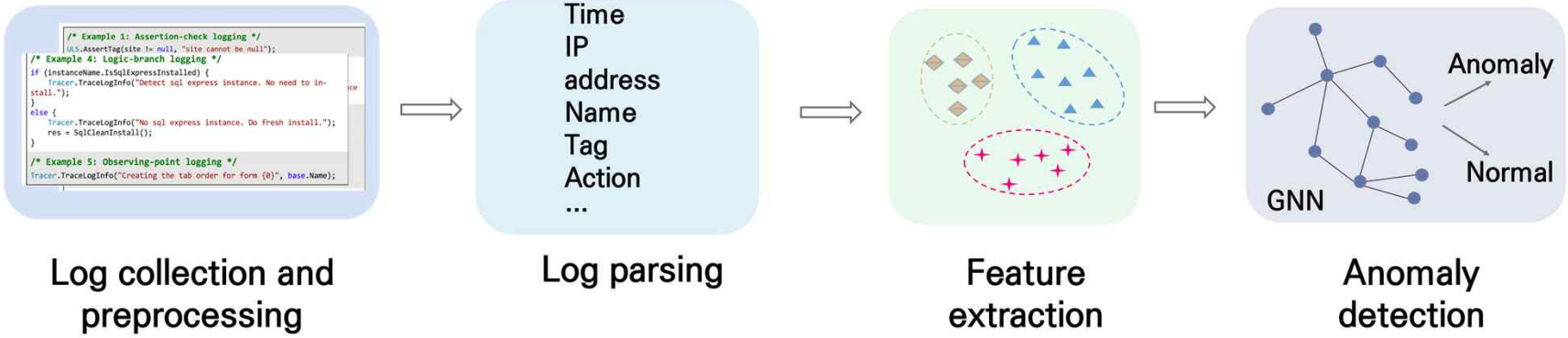
그림 – 검증 시스템(Flood and Facility Monitoring System) 화면

Kubernetes 기본 HPA Scale-out 결과
통신 실패율 : **6%**

이상 예측을 통한 사전대응 후 안정성 향상
통신 실패율 : **0%**

로그 기반 이상징후 탐지 (기존, ~ 2024)

- 개요



- 로그 데이터의 그래프화

Figure 2: The example of raw log parsing and graph construction.

로그 기반 이상징후 탐지 (기존, ~ 2024)

Message	Level	EventID	Event Template
org.apache.hadoop.hdfs.server.namenode.NameNode: registered UNIX signal handlers for [TERM, HUP, INT]	Info	-1	
org.apache.hadoop.hdfs.server.namenode.NameNode: createNameNode []	Info	51	INFO org.apache.hadoop.hdfs.server.namenode.NameNode: createNameNode .*
org.apache.hadoop.hdfs.server.namenode.FSNamesystem: Only one namespace edits storage directory (dfs.namenode.edits.dir) configured. Beware of data loss due to lack of redundant storage	Warn	503	org.apache.hadoop.hdfs.server.namenode.FSNamesystem: Only one namespace edits storage directory \(dfs.namenode.edits.dir\) configured. Beware of data loss due to lack of redundant storage directories!
org.apache.hadoop.metrics2.impl.MetricsSystemImpl: NameNode metrics system started	Info	22	org.apache.hadoop.metrics2.impl.MetricsSystemImpl: .* metrics system started
org.apache.hadoop.metrics2.impl.MetricsSystemImpl: Scheduled Metric snapshot period at 10 second(s).	Info	512	org.apache.hadoop.metrics2.impl.MetricsSystemImpl: Scheduled Metric snapshot period at .* second\(s\).
org.apache.hadoop.hdfs.server.namenode.NameNode: Clients should use master:9000 to access this namenode/service.	Info	507	org.apache.hadoop.hdfs.server.namenode.NameNode: Clients should use master:.* to access this namenode/service.
org.apache.hadoop.hdfs.server.datanode.fsdataset.impl.FsDatasetImpl: dfsUsed file missing in /data/tmp/dfs/data/current/BP-1344050560-172.20.1.34-1708985604616/current, will proceed with	Warn	31	org.apache.hadoop.hdfs.server.datanode.fsdataset.impl.FsDatasetImpl: dfsUsed file missing in .* will proceed with Du for space computation calculation,
org.apache.hadoop.hdfs.server.datanode.fsdataset.impl.FsDatasetImpl: dfsUsed file missing in /data/tmp/dfs/data/current/BP-1344050560-172.20.1.34-1708985604616/current, will proceed with	Warn	31	org.apache.hadoop.hdfs.server.datanode.fsdataset.impl.FsDatasetImpl: dfsUsed file missing in .* will proceed with Du for space computation calculation,
org.apache.hadoop.hdfs.DFSUtil: Filter initializers set : org.apache.hadoop.http.lib.StaticUserWebFilter,org.apache.hadoop.hdfs.web.AuthFilterInitializer	Info	27	org.apache.hadoop.hdfs.DFSUtil: Filter initializers set : org.apache.hadoop.http.lib.StaticUserWebFilter,org.apache.hadoop.hdfs.web.AuthFilterInitializer
org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: dfs.datanode.directoryscan.throttle.limit.ms.per.sec set to value above 1000 ms/sec. Assuming	Info	46	org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: dfs.datanode.directoryscan.throttle.limit.ms.per.sec set to value above .* ms/sec. Assuming default value of
org.eclipse.jetty.util.log: Logging initialized @899ms to org.eclipse.jetty.util.log.Slf4jLog	Info	19	org.eclipse.jetty.util.log: Logging initialized .* to org.eclipse.jetty.util.log.Slf4jLog
org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: Periodic Directory Tree Verification scan starting in 1166521ms with interval of 21600000ms and throttle limit of -1ms/s	Info	33	org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: Periodic Directory Tree Verification scan starting in .* with interval of .* and throttle limit of .*
org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: dfs.datanode.directoryscan.throttle.limit.ms.per.sec set to value above 1000 ms/sec. Assuming	Warn	401	org.apache.hadoop.hdfs.server.datanode.DirectoryScanner: dfs.datanode.directoryscan.throttle.limit.ms.per.sec set to value above .* ms/sec. Assuming default value of
org.apache.hadoop.http.HttpServer2: Added global filter 'safety' (class=org.apache.hadoop.http.HttpServer2$QuotingInputFilter)	Info	26	org.apache.hadoop.http.HttpServer2: .* global filter 'safety' \(class=.*\)
org.apache.hadoop.http.HttpServer2: Added filter static_user_filter (class=org.apache.hadoop.http.lib.StaticUserWebFilter$StaticUserFilter) to context hdfs	Info	71	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context .*
org.apache.hadoop.http.HttpServer2: Added filter static_user_filter (class=org.apache.hadoop.http.lib.StaticUserWebFilter$StaticUserFilter) to context logs	Info	92	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context logs
org.apache.hadoop.http.HttpServer2: Added filter static_user_filter (class=org.apache.hadoop.http.lib.StaticUserWebFilter$StaticUserFilter) to context static	Info	71	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context .*
org.apache.hadoop.http.HttpServer2: Added filter AuthFilter (class=org.apache.hadoop.hdfs.web.AuthFilter) to context hdfs	Info	71	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context .*
org.apache.hadoop.http.HttpServer2: Added filter AuthFilter (class=org.apache.hadoop.hdfs.web.AuthFilter) to context logs	Info	92	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context logs
org.apache.hadoop.http.HttpServer2: Added filter AuthFilter (class=org.apache.hadoop.hdfs.web.AuthFilter) to context static	Info	71	org.apache.hadoop.http.HttpServer2: .* filter .* \(class=.*\) to context .*

Few-shot Prompt

Prompt: "Here are a few examples of how to classify log sequences. Based on these examples, classify the new log provided.

Examples:

1) Log Sequence: {Example log 1} --> Anomaly Type: {Class 1};

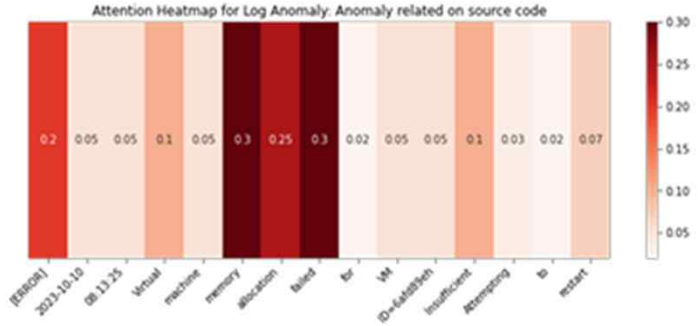
2) Log Sequence: {Example log 2} --> Anomaly Type: {Class 2}.

Input & Output:

Log Sequence: [New log data] --> Anomaly Type: Class 3

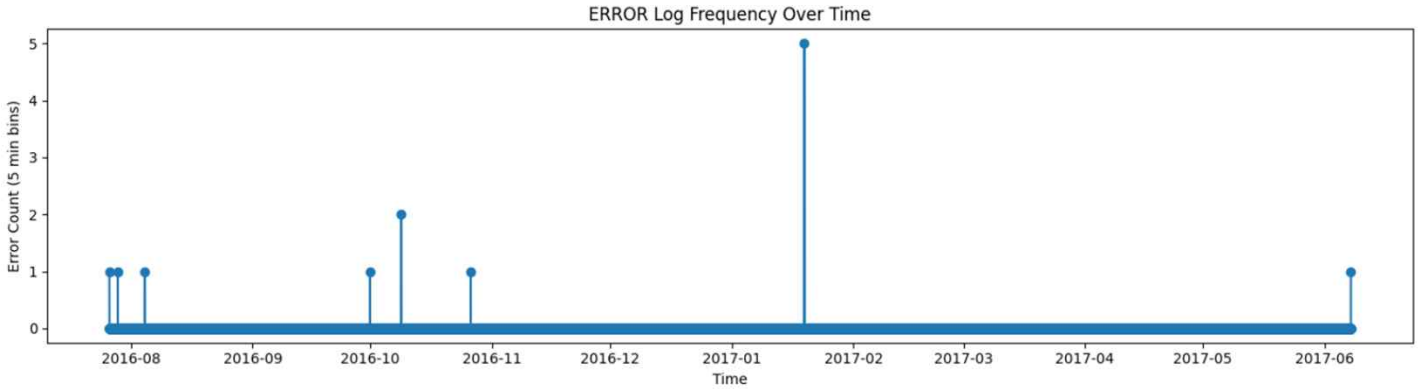
Log Sample (Related source code):

[ERROR] 2023-10-10 08:13:25: Virtual machine memory allocation failed for VM ID=6afd89eh: Insufficient memory. Attempting to restart VM ID=6afd89eh.



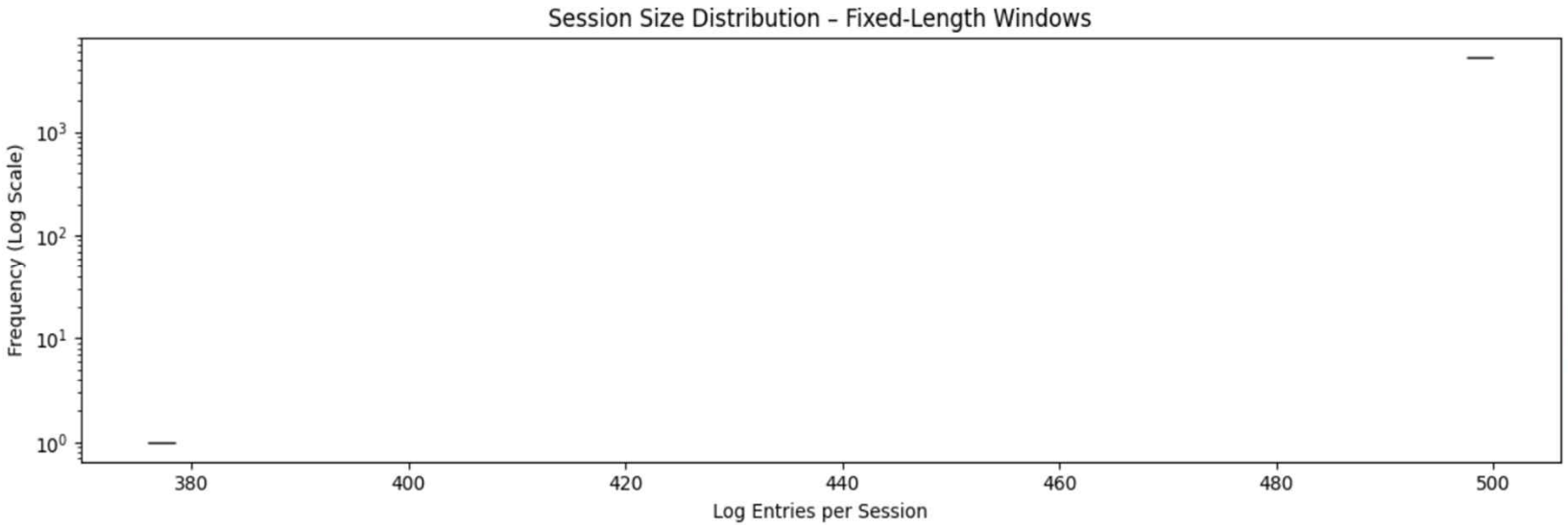
로그 기반 이상징후 탐지

- Visualize how errors or important events occur over time



Grouping for Graph- based Log Analysis

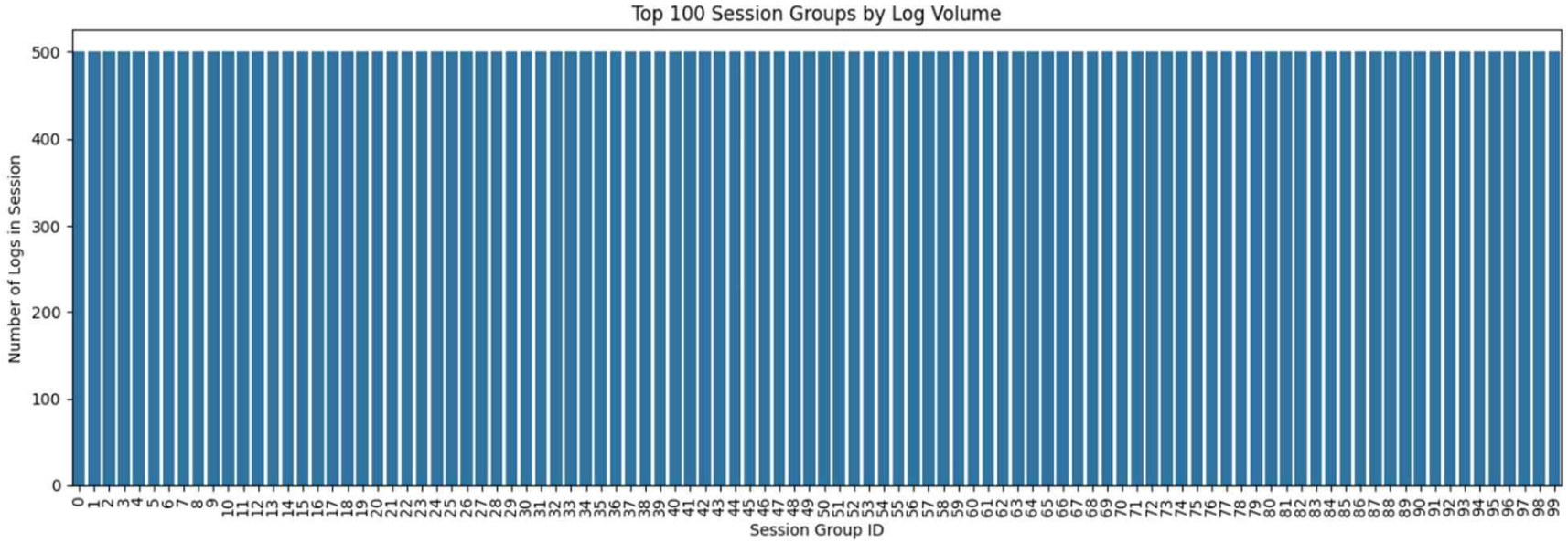
- **Fixed- length Windows**
  - For ML models
  - Consistent size
  - Ignore semantic flow




```
SessionGroup_FixedWindow
0       500
1       500
2       500
3       500
4       500
       ...
5218    500
5219    500
5220    500
5221    500
5222    376
Name: count, Length: 5223, dtype: int64
```

Grouping for Graph- based Log Analysis

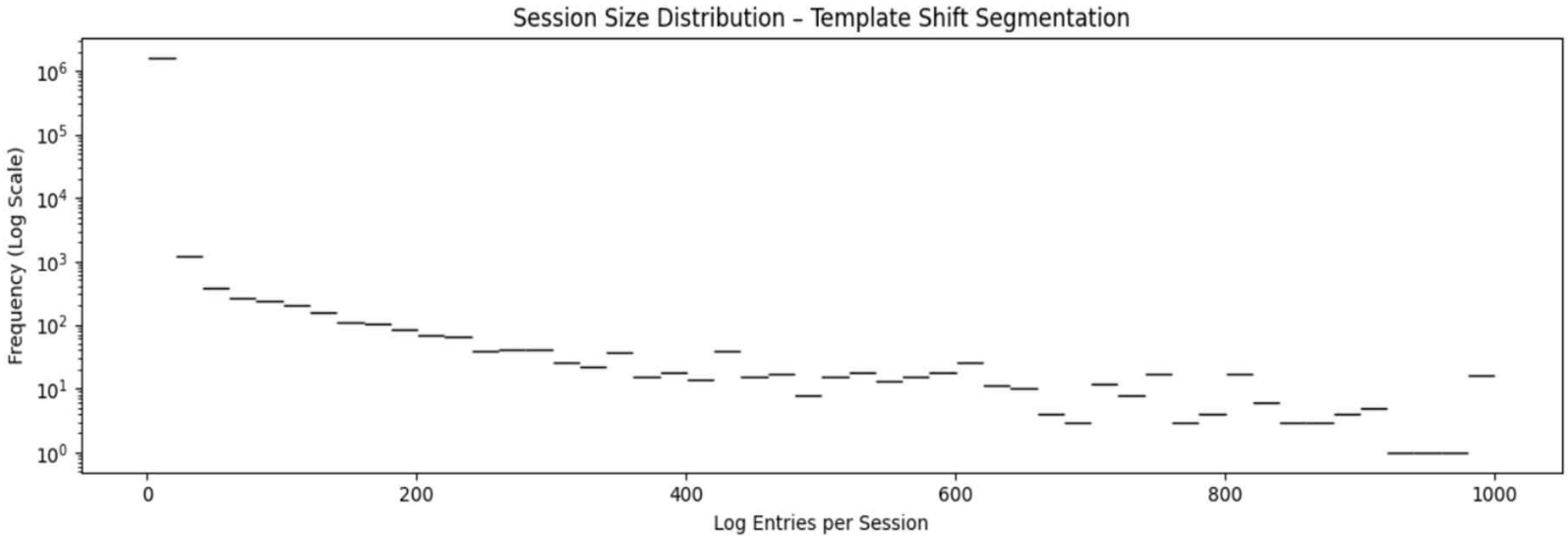
- **Fixed- length Windows**
  - For ML models
  - Consistent size
  - Ignore semantic flow



count	5223.000000
mean	499.976259
std	1.715780
min	376.000000
25%	500.000000
50%	500.000000
75%	500.000000
max	500.000000

Grouping for Graph- based Log Analysis

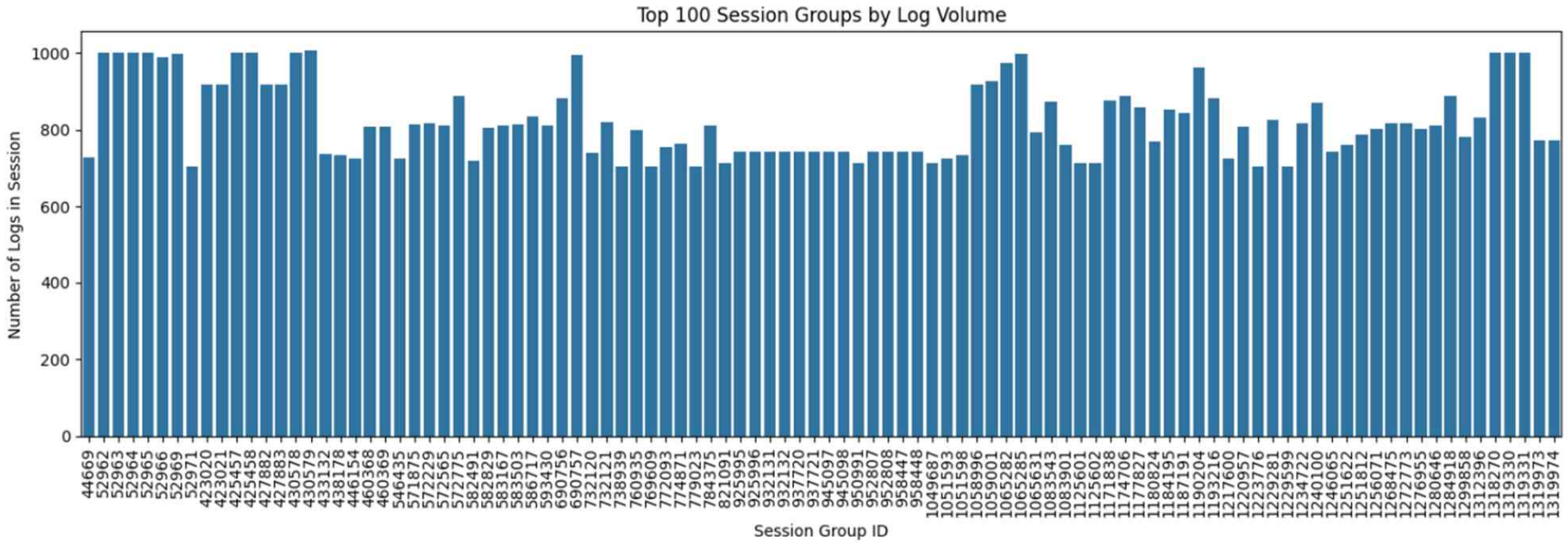
- **Template Shift Segments**
  - When template changes mark logical steps
  - Highlight state changes
  - May miss long-range dependencies




```
SessionGroup_TemplateShift
53510      1000
53513      1000
1349191    1000
53512      1000
438900     1000
           ...
25            1
26            1
27            1
28            1
1579101       1
Name: count, Length: 1579117, dtype: int64
```

Grouping for Graph- based Log Analysis

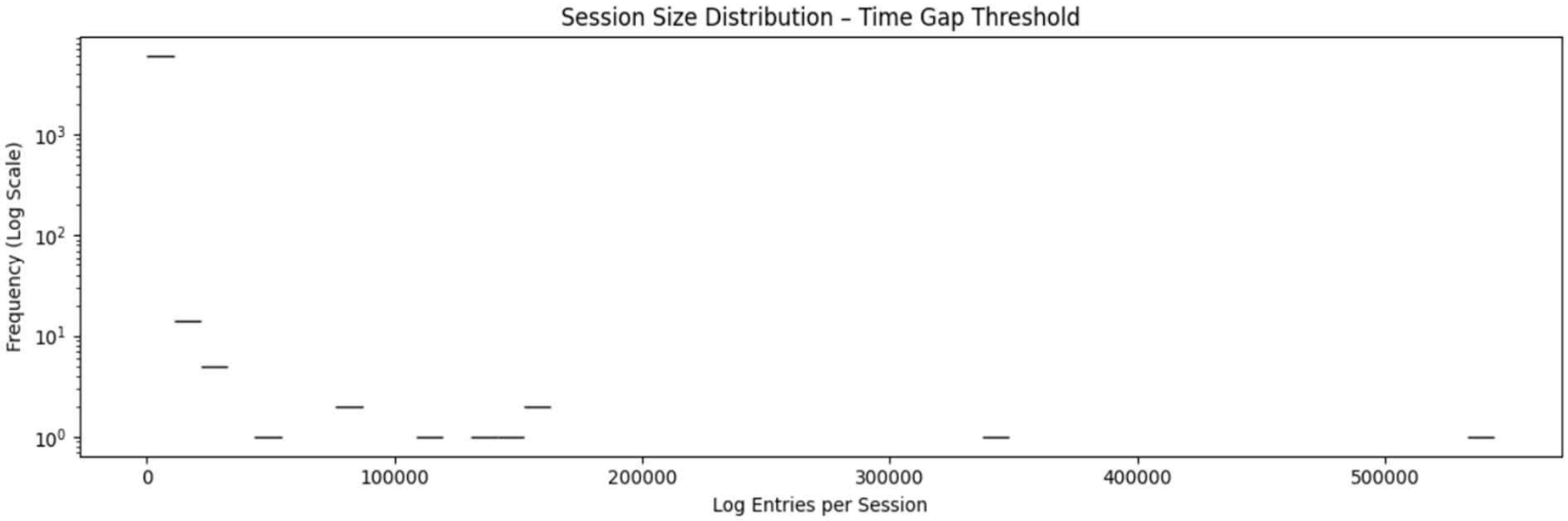
- **Template Shift Segments**
  - When template changes mark logical steps
  - Highlight state changes
  - May miss long-range dependencies



count	1.543917e+06
mean	1.691397e+00
std	1.078215e+01
min	1.000000e+00
25%	1.000000e+00
50%	1.000000e+00
75%	1.000000e+00
max	1.006000e+03

Grouping for Graph- based Log Analysis

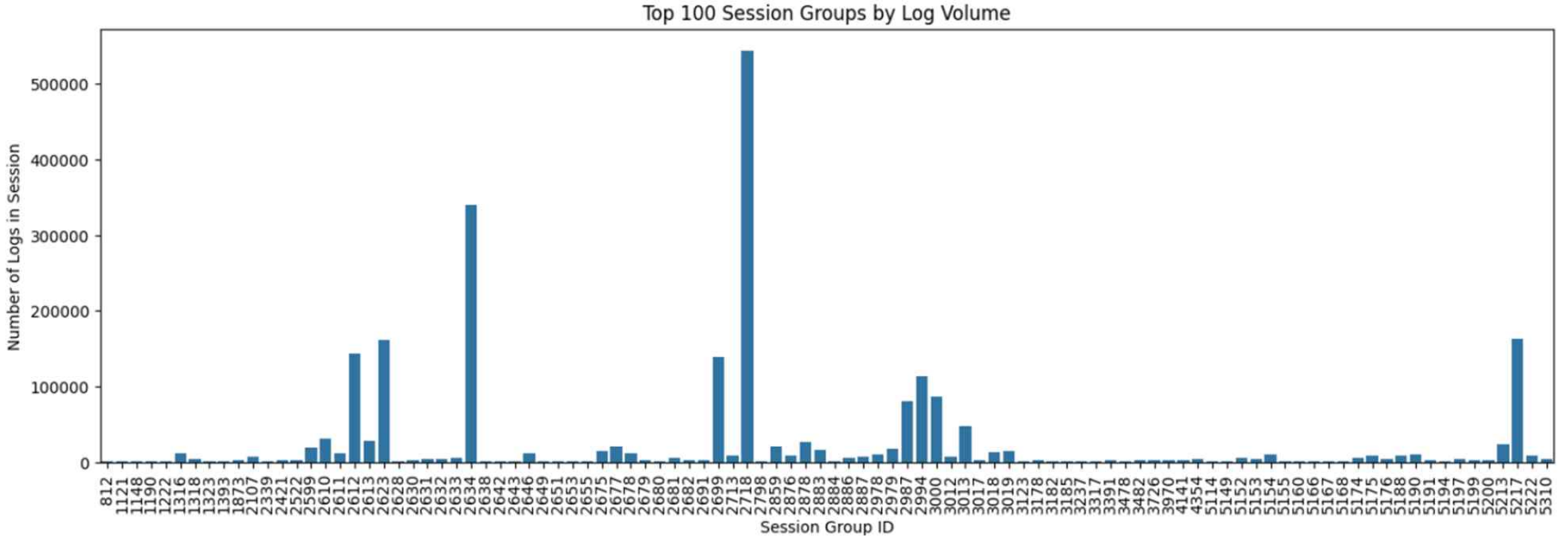
- **Time Gap Thresholds**
  - When sessions are temporally bursty
  - Captures real execution flows and transitions
  - Risk of skewed session sizes




```
SessionGroup_TimeGap
2718    544188
2634    340599
5217    162887
2623    161371
2612    143298
        ...
10           1
8            1
6            1
4            1
2            1
Name: count, Length: 6019, dtype: int64
```

Grouping for Graph- based Log Analysis

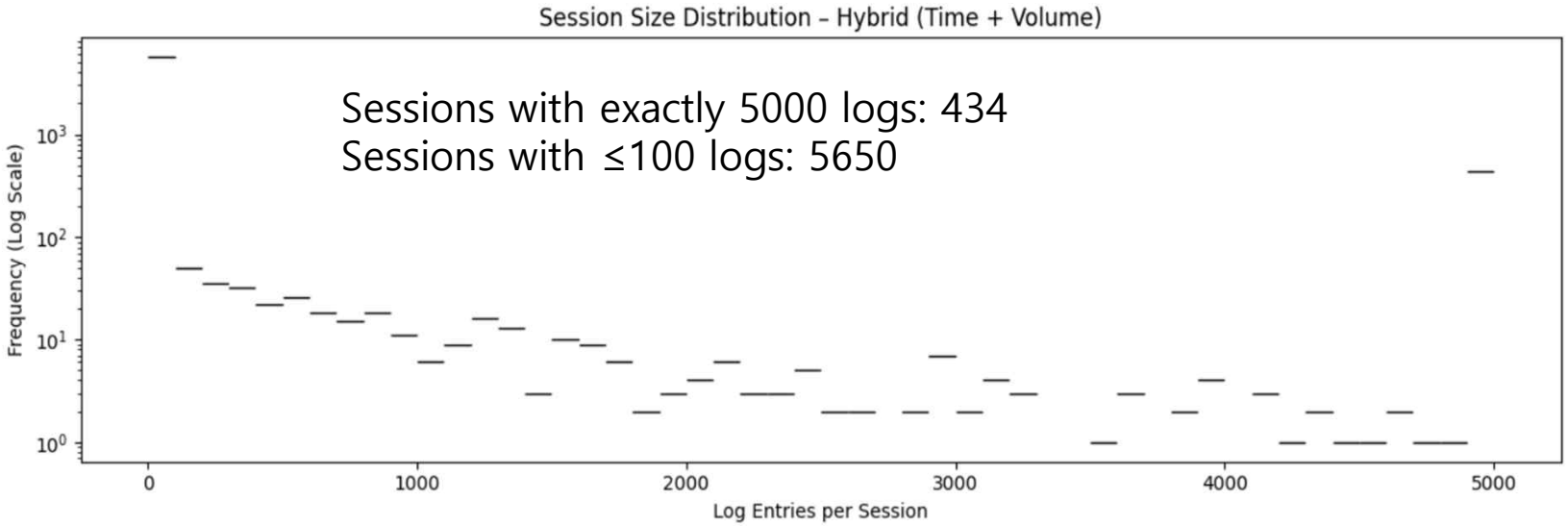
- **Time Gap Thresholds**
  - When sessions are temporally bursty
  - Captures real execution flows and transitions
  - Risk of skewed session sizes



count	6019.000000
mean	433.855458
std	9484.835149
min	1.000000
25%	1.000000
50%	2.000000
75%	2.000000
max	544188.000000

Grouping for Graph- based Log Analysis

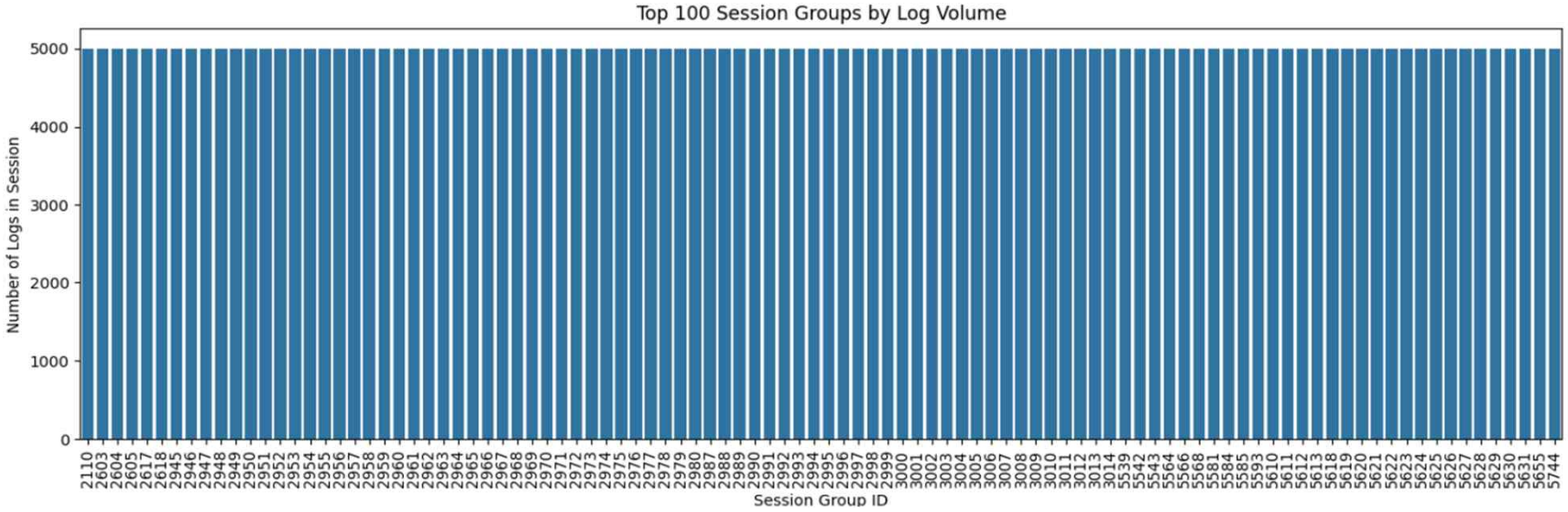
- **Hybrid (Time + Max Events)**
  - Default for production logs
  - Balanced node/edge density across graphs
  - May split actual sessions




```
SessionGroup_Hybrid
5744    5000
5655    5000
2110    5000
2980    5000
2979    5000
        ...
11         1
9          1
7          1
5          1
3          1
Name: count, Length: 6453, dtype: int64
```

Grouping for Graph- based Log Analysis

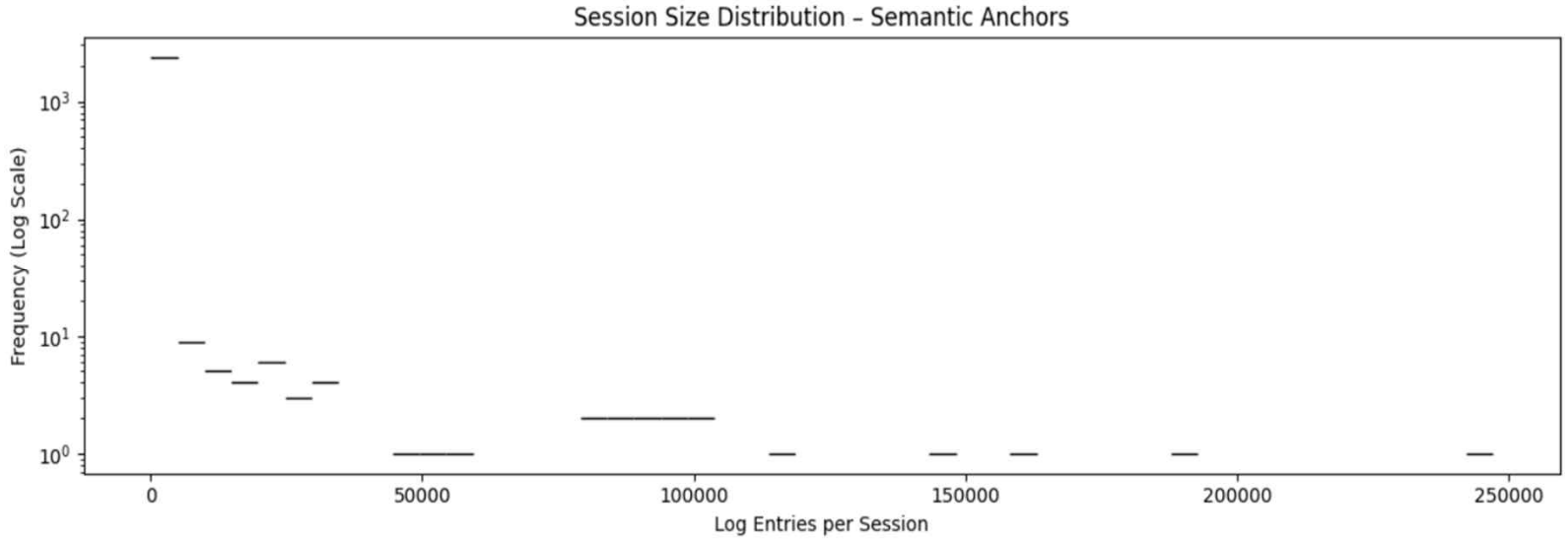
- **Hybrid (Time + Max Events)**
  - Default for production logs
  - Balanced node/edge density across graphs
  - May split actual sessions



count	6453.000000
mean	404.676275
std	1288.688473
min	1.000000
25%	1.000000
50%	2.000000
75%	2.000000
max	5000.000000

Grouping for Graph- based Log Analysis

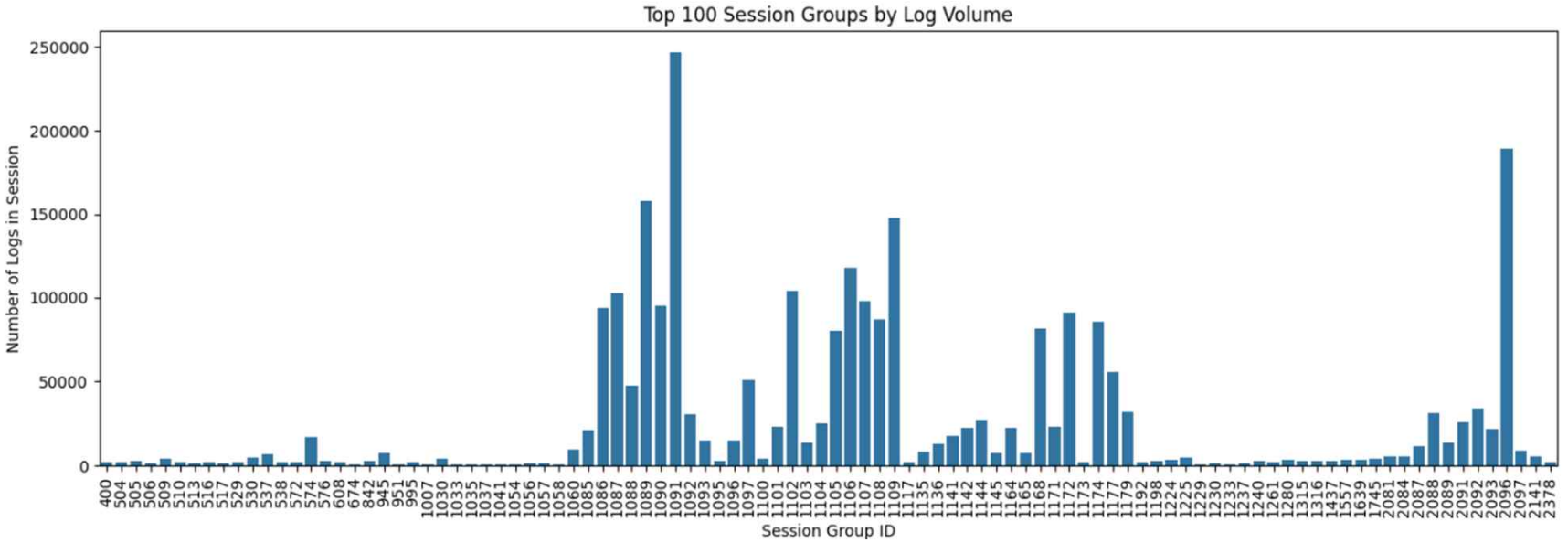
- **Semantic Anchors (e.g. RPC, login)**
  - If known session starters exist
  - Logically pure sessions
  - Needs domain specific templates




```
SessionGroup_Anchors
1091    247178
2096    189094
1089    158339
1109    148120
1106    117776
         ...
2278         1
2279         1
2260         1
2261         1
2343         1
Name: count, Length: 2395, dtype: int64
```

Grouping for Graph- based Log Analysis

- **Semantic Anchors (e.g. RPC, login)**
  - If known session starters exist
  - Logically pure sessions
  - Needs domain specific templates



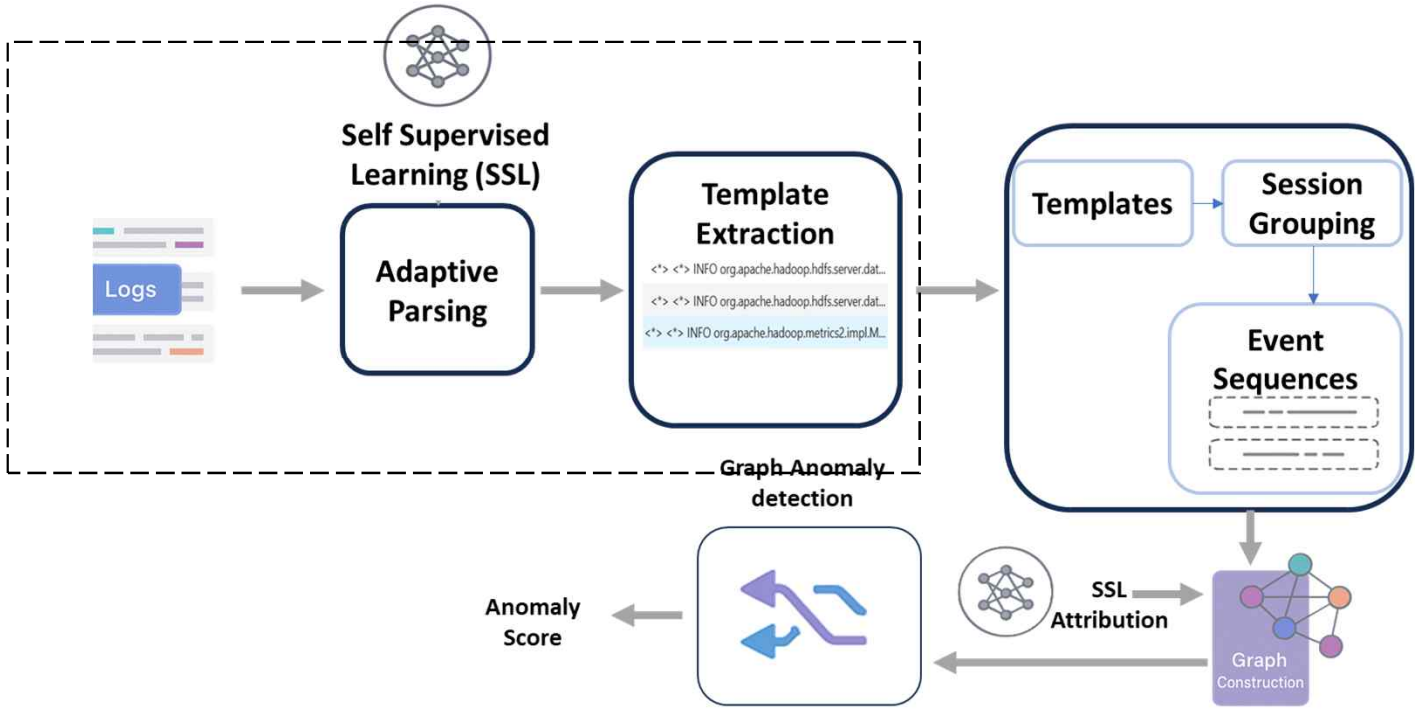
count	2395.000000
mean	1090.344885
std	10409.205436
min	1.000000
25%	3.000000
50%	3.000000
75%	4.000000
max	247178.000000

Summary

- Fixed-length Windows
  - Ensures consistent data shapes
  - Ignores semantic context or flow
- Time Gap Thresholds
  - Captures authentic execution flows and transitions
  - Session sizes may vary wildly
- Hybrid (Time + Max Events)
  - Balances node and edge density in graphs
  - May split real sessions prematurely
- Semantic Anchors
  - Best if you have known session start templates
  - Creates clean, meaningful session boundaries
  - Requires domain-specific anchor templates

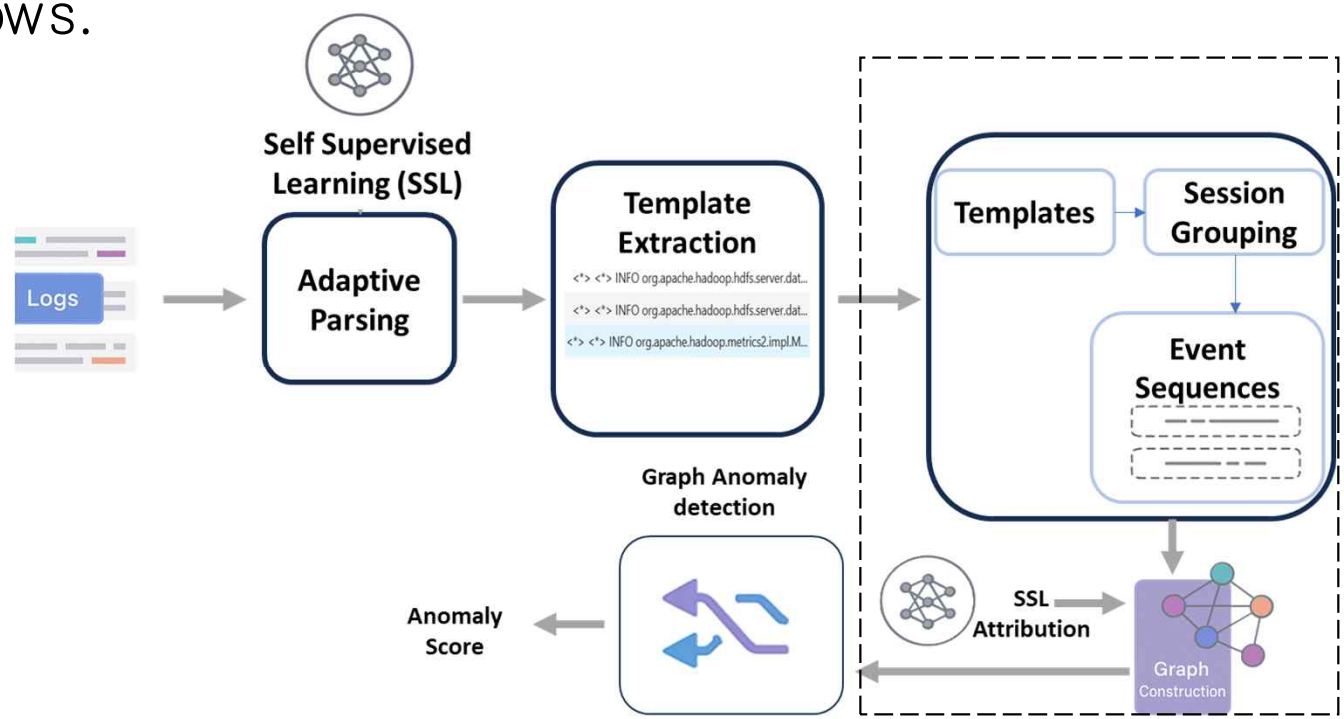
로그 기반 이상징후 탐지

- Semantic-Guided LognRoll Filtering
  - Enhance raw log filtering by integrating semantic understanding using Self-Supervised Learning (SSL)
  - Logs are processed through an SSL model to extract embeddings or semantic clusters.



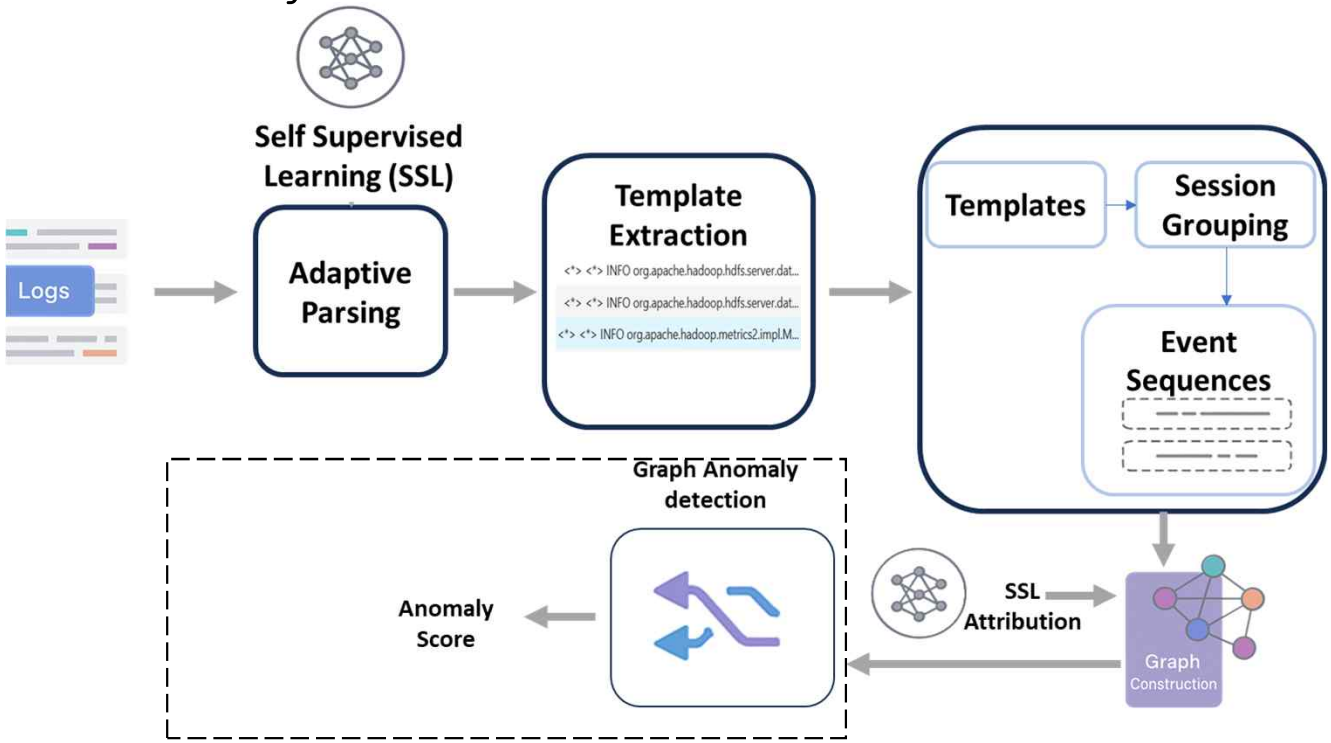
로그 기반 이상징후 탐지

- Adaptive Graph Construction
  - Enhance raw log filtering by templates are grouped into sessions
  - Graphs are formed to represent temporal or causal relations
  - Creates flexible graph structures that preserve both structure and context of execution flows.



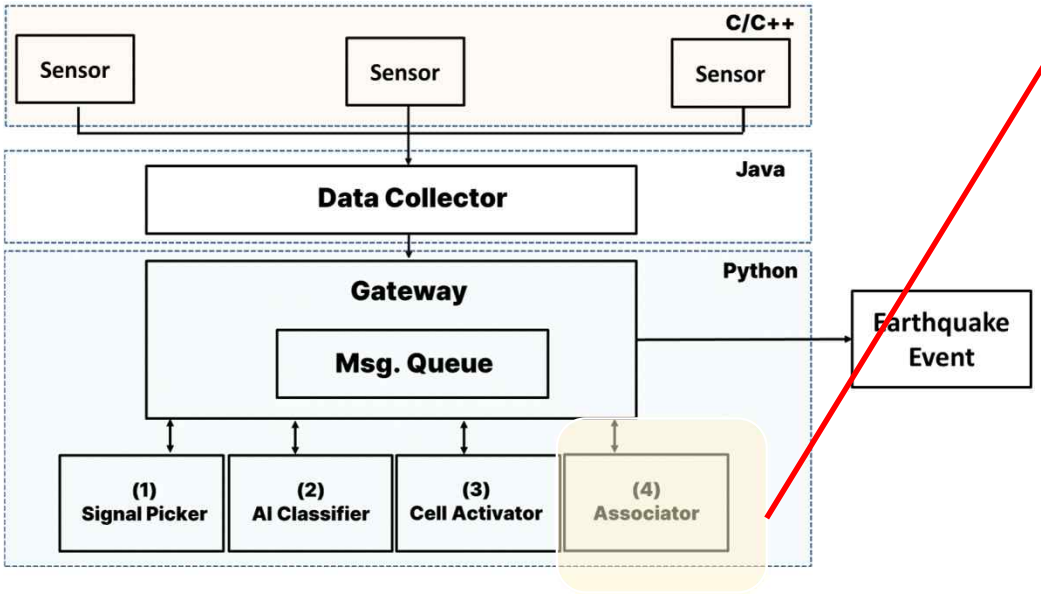
로그 기반 이상징후 탐지

- Analyze graphs for anomalies and predictions
  - Graphs are passed into the model (e.g., GNN, Auto Encoder, Graphformer, Graph Informer), which applies attention over long sequences.
  - Outputs include anomaly scores



센터 내 연구협력

- 연구 협력 내용 (오학주, 최윤자 교수님)
  - 테스트베드를 활용한 타입 오류 패치 생성 연구




```python
def add_trigger(self, sensor_id: Union[bytes, str],
                lat: float, lng: float,
                timestamp_msec: int):

    sensor_id = self._convert_sensor_id(sensor_id)
```

```python
def _convert_sensor_id(sensor_id):
    sensor_id = bytes_to_usim_str(sensor_id,
                                  byteorder='little')
    return sensor_id
```

```python
def bytes_to_usim_str(b: bytes,
                      byteorder='little') -> str:
    i = int.from_bytes(b, signed=False,
                       byteorder=byteorder)
    return f'{i:011d}'
```

Patches (LLM, PySTAAR)

```python
def bytes_to_usim_str(b: bytes):
    # 11: early return from input 'b'
    if b is None:
        return '0' * 11
    # ---
```

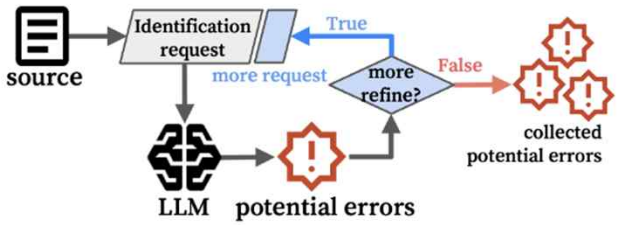
```python
def bytes_to_usim_str(b: bytes):
    # 11: convert 'b' to utf-8 encodable
    if not isinstance(b, bytes):
        b = b.encode('utf-8')
    # ---

    i = int.from_bytes(b, signed=False, byteorder='little')
    return f'{i:011d}'
```

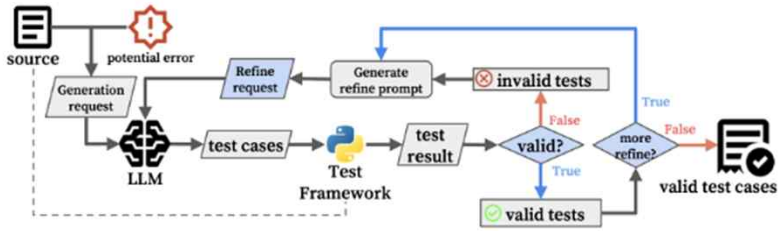
```
    @staticmethod
    def _convert_sensor_id(sensor_id):
-       sensor_id = bytes_to_usim_str(sensor_id, byteorder='little')
+       if not isinstance(sensor_id, str):
+           sensor_id = bytes_to_usim_str(sensor_id, byteorder='little')
        return sensor_id
```

센터 내 연구협력

- 연구 협력 내용 (오학주, 최윤자 교수님)
  - 테스트베드를 활용한 타입 오류 패치 생성 연구
    - 지진경보 시스템에서 LLM과 PySTAAR를 활용한 타입오류 패치 생성 결과 비교 평가
    - LLM을 사용하여 타입오류 발생 가능성이 있는 지점을 식별하고 테스트 케이스 생성 후 LLM과 PySTAAR로 패치 생성



LLM을 사용한 잠재적 오류 식별



오류에 대한 테스트케이스 생성 LLM 사용

Modules	PySTAAR		LLM	
	Patch(#F)	Patch(#E)	Patch(#F)	Patch(#E)
Association	15	16	12	13
Gateway	9	16	8	15
BatchML	2	3	2	3
CliTools	1	1	1	1
MseedSink	1	1	0	0
ObjSink	1	2	1	2
PacketGather	3	4	3	4
STALTA	2	3	2	3
Total	34	46	29	41
Succ. Rate	94.44%	93.88%	80.56%	83.67%

패치 생성 결과

감사합니다.