202488539 도건우

AI Security Term Project Final Report

시계열 데이터 기반 디스크 이상 탐지 모니터링 시스템

1. Introduction

현대 컴퓨팅에서 데이터는 스토리지에 저장된다. 안정적인 스토리지 시스템은 컴퓨팅의 가장 기본적인 요소이다. 디스크의 정상 동작 여부는 데이터 신뢰성과 시스템 가용성을 결정짓는 요소이다. 그러나 디스크 이상 탐지는 복잡성과 불편함, 그리고 비가시성으로 판단에 어려움이 있다. blktrace, iostat과 같은 디스크 탐지 프로그램은 디스크 I/O 성능 및 동작을 모니터링하는 데에는 유용하지만, 실질적인 디스크 이상 탐지 관점에서는 한계를 가지고 있다. blktrace는 사용자 큐까지 요청 큐에 대한 자세한 정보를 제공하는 블록 계층 IO 트레이스 툴이지만 시각적으로 데이터를 판단하기 어렵다. 데이터 구조가 복잡하고 해석이 어렵기 때문에 사용자의 전문성이 요구된다. 또한 iostat은 사용자가 보기 쉬운 형태로 데이터를 제공하나, 제공되는 형태의 데이터는 디스크 사용률로서 이러한 데이터로는 디스크의 가비지 컬렉션, 디스크 증폭 등의 내부적인 문제를 파악할 수 없다. 이러한 문제들은 사용자가 결국 디스크 트레이스 툴을 사용하더라도 디스크의 이상 상태를 예측할 수 없다는 문제가 존재한다. 이를 보완하기 위해 blktrace에서 발생하는 블록 큐 데이터를 시계열 데이터로 구성하여 머신 러닝 알고리즘을 활용하여 이상 패턴을 확인할 수 있는 모델을 본 보고서에서 제시한다.

2. Background & Related Works & Proposed System

본 2장에서는 디스크 이상 탐지 모델에 대해서 서술한다.

2.1 AAE(Adversarial AutoEncoder) 모델

AAE 모델은 특정 데이터에서 이상(Anomaly)를 탐지하기 위한 모델이다. 해당 모델은 정상 데이터만을 학습 데이터로 사용하여 정상 데이터의 분포를 학습하고, 새로운 데이터가 정상 데이터의 분포를 따르지 않는지 판단하여 이상 여부를 탐지하는 데 사용된다. 참고 논문[1]에서는 오토인코더, LSTM 모델을 기반으로 하는 AAE 모델을 제시한다. 본 프로젝트에서는 참고 논문[1]의 아키텍처를 참고하여 모델을 구성한다. Fig 1은 참고 논문[1]에서 제시하는 아키텍처이다. 해당 아키텍처에서는 정상 상태의 시계열 데이터를 입력 데이터로 받아서 LSTM 기반 인코더(Encoder)를 통해 시계열 데이터를 잠재 공간(latent space) 벡터 Z로 매핑한다. 디코더는(Decoder)는 잠재 공간 벡터 Z를 다시 원래 데이터로 복원한다. 디스크리미네이터(Discriminator)는 GAN(Generative Adversarial Network)의 일부로 동작하면서 복원된 데이터가 정상 데이터 분포를 따르는 지 평가한다. Fig 2는 Fig 1의 아키텍처를 기반으로 경량화된 아키텍처이다.

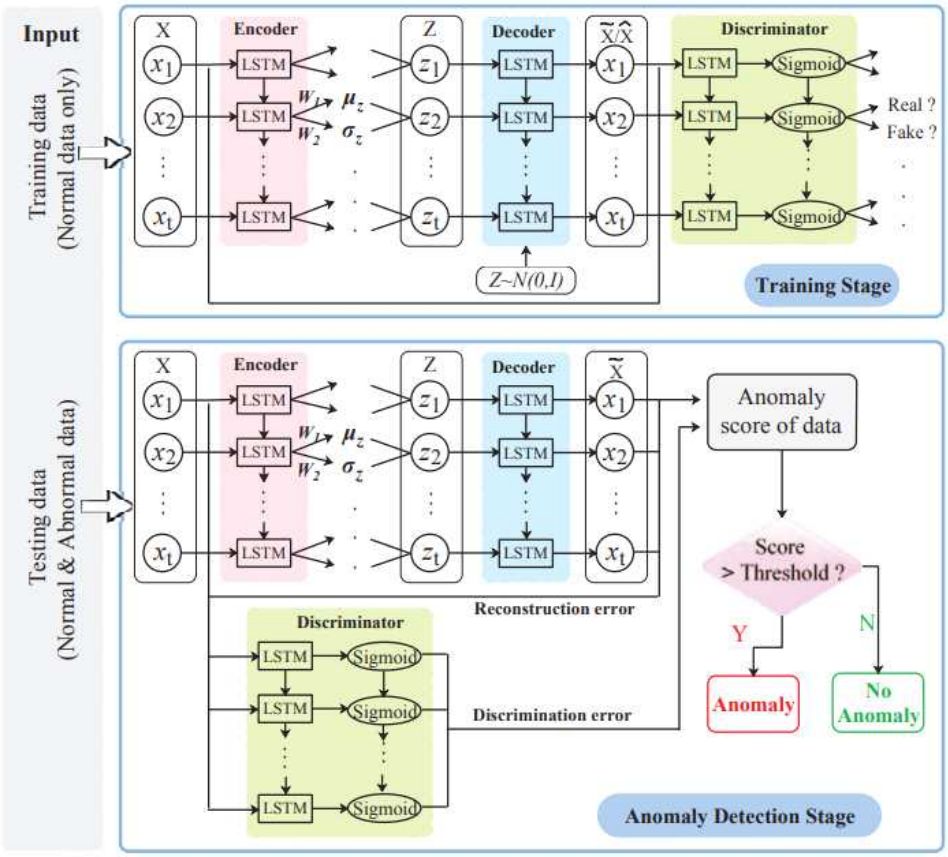

Fig. 1. AAD 아키텍처

3. Proposed System

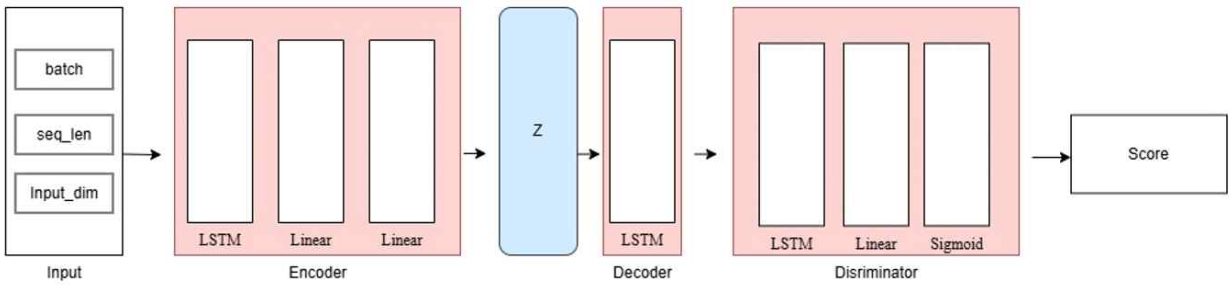

Fig. 2. AAD 아키텍처를 기반으로 재구성된 LSTM 기반 오토인코더 모델

Fig 2는 본 프로젝트에서 구현한 모델의 아키텍처를 보인다. 인코더(Encoder)에서 입력 데이터 X를 처리하여 잠재 공간 벡터로 변환한다. 시계열 데이터를 학습하여 최종적인 hidden state

를 통해 잠재 공간의 평균(μ_z)과 분산(σ_z)을 계산한다. 디코더(Decoder)에서는 잠재 공간 벡터 Z를 입력으로 받아 데이터를 복원한다. 디스크리미네이터(Discriminator)에서는 복원된 데이터(X^)를 입력으로 받아서 원본 데이터 분포에 가까운지 시그모이드를 통해서 판별한다. 학습 과정은 다음과 같다. 데이터를 배치(Batch) 단위로 처리하며, 각 배치는 입력 데이터 X로 구성된다. X를 모델에 전달하여 복원된 데이터와 잠재 벡터를 생성하고 재구성 손실과 KL 손실을 계산하여 총 손실을 구한다. 이 때 사용된 옵티마이저는 RMSprop를 사용하였다. RMSprop는 가중치 업데이트 시 기울기의 제곱 이동 평균을 사용하여 학습률을 조정한다.

4. Dataset configuration

데이터셋은 blktrace와 fio를 사용하여 데이터를 구성하였다. fio는 디스크 입출력 성능 테스트를 위해 설계된 도구이다. 다양한 디스크 I/O 작업을 시뮬레이션하고, 디스크의 읽기, 쓰기, 랜덤 접근 등을 측정하는데 사용된다. 우선 blktrace를 사용하여 커널의 블록 계층에서 발생하는 디스크 입출력을 추적한다. 동시에 다양한 fio 스크립트(랜덤 읽기/쓰기, 순차적 읽기/쓰기)를 발생시켜서 이에 따른 블록 계층 트레이스 로그를 파싱하고 데이터 전처리 과정을 통해 [timestamp, IO-type, Secotr, Size] 형태로 데이터셋을 구성했다.

5. Conclusion

본 프로젝트 리포지토리에 포함된 “main.py”를 실행시키면 그래프를 통해 이상 탐지를 시각화 할 수 있다. 실행결과에는 I/O Tpye 분포와 이상치 선형 그래프를 확인할 수 있다. 설계 의도에 따라 IO Tpye 분포에 따라 이상치 그래프가 달라지는 것을 확인할 수 있다. Fig 4의 실행결과2에서는 특정 섹터에 과도한 읽기 동작을 수행하는 워크로드를 수행하였다. Fig 3은 디스크에 워크로드를 동작하지 않은 그래프이다. 그러나 이상치 수치로 이상을 탐지하는 형태가 아닌 진동 형태로 디스크에 어떤 특정 동작이 수행됨을 확인할 수 있게 되었다. 그래프 개형으로는 Fig 1에서는 800~1000 구간에서 특정 스케쥴링 문제나 부하가 발생한 것처럼 보이며, Fig 2에서는 중간 지점에서 워크로드가 동작했기 때문에 변동성이 크게 증가한 것을 알 수 있다. 그러나 쓰기 워크로드는 마운트된 디스크에서 수행할 경우 치명적인 시스템 손상을 유발할 수 있기 때문에 로컬 환경에서 수행하기에는 어려움이 존재했다.

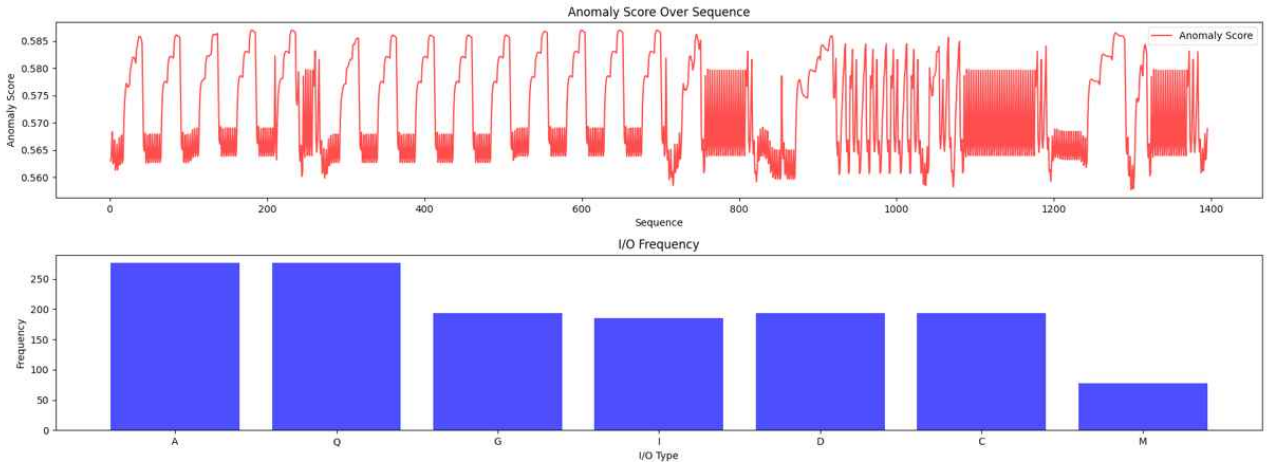

Fig. 3. 실행결과1

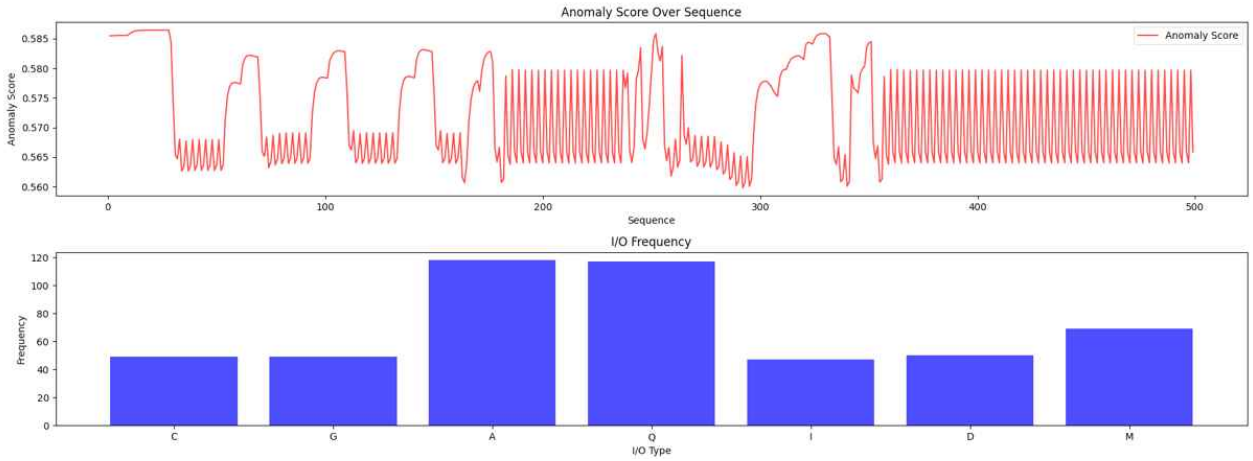

Fig. 4. 실행결과2

< References >

[1] A One-Class Anomaly Detection Method for Drives based on Adversarial Auto-Encoder, Yufei Wang, 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th