표현 학습 기반의 딥러닝 모델을 활용한 클라우드 자원 이상 감지 시스템

이민영 [1], 유헌창 [2]
[1] 고려대학교 SW·AI 융합대학원 석사과정
[2] 고려대학교 정보대학 컴퓨터학과 교수

eheh12eh@korea.ac.kr, yuhc@korea.ac.kr

Anomaly Detection System for Cloud Resources Using Representation Learning-Based Deep Learning Models

Min-Yeong Lee[1], Heon-Chang Yu[2]
[1]Dept. of Applied Artificial Intelligence, Graduate School of SW·AI Convergence, Korea University
[2]Dept. of Computer Science & Engineering, Korea University

요 약

퍼블릭 클라우드 시장이 성장하면서 퍼블릭 클라우드에서 호스팅하는 컴퓨팅 자원으로 구축된 거대하고 복잡한 IT 시스템이 점차 많아지고 있다. 이러한 시스템의 증가는 서비스 장애 발생 확률을 높이므로, 장애 관리 및 선제 감지를 위한 퍼블릭 클라우드 자원의 이상 감지 연구에 대한 수요 또한 증가하고 있다. 그러나 연구에 활용할 수 있는 벤치마크 데이터셋이 없다는 점과, 실제 자원에서 추출할 수 있는 데이터는 레이블링이 되어 있지 않은 불균형 데이터라는 점 때문에 관련 연구가 부족한 상황이다. 이러한 문제를 해결하고자 본 논문은 비지도 방식의 표현 학습 기반 딥러닝 모델을 활용한 이상 감지 시스템을 제안한다. 시스템의 이상 감지 성능을 유지하고자 일정 주기마다 다수의 딥러닝 모델을 재학습하고 비교하여 최적의 모델로 업데이트 하는 방식을 고안하였다. 해당 시스템의 평가에는 실제 퍼블릭 클라우드 자원에서 발생한 메트릭 데이터가 활용됐으며, 그 결과 준수한 이상 감지 성능을 보인다는 것을 확인하였다.

1. 서론

퍼블릭 클라우드는 유연성, 확장성, 비용 효율성을 기반으로 기업과 개인의 IT 환경에 필수적인 요소로 자리 잡았다. 이에 힘입어 퍼블릭 클라우드 시장은 향후 4 년간 연평균 19,9%의 성장이 예측될 정도로 급격한 성장세를 유지하고 있다[1].

그 결과 퍼블릭 클라우드 환경에서 호스팅 되는 다양한 클라우드 컴퓨팅 자원으로 구성된 IT 시스템들이 점차 증가하고 있다. 이러한 크고 복잡한 시스템의 증가는 장애(System Failure) 발생 가능성을 높이는 주요 요인 중 하나이므로, 오늘날 장애 관리의 중요도 또한 커지고 있다[2, 3].

IT 운영 담당자들이 장애 발생을 최소화하고자 활용하는 전통적인 방법 중 하나가 모니터링이다. 이 방식은 클라우드 컴퓨팅 자원에서 발생하는 성능 지표인 메트릭(metric) 데이터(CPU 사용률, 메모리 사용률, 응답시간 등)를 활용한다. 각 메트릭의 임계치(threshold) 혹은 정상 범위를 설정한 다음, 해당 값이나 범위를 넘어가면 IT 운영 담당자에게 알림을 보내 자원의 이상(anomalous) 상태를 파악하는 것이 목표이다.

하지만 이와 같은 단순 모니터링에는 두 가지 단점이 존재한다. 첫째, 정적(static) 임계치 설정 방식은 빠르게 변화하는 클라우드 자원의 상태를 실시간으로 반영하지 못한다[4]. 둘째, 실제 장애 여부와 무관하게 임계치를 넘어가는 모든 경우에 알림을 보내기 때문에 장애 상황이 아님에도 알림을 보내는 허위 알림(false alert)의 빈도가 증가하여 IT 운영 담당자들의 업무 피로도가 증가한다.

이를 보완하고자 등장한 해결책 중 하나가 바로 이상 감지(Anomaly Detection)이다. 퍼블릭 클라우드 자원 이상 감지의 핵심은 실시간으로 흘러 들어오는 자원들의 메트릭 데이터에 통계 혹은 기계학습 모델을 적용하여 이상 패턴을 찾아내 장애를 미리 감지하는 것이다.

그러나 해당 분야의 연구는 벤치마크 데이터셋의 부재로 매우 부족한 상황이다[5]. 각 기업 혹은 개인이 퍼블릭 클라우드 자원으로 구축한 시스템은 구조가 전부 다르므로 범용적인 데이터를 정의하는 것이 까다롭고, 보안상 자세한 데이터를 구하는 것이 어렵기 때문이다.

더욱이 IT 운영 환경에서 모든 클라우드 자원의 메트릭 데이터에 장애 여부를 일일이 레이블링(labeling) 하는 것은 현실적으로 어렵다. 이는 메트릭 데이터가 실시간으로 발생하며 다양한 지표로 구성된 대규모 다변량 시계열 데이터인 동시에 장애 데이터의 비율이 현저히 낮은 불균형 데이터라는 특성에 기인한다.

따라서 본 연구는 표현(Representation) 학습 기반의 비지도 딥러닝 모델을 활용한 클라우드 자원의 이상 감지 시스템을 소개한다. 실제 운영 중인 퍼블릭 클라우드 자원의 메트릭 데이터를 활용하여 실시간으로 최적의 모델을 업데이트 하는 방법을 제시하고, 업데이트 된 모델의 이상 감지 성능을 확인하였다.

2. 관련 연구

2.1 표현 학습 기반(Representation Learning Based) 이상감지

표현 학습 기반의 이상감지 모델은 정상 데이터에 내재된 표현을 학습함으로써 정상적인 상황에서의 특징과 패턴을 파악한다. 이때 모델에 새로 들어오는 데이터에서 학습한 표현과 정상 데이터로부터 학습한 표현 간의 차이가 클수록 비정상 데이터일 가능성이 높다고 보고 이를 이상으로 감지한다.

즉, 정상 데이터의 학습만으로도 이상 감지가 가능하기 때문에 레이블이 없고 대부분이 정상 데이터인 클라우드 자원 메트릭 데이터의 이상 감지에 적합하다고 할 수 있다[6, 7].

2.2 표현 학습 기반의 비지도 딥러닝 모델

본 절에서는 시스템 구현에서 최적 모델 후보군으로 사용하고자 하는 DCdetector, TimesNet, TranAD, USAD, DeepSVDD 모델에 대해 살펴보려 한다. 다음의 모델은 모두 정상 데이터의 표현을 학습하는 방식을 기반으로 이상을 감지한다.

DCdetector 는 대조 학습 기반의 이중 브랜치 어텐션(contrastive learning-based dual-branch attention) 구조를 제안한다. 입력된 시계열 데이터를 패치(patch) 단위로 나누고, 이를 패치 간(patch-wise) 표현을 학습하는 브랜치와 패치 내(in-patch) 표현을 학습하는 브랜치에 동일하게 통과시킨다. 이때 정상 데이터는 각 브랜치에서 도출되는 표현이 서로 유사하지만 비정상 데이터는 그렇지 않다는 가정 하에 이상을 감지한다[8].

TimesNet 은 시계열 데이터를 2 차원으로 변환하는 과정을 통해 시계열 데이터가 가지는 다중 주기성(multi-periodicity)을 반영한다. 모델이 주기 내 변동성(intraperiod variation)과 주기 간 변동성(interperiod variation)을 동시에 고려한 표현을 추출하여 학습하므로 시계열 이상 감지 뿐만 아니라 예측 등 다양한 과제에서 활용할 수 있다[9].

TranAD 는 다변량 시계열 이상 감지에 특화된 모델로, 디코더(decoder)가 두 개인 트랜스포머(Transformer) 구조를 가진다. 인코더(encoder)는 시계열 데이터의 장·단기 특징을 모두 학습하고, 디코더는 정상 데이터만 복원이 잘 되도록 적대적(adversarial) 학습을 한다. 즉 입력한 데이터가 복원이 잘 되지 않았을 경우 이를 비정상 데이터로 판단한다[10].

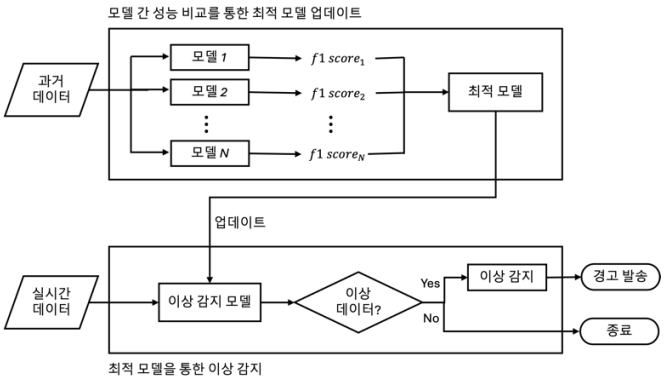
USAD 는 두 개의 오토인코더(Autoencoder)로 정상 데이터의 표현을 학습한다. 이때 각 오토인코더에 입력 데이터를 더 정확하게 복원하도록 서로 경쟁시키는 적대적 학습 방식을 적용한다. 입력 데이터와 그것의 복원 결과로 계산한 재구성 오차(reconstruction error)가 임계치(threshold)를 넘는 경우, 이를 이상치로 판단한다[11].

DeepSVDD 는 SVDD(Support Vector Data Description)에 딥러닝을 접목한 모델이다. 비지도 방식으로 정상 데이터의 표현을 학습하여 특성 공간(feature space)에서 정상 특성들 만을 포함하고 있는 초구(hypersphere)를 찾고, 해당 구 밖에 위치하는 데이터는 비정상 데이터로 판별함으로써 이상을 감지한다[12].

3. 표현 학습 기반 딥러닝 클라우드 자원 이상 감지 시스템

3.1 이상 감지 시스템의 구조

본 논문에서 제안하는 시스템은 (그림 1)과 같이, 일정 기간 축적한 데이터를 학습시켜 딥러닝 모델 간의 이상 감지 성능을 비교하여 최적의 모델을 찾는 부분(3.1.1)과 업데이트 된 최적 모델을 바탕으로 실시간으로 스트리밍 되는 데이터의 이상을 감지하는 부분(3.1.2)으로 구성된다.



(그림 1) 제안하는 이상 감지 시스템 구조도

3.1.1 모델 간 성능 비교를 통한 최적 모델 업데이트

클라우드 자원은 가변성이 강하므로 자원에서 발생하는 메트릭 데이터의 패턴 또한 가변적일 수 있다. 이에 시간이 지남에 따라 모델의 성능이 저하되는 모델 드리프트(Model Drift) 현상이 발생할 수 있으므로, 모델을 주기적으로 업데이트 하는 것은 이상 감지 성능 유지에 중요하다[13]. 따라서 특정 딥러닝 모델 하나를 활용하기보다는, 주기적으로 다수의 모델 중에서 최적의 모델을 선정하는 방식을 고안하였다.

이 단계에서는 일정 주기마다 수집한 데이터를 여러 딥러닝 모델에 학습시킨 다음, 이상 감지 성능이 가장 뛰어난 하나의 모델을 실시간 데이터의 최적 이상 감지 모델로 업데이트 한다. 최적 모델 후보군으로는 2.2 절에서 언급한 딥러닝 모델들이 선정되었으며, 각 모델을 구현하기 위해 deepod 라이브러리를 활용하였다[14].

모델 간 성능 비교를 위한 평가 지표로는 정밀도(Precision)와 재현율(Recall)의 조화 평균인 F1 스코어를 사용한다. 이는 불균형 데이터셋을 활용한 모델의 성능 평가에 적합하며, 값이 1 에 가까울수록 이상 감지 성능이 뛰어남을 의미한다.

3.1.2 최적 모델을 통한 이상 감지

클라우드 자원에서 실시간으로 생성되는 메트릭 데이터를 앞 단계에서 업데이트 된 최적 모델에 입력하여 이상 여부를 판별한다. 판별 척도로는 해당 시점에서 최적 모델로 선정이 된 딥러닝 모델 각각의 이상 점수(anomaly score)가 사용된다.

비정상 데이터가 식별된 시점에 외부로 경고 알람을 보내는 모듈을 시스템에 추가하는 것이 이상적이나, 이 논문에서는 구현하지 않았다.

3.2 데이터셋

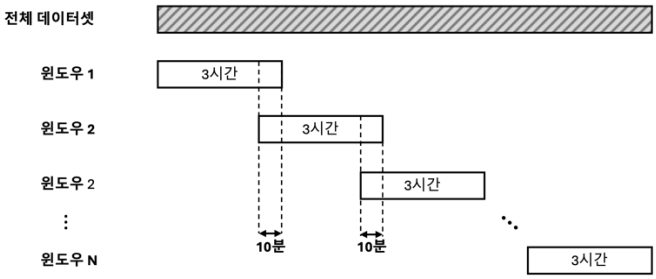
3.2.1 출처 및 구성

모델의 학습 및 전체 시스템의 평가에는 실제 서비스 중인 솔루션의 데이터베이스 역할을 하는 퍼블릭 클라우드 자원의 1 분 단위 메트릭 데이터를 활용했다.

데이터셋은 약 1 개월 간 수집한 총 12 개의 성능 지표로(CPU 사용률, DB 연결 클라이언트 수, DB 작업량, 읽기/쓰기 지연 시간, 읽기/쓰기 처리량 등) 구성되어 있다.

3.2.2 전처리 과정

전처리 단계에서는 12 개 성능 지표 간 값의 규모(scale)의 편차가 심하므로 표준화(Standardization)를 진행하였다. 이후 원 데이터셋을 학습·검증·테스트용 데이터셋으로 분리하였다. 또한 (그림 2)와 같이 데이터셋 각각에 10 분의 중첩(overlap)이 포함된 윈도우(window)를 3 시간 단위로 생성하는 과정을 추가하였다.



(그림 2) 중첩이 포함된 윈도우 생성 예시

윈도우란 시계열 데이터를 사전에 설정한 시간 길이만큼 나눈 구간으로, 딥러닝 시 데이터에 내재된 시간적 패턴과 동적 변화를 분석하는 데 중요한 역할을 한다. 특히 각 윈도우를 앞뒤로 일정 구간이 중첩되도록 생성하면 연속적인 시점들 사이의 중요한 정보를 보존할 수 있다. 결국 이상 감지 모델이 시계열 데이터의 전체적인 맥락을 보다 정확하게 파악할 수 있게 되어 더욱 효과적인 이상 감지가 가능해진다[15].

다만, 모델 간 성능 평가 및 시스템의 최종 성능 평가를 위해 인위적으로 정상 데이터를 비정상 데이터로 변환하여 검증(validation) 데이터셋과 테스트 데이터셋에 주입하였다. 또한 모델 평가 시 활용하기 위해 정상·비정상 여부를 나타내는 레이블 컬럼을 추가하였다.

검증 데이터셋은 최적 모델의 업데이트를 위한 모델 간 성능 평가에, 테스트 데이터셋은 실시간 데이터를 대신하여 업데이트 된 최적 모델의 이상 감지 성능 평가에 활용하였다.

4. 이상 감지 결과

4.1 최적 모델 업데이트를 위한 모델 간 성능 비교

전처리를 마친 학습용 데이터셋을 2.2 절의 딥러닝 모델 각각에 학습시킨 다음, 검증용 데이터셋으로 각 모델의 이상 감지 성능을 비교하였다.

<표 1> 최적 모델 선정을 위한 모델 간 이상 감지 성능 비교

모델	**F1-Score**	Precision	Recall
DCdetector	0.0168	0.0087	0.2558
TimesNet	0.9136	0.9737	0.8605
TranAD	**0.9639**	0.9999	0.9302
USAD	0.7835	0.7037	0.8837
DeepSVDD	0.9512	0.9999	0.9070

그 결과, <표 1>과 같이 TranAD 의 F1 스코어가 가장 1 에 가깝게 나왔다. F1 스코어가 1 에 가장 가깝다는 것은 주어진 데이터에 대해 비정상 여부를 가장 정확히 식별하면서도 거짓 양성(False Positive, 정상적인 데이터를 비정상이라고 판단하는 경우)의 수를 최소화할 수 있음을 의미한다. 따라서 이 실험에 사용된 데이터셋에

대해서는 TranAD 가 실시간 데이터의 이상 감지를 위한 최적의 모델로 선정되었다.

4.2 업데이트 된 최적 모델의 이상 감지 성능 평가

제안한 시스템의 최종 이상 감지 성능 평가에는 실시간 데이터를 사용해야 하나, 실험에서는 3.2.2 에서 언급한 테스트 데이터셋으로 실시간 데이터를 대체하였다.

<표 2> 제안한 시스템의 이상 감지 성능 평가

F1-Score	Precision	Recall
0.9398	0.9750	0.9070

최적 모델이 업데이트 된 후의 시스템 성능을 평가한 결과 정확도 0.975, 재현율 0.907 로 이상 상황을 거의 놓치지 않고 식별해낸다는 것을 알 수 있다. F1 스코어 또한 0.9398 로 높아 본 논문이 제안한 시스템의 이상 감지 성능이 준수함을 확인하였다<표 2>.

5. 결론 및 고찰

오늘날 퍼블릭 클라우드 자원으로 구축된 복잡한 IT 서비스의 수는 점차 늘어나고 있으며, 서비스의 안정성을 보장하기 위해 클라우드 자원의 장애를 선감지하는 방법을 마련하는 것의 중요도 또한 높아지고 있다.

본 연구는 주기적으로 다수의 표현 학습 기반 비지도 딥러닝 모델의 성능을 비교하여 최적의 이상 감지 모델을 업데이트하고, 이를 바탕으로 실시간 다변량 시계열 데이터의 이상을 감지하는 시스템을 제안하였다.

실제 퍼블릭 클라우드 자원에서 추출한 메트릭 데이터를 활용하였으므로, 해당 도메인의 데이터를 사용한 연구가 부족한 상황에서 관련 연구를 시도했다는 것에 의의가 있다.

다만 위 시스템을 실제 IT 환경에 적용하기 위해서는 다음과 같은 항목들의 개선이 필요하다. 첫째, 다수의 IT 서비스는 단일 클라우드 자원이 아닌 여러 종류의 자원을 복합적으로 사용하므로 다중 자원의 데이터셋을 활용한 연구로 확장되어야 한다. 둘째, 데이터 전처리 과정에서 윈도우 길이를 정할 때 값을 바꿔 가며 시스템의 이상 감지 성능을 비교하여 최적의 윈도우 길이를 찾는 과정이 추가되어야 한다. 셋째, 앞서 언급했듯이 실시간 데이터를 스트리밍 하는 부분과, 실제로 검출된 이상치에 대해 경고 알람을 보내는 부분이 추가로 구현되어야 한다.

향후 보완을 통해 더 뛰어나고 범용적인 퍼블릭 클라우드 자원의 이상 감지 시스템이 마련될 것을 기대한다.

참고문헌

[1] Michael Shirer, "Worldwide Spending on Public Cloud Services is Forecast to Reach $1.35 Trillion in 2027, According to New IDC Spending Guide", IDC Media Center, 2023.08.29.

[2] AlTwaijiry, A, "Cloud computing present limitations and future trends.", Journal of Grid and Distributed Computing, 6(6), 93-102, 2021.

[3] Gill, Sukhpal Singh, and Rajkumar Buyya, "Failure management for reliable cloud computing: a taxonomy, model, and future directions.", Computing in Science & Engineering, 22.3, 52-63, 2018.

[4] Cotroneo, Domenico, et al., "Enhancing the analysis of software failures in cloud computing systems with deep learning.", THE JOURNAL OF SYSTEMS AND SOFTWARE, 111043, 2021.

[5] Hagemann, T., & Katsarou, K.. "Reconstruction-based anomaly detection for the cloud: A comparison on the yahoo! webscope s5 dataset.", Proceedings of the 2020 4th International Conference on Cloud and Big Data Computing, 2020, 68-75.

[6] Trirat, Patara, et al., "Universal Time-Series Representation Learning: A Survey.", arXiv preprint arXiv:2401.03717, 2024.

[7] 조현수, “A Deep Representation Learning for Unsupervised Anomaly Detection : 비지도 이상 탐지를 위한 표현 학습론", 박사학위논문, 서울대학교, 2023.

[8] Yang, Yiyuan, et al., "Dcdetector: Dual attention contrastive representation learning for time series anomaly detection.", Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 3033-3045, 2023.

[9] Wu, Haixu, et al., "Timesnet: Temporal 2d-variation modeling for general time series analysis.", The eleventh international conference on learning representations, 2022.

[10] Tuli, Shreshth, Giuliano Casale, and Nicholas R. Jennings, "TranAD: deep transformer networks for anomaly detection in multivariate time series data.", Proceedings of the VLDB Endowment, 15.6, 1201-1214, 2022.

[11] Audibert, Julien, et al., "Usad: Unsupervised anomaly detection on multivariate time series.", Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining, 3395-3404, 2020.

[12] Ruff, Lukas, et al., "Deep one-class classification.", International conference on machine learning. PMLR, 4393-4402, 2018.

[13] Webb, Geoffrey I., et al., "Characterizing concept drift.", Data Mining and Knowledge Discovery, 30.4, 964-994, 2016

[14] Hongzuo Xu, et al., DeepOD, GitHub Repository, https://github.com/xuhongzuo/DeepOD

[15] Li, Jinbo, et al., "Clustering-based anomaly detection in multivariate time series data.", Applied Soft Computing 100, 106919, 2021.