DeepAD: A Generic Framework based on Deep Learning for Time Series Anomaly Detection

23.05.19

이정민

연구 배경

❖ 기존 연구들의 한계

- 다수의 false positive 발생(false alarm)
- 지도 학습 기반의 방법론들은 다량의 labeled data 필요
  - ➢ Class imbalance problem
- 하나의 모델은 특정 데이터셋에만 적합할 수 있음

기여점

Deep AD

❖ Main Contributions

- 이상 데이터에 대한 label 정보를 모델 학습 및 threshold를 정하는데 사용하지 않음
- 다양한 패턴에 적용 가능한 **dynamic threshold** 설정
- 단변량 뿐만 아니라 다변량 데이터셋에 적용 가능
- 다양한 모델을 결합함으로써, 보다 robust한 예측 접근법 제안

방법론

Deep AD

❖ Framework

- Step 1 : Time Series Forecasting(TSF)
- Step 2: Merge Prediction(MP)
- Step 3: Anomaly Detection(AD)

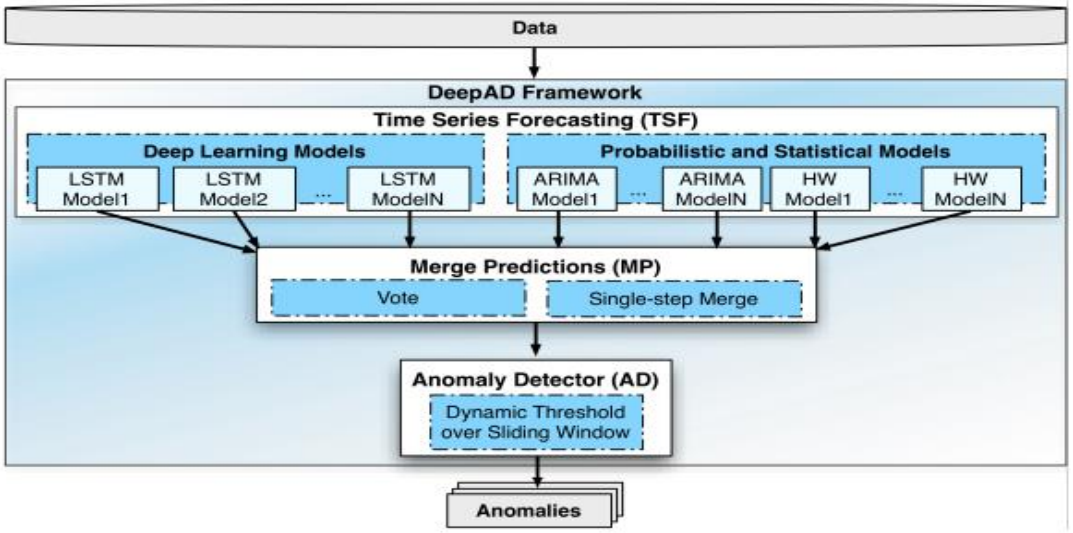


Fig. 1: DeepAD Framework Overview.

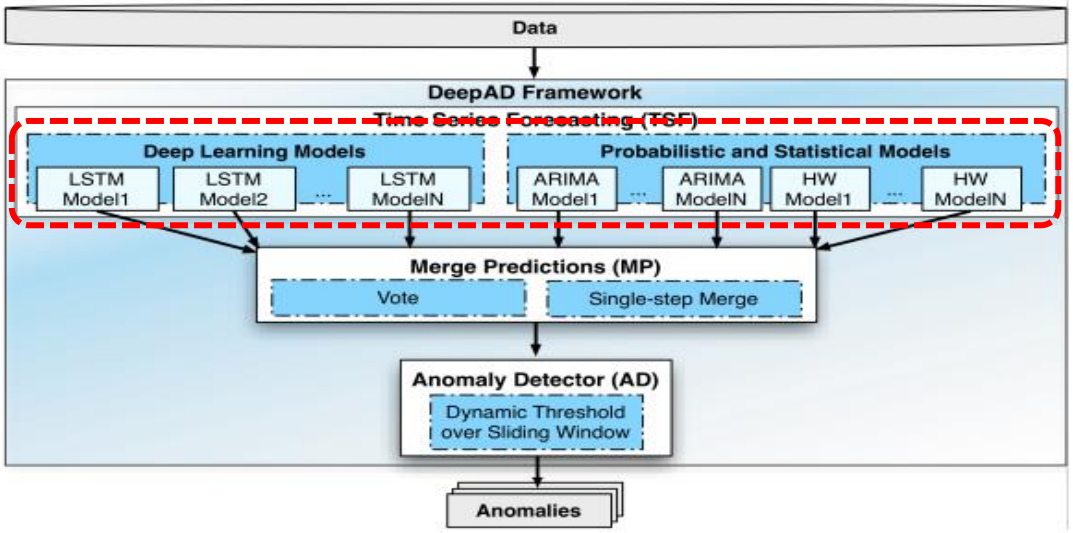
Buda, T. S., Caglayan, B., & Assem, H. (2018, June). Deepad: A generic framework based on deep learning for time series anomaly detection. In *Advances in Knowledge Discovery and Data Mining: 22nd Pacific-Asia Conference, PAKDD 2018, Melbourne, VIC, Australia, June 3-6, 2018, Proceedings, Part I* (pp. 577-588). Cham: Springer International Publishing.

방법론

Deep AD

❖ Framework

- Step 1 : Time Series Forecasting(TSF)
- Step 2: Merge Prediction(MP)
- Step 3: Anomaly Detection(AD)



각 모델별로 정상 데이터 학습

Fig. 1: DeepAD Framework Overview.

Buda, T. S., Caglayan, B., & Assem, H. (2018, June). Deepad: A generic framework based on deep learning for time series anomaly detection. In *Advances in Knowledge Discovery and Data Mining: 22nd Pacific-Asia Conference, PAKDD 2018, Melbourne, VIC, Australia, June 3-6, 2018, Proceedings, Part I* (pp. 577-588). Cham: Springer International Publishing.

방법론

Framework

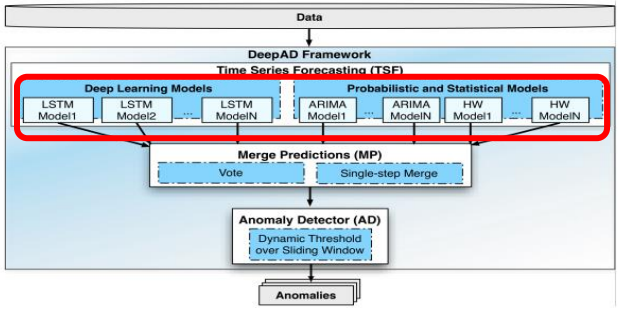
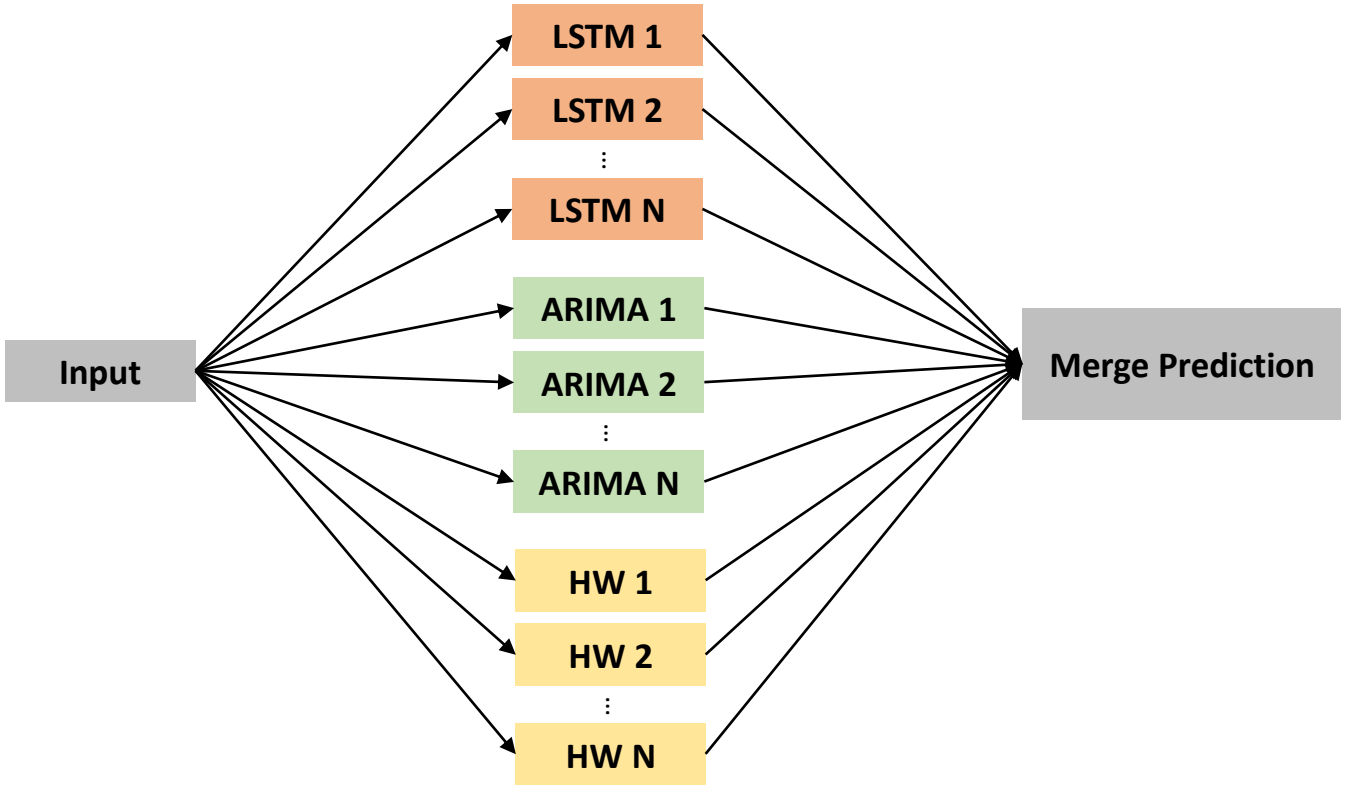


Fig. 1: DeepAD Framework Overview.

❖ Time Series Forecasting(TSF)

- 다양한 모델 사용(LSTM, ARIMA, Holt-Winters)
  - ➢ 각 모델은 특정 데이터셋에만 의존할 수 있기 때문



방법론

Framework

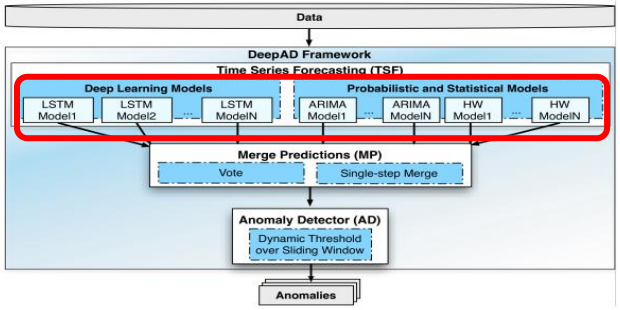
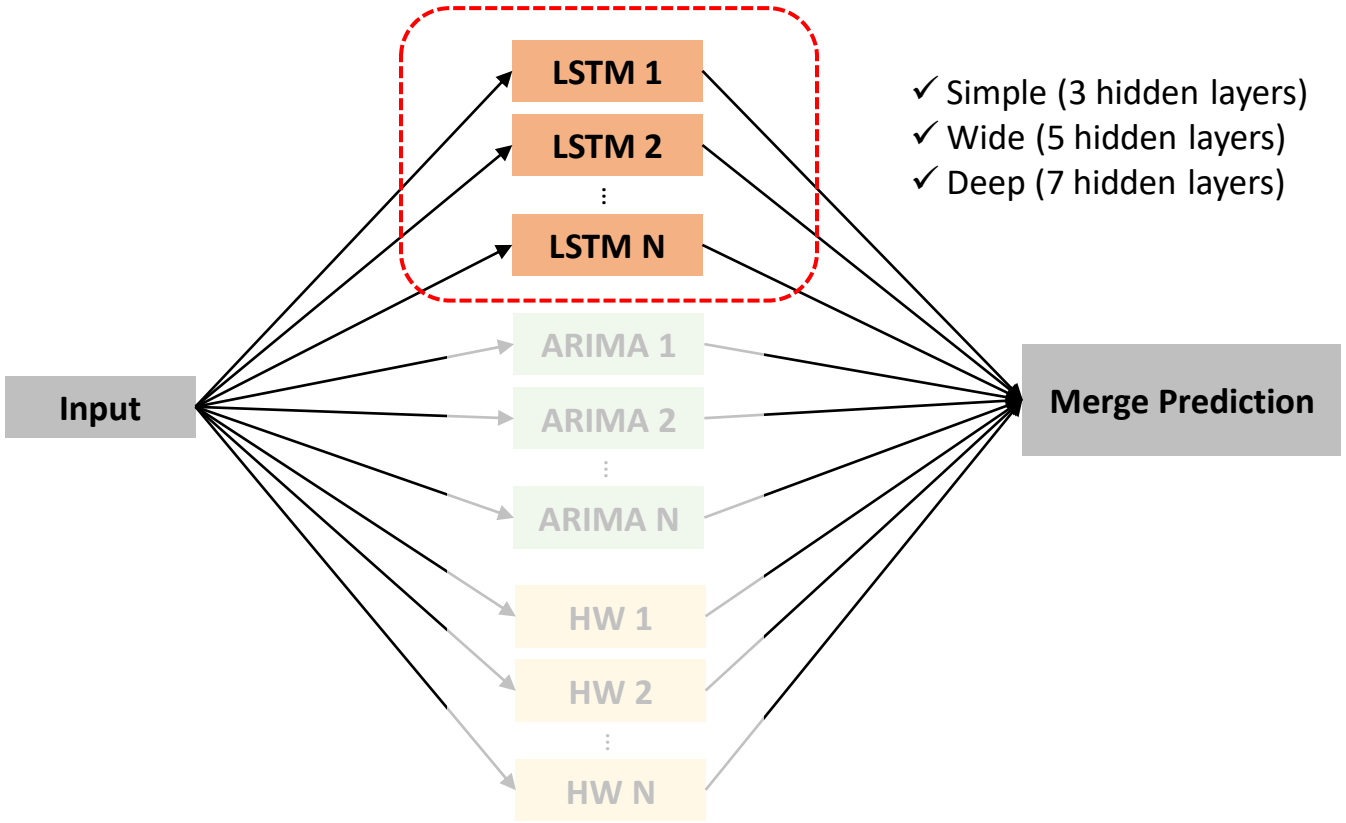


Fig. 1: DeepAD Framework Overview.

❖ Time Series Forecasting(TSF)

- 다양한 모델 사용(LSTM, ARIMA, Holt-Winters)
  - ➢ 각 모델은 특정 데이터셋에만 의존할 수 있기 때문



✓ Simple (3 hidden layers)
✓ Wide (5 hidden layers)
✓ Deep (7 hidden layers)

방법론

Framework

❖ Merge Prediction(MP)

- Single-step merge
- Vote

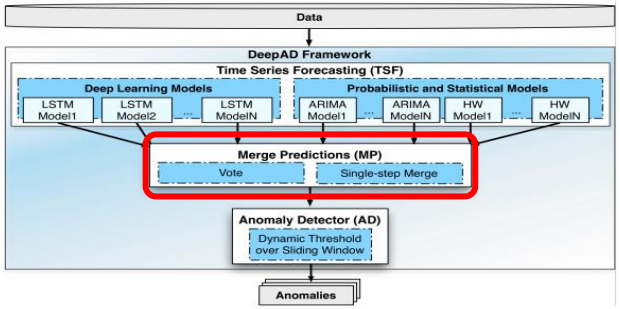


Fig. 1: DeepAD Framework Overview.

방법론

Framework

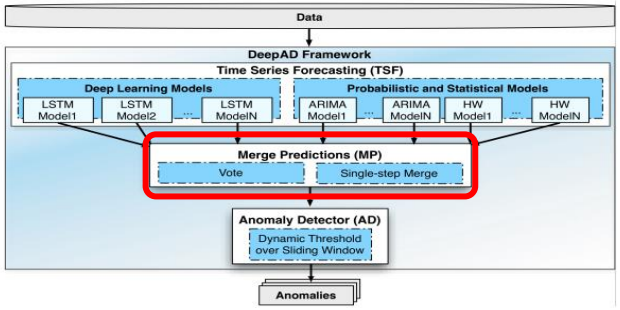
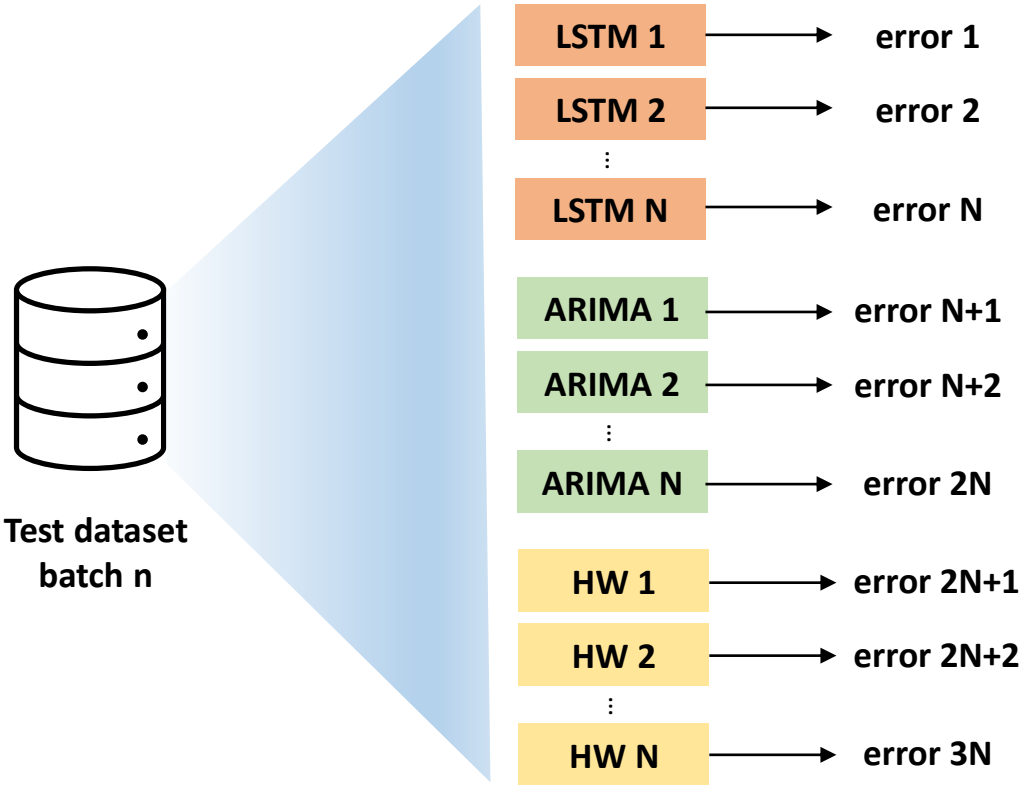


Fig. 1: DeepAD Framework Overview.

❖ Merge Prediction(MP)

- Single-step merge
  - ➢ 각 모델별로 학습
  - ➢ test set에 대해 **각 batch 마다** best model (RMSE 기준)의 예측 값을 output으로 사용



방법론

Framework

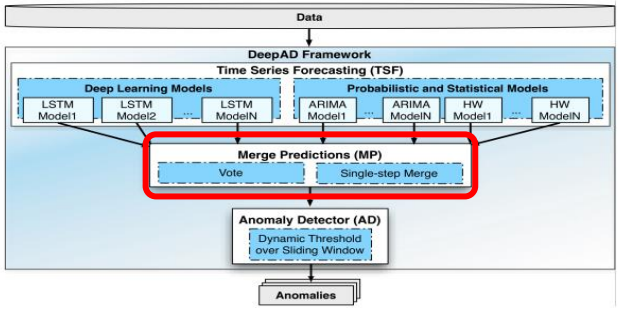
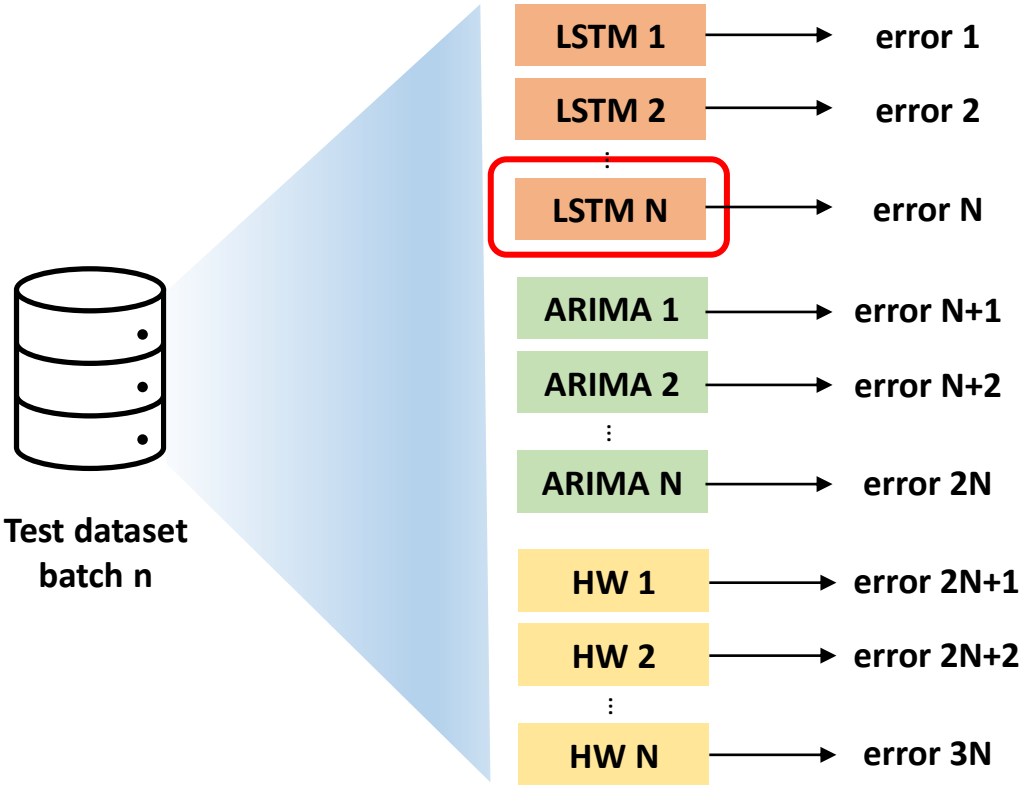


Fig. 1: DeepAD Framework Overview.

❖ Merge Prediction(MP)

- Single-step merge
  - ➢ 각 모델별로 학습
  - ➢ test set에 대해 **각 batch 마다** best model (RMSE 기준)의 예측 값을 output으로 사용



방법론

Framework

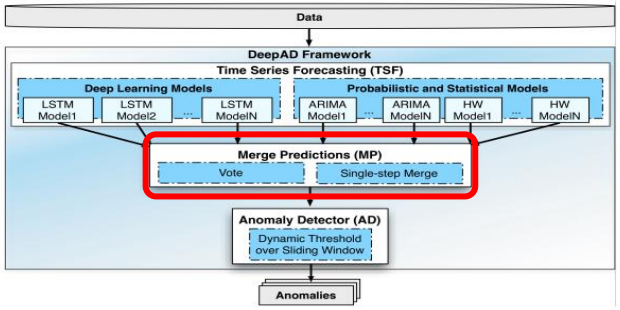
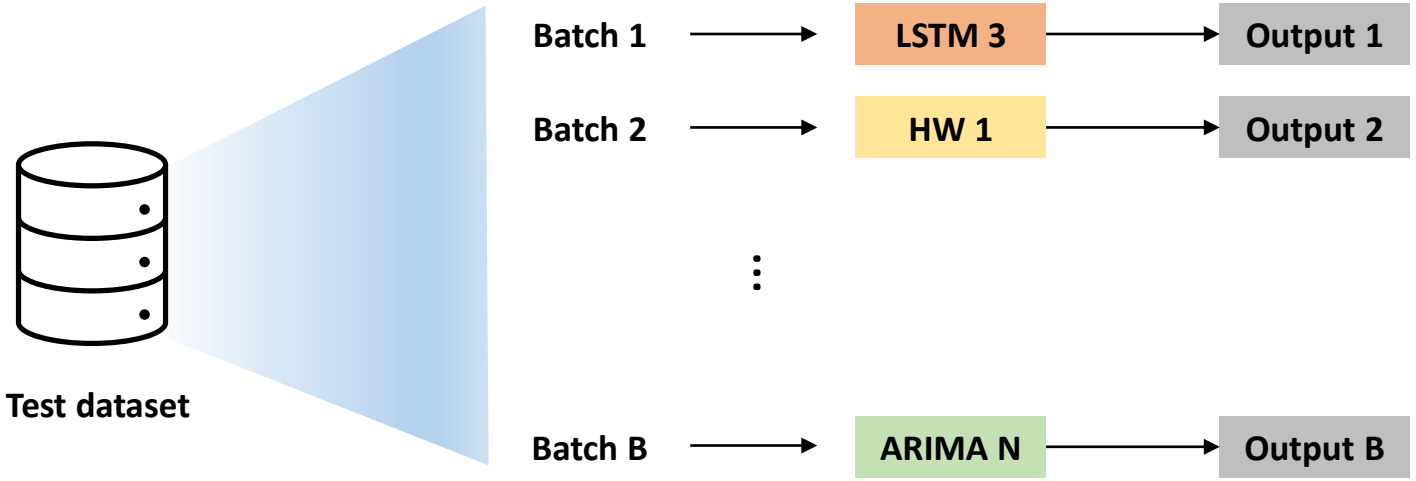


Fig. 1: DeepAD Framework Overview.

❖ Merge Prediction(MP)

- Single-step merge
  - ➢ 각 모델별로 학습
  - ➢ test set에 대해 **각 batch 마다** best model (RMSE 기준)의 예측 값을 output으로 사용



방법론

Framework

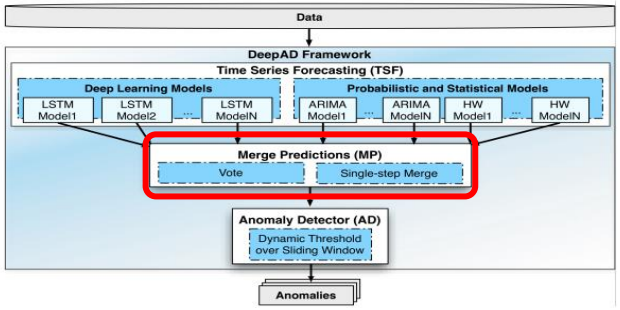
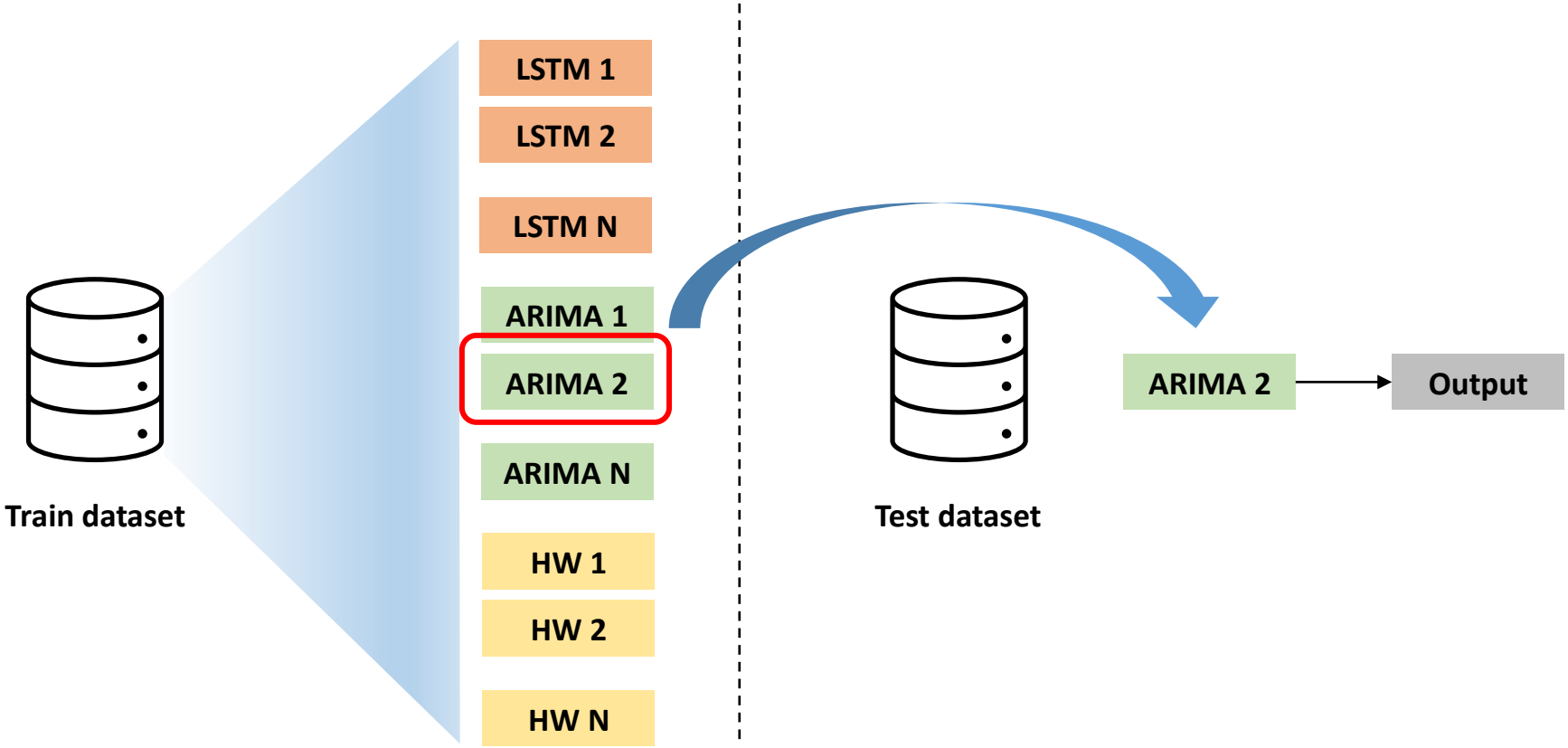


Fig. 1: DeepAD Framework Overview.

❖ Merge Prediction(MP)

- Vote
  - ➢ **전체 train set에서의** best model (RMSE 기준)을 test에 사용



방법론

Framework

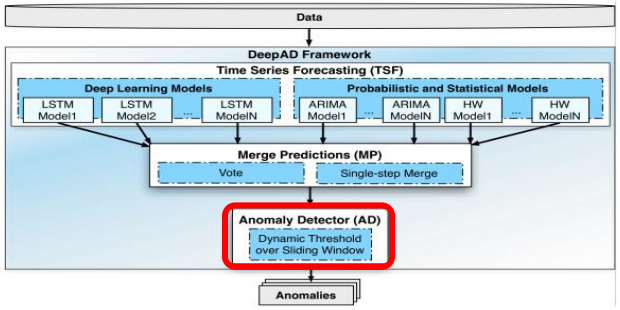


Fig. 1: DeepAD Framework Overview.

❖ Anomaly Detector(AD)

1. 예측 시점 직전(window size)의 errors를 스케일(0~1)
2. Queue에 저장
3. 각 시점 $threshold \leftarrow 10 \times \sigma(scaled\ errors)$
4. 예측 시점의 scaled error가 threshold보다 작으면 queue에 추가