An Improved Sensor Anomaly Detection Method in IoT System using Federated Learning

Duc Hoang Tran, Van Linh Nguyen, Ida Bagus Krishna Yoga Utama, Yeong Min Jang
Department of Electronics Engineering
Kookmin University
Seoul 136-702, Korea
Email: duchoangbkdn.1995@gmail.com, linhnv@kookmin.ac.kr, idabaguskrishnayogautama@gmail.com, yjang@kookmin.ac.kr

***Abstract*— The industrial sensor has emerged as a critical device to monitor environment condition in the manufacturing system. However, abnormal behaviors of these smart sensor may indicate some failure or potential risk during system operation, thereby increasing high availability of the entire manufacturing process. Data collected from many edge devices for detecting failure contain private data of different enterprises which is challenging current detection approaches as user privacy has attracted more concerns. Moreover, detecting anomalies in the centralized system is often more time consuming due to the response time. To overcome these issues, we proposed an anomaly detection method using a clustering federated learning framework with a long short-term memory (LSTM) to improve model performance in term of accuracy, scalability and more secure.**

Keywords*— *anomaly detection, federated learning, timeseries forecasting

I. INTRODUCTION

The Internet of Things (IoT) and machine learning are critical for increasing living standards and sustaining urban growth in the past decade. By connecting various types of sensors and other devices, IoT contributes to the generation of interoperable networks in smart manufacturing, from which actionable insights may be extracted through the connection and analysis of large volumes of real-time data. Hence, sensor anomaly detection becomes the common method for predictive maintenance of Supervisory Control and Data Acquisition (SCADA) systems, which aims to detect sensor signal that may indicate abnormal behaviors on environments or device malfunctions. There are three basic methods using machine learning for anomaly detection including supervised learning, semi-supervised learning, and unsupervised learning [8]. However, these approaches are facing with many challenges on accuracy measurement, real-time issues, imbalanced samples, and practicality. Recently, many studies found the solution on unsupervised learning technique consisting of reconstruction method for anomaly detection [9]. Specifically, they attempt to predict or reconstruct a time series signal and then, it makes a comparison between the real and the predicted or reconstructed values [1]. High prediction or reconstruction errors suggest the presence of anomalies. However, these methods generally generate the predictor with overfitted issues, resulting in low performance [2]. In this paper, we proposed the use of federated learning with clustering clients and Autoencoder LSTM (AE-LSTM) for creating effective predictor to detect anomalous. According to Federated Learning (FL) principle, the training model will take place on edge devices before uploading the model into centralized server. Thus, our method allows exploited the potential information from different place with high privacy on smart factory system. By the novelty of clustering time-series data, we can improve the predictability in different range value of industrial sensor data. Therefore, our method can archive good performance of detecting anomalous on multivariate data from diverse spatial locations at different times. The remainder of the paper is organized as follows. Section II presents the Federated Learning with clustering the clients in SCADA system; Then, we describe anomaly detection method using AE-LSTM in Section III; Section IV provides detail of our frameworks; we also detail the experimental result and comparison with others method, some discussion and future works are given.

II. FEDERATED CLUSTERING METHOD

A. Federated learning

Federated Learning allow learning from different geographical data without store it in central server [3][10]. The global model is trained from updated version in local as follows Figure 1. First, the server selects a list of subset clients and transmits the model to each subset. Second, each

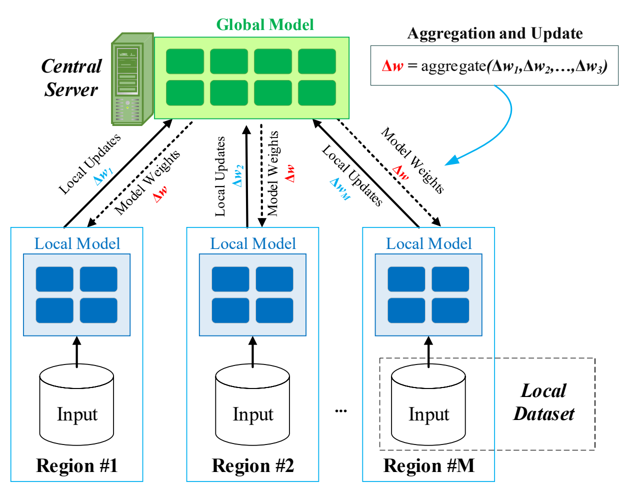


Figure 1. Federated Learning diagram

client trains received global model on local device and transmits the trained model parameter to the server. Third, the server averages all version of trained models which generally be used Federated Average (FedAvg) for aggregating local learner model from many clients.

B. Federated Clustering

One challenge of FedAvg method is the requirement of similar patterns [5]. Otherwise, the heterogeneity in local data may lead to misconvergence of the global model. For instance, one sensor device collects local data from high temperature environment and different from others might affect to global model weights due to its desire for fitting data. This will cause high error to obtained model and decrease performance of another client's model. To solve this issue, we proposed a framework to group the clients based on their similarities. Because FL method cannot access to client data, we will not consider the clustering method on original data. Instead of that, we conduct a new method allowing group client based on their representation which is took into an autoencoder model on neural network. Autoencoder will not only support for generating predictor, but it also presents the useful representation from the output of the encoder layer. Typically, we collect the deep representation and local hyperparameter simultaneously after training raw data in device by autoencoder LSTM model as shown as Figure 2 and Algorithm 1. The main feature from each client can be group by K-means clustering algorithm and in step of FedAvg, server can define which model can send again to which group devices and then increase performance of entire network. Thank to this method, we can archive a reliable predictor for anomaly detection.

III. LSTM-based Anomaly Detection Framework

Many researchers recently pay attention on improve LSTM model to obtain high accuracy predictor. Despite proving effective in anomaly detection, LSTM often easily overfit with the training data and the anomaly precision will be impacted also [2]. To tackle this issue, the continuous real-time learning is necessary for incrementing the ability to learn

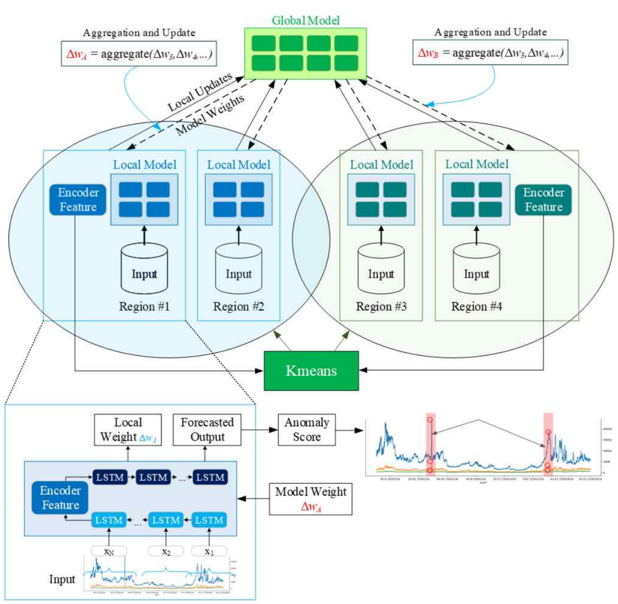
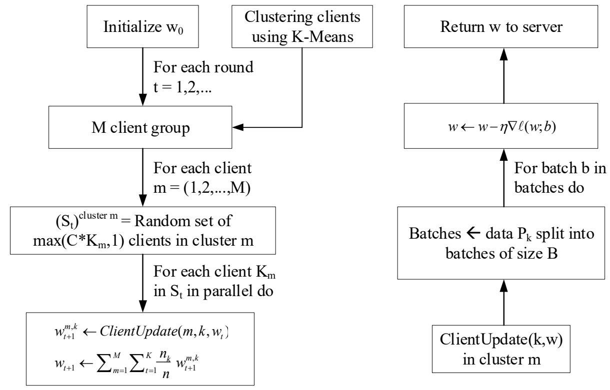


Figure 2. Proposed Federated Learning with K-means Clustering for anomaly detection



Algorithm 1. FedAvg algorithm with K-means for client clustering

new real-world data. Therefore, we proposed the combination between robust algorithm using AE-LSTM and inspiration from the benefits of Federated Learning with Clustering method to simultaneously enhance IoT system's performance.

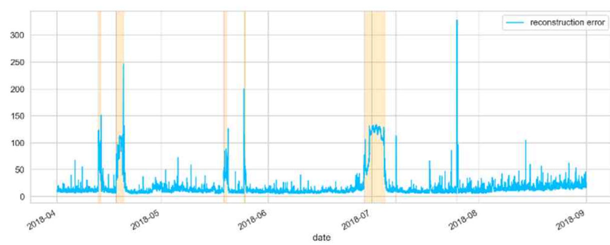
In this paper, we work on a multivariate timeseries data which is integrated the useful information from different sensor variables. In IoT system, this data was be collected in real time by the edge devices and stored in the database for analysis and perform intelligent services. Then, the historical data was fed into the preprocessing function before training with autoencoder LSTM received global weight from server. All task to make the predictor will be taken place in the local devices and send the updated weight to central server every round. The training output was used for detecting anomalous based on absolution of difference $e^i = \left|x^i - \hat{x}^i\right|$ where x^i is real data and $\hat{x}^i$ is forecast value. The error vector calculated on the timeseries predictor are the mean absolute error (MAE) for each output sequence. We also set threshold for anomaly detection as the maximum value of MAE in the training (normal) dataset. Moreover, the autoencoder LSTM model provide encoder output as a basis input for K-means clustering in central server which improve all clients' model in entire network.

IV. Experimental Results

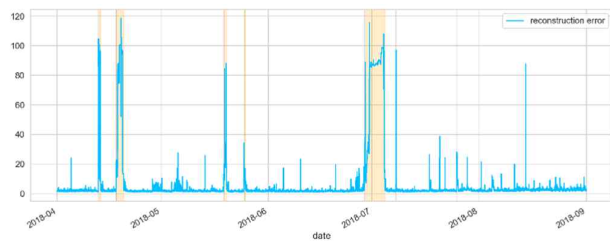
A. Dataset

We performed a set of experiments on pump sensor dataset taken from 53 sensors installed on a pump to measure various behaviors of them [7]. To facilitate testing, we divide the dataset into 50 clients, and set the fraction of Federated model is 0.1. We set having 3 level for each sensor data, hence, 3 clusters are made from these clients with different number of participants. The AE-LSTM is deployed for create the predictor in every client. The clients share representation data to the central server and the servers group the clients into three clusters using K-means clustering method [6]. After training only normal data to generate predictor over some step, the distributed probability of error signal will be estimated and be used to assess the likelihood of anomaly score. We divided 80% of data for training and 20% for evaluate validation dataset. Our programming was deployed by Pytorch and compared with other traditional model for evaluation.

B. Implemetation and Evaluation



b)



a)

Figure 3. Reconstruction Error for calculating anomaly score.
a) AE-LSTM with traditional FL; b) AE-LSTM with clustering FL

Firstly, we conduct a preprocessing for analyze data before fed it into our machine learning method. The time series data is normalized using standard scaler and fill in the missing data by mean value of entire dataset. Then, we provide an AE-LSTM to learn compressed representation of normal data and do the reconstruction. The local weight of model is sent to server and deploy the aggregation of these local weights. After that, we conduct the average model on validation dataset and set for early stop metric. Figure 3 shows reconstruction error of Federated Learning comparing with traditional LSTM. Based on this reconstruction error, the anomaly score is calculated, and threshold τ also be established to make detection decision. Specifically, the anomaly score will be defined as:

$$a^i = (e^i - \mu)^T \Sigma^{-1} (e^i - \mu) \qquad (1)$$

where μ, Σ is the parameter of a normal distribution $\mathbb{N}(\mu, \Sigma)$ using Maximum Likelihood Estimation. if $a^i > \tau$, a point in a sequence can be predicted to be “anomalous”, otherwise “normal” The FL method can help to solve false alarm problem in testing dataset due to the overfit issues of LSTM model.

We also fed the compressed encoder of local clients into the K-means model for picking up accurately suitable group with its and speed up the convergence of model. Figure 4 shows the improvement of clustering FL comparing with original FL. Specifically, the training loss without clustering uses more epochs to converge and is higher compared to training with clustering. By using this technique, our proposed model early stops when the training round is 13.

For sensor anomaly detection, our experiments prove AE-LSTM with FL can enhance accuracy of detector compare with other method as shown in Table I. Typically, F1-score of our method is significantly higher than centralized LSTM and FL-LSTM which reach 97.15%. Although the precision of clustering FL LSTM lower than our proposed scheme, it still cannot reach higher recall which get false alarm in detection algorithm. Moreover, the group progress using cluster model make the training time consuming become shorter than the baseline method. In addition, our proposed scheme guarantees the privacy of client’s data while real-time detection and also reduce the training time due to available net parameter sharing between different clients.

TABLE I: The Comparison of our proposed model to baseline methods

Methods	Precision (%)	Recall (%)	F1 score (%)
Centralized LSTM	96.45	89.08	92.62
FL-LSTM	**97.58**	95.66	96.57
Clustering FL-LSTM (proposed)	96.36	**97.94**	**97.15**

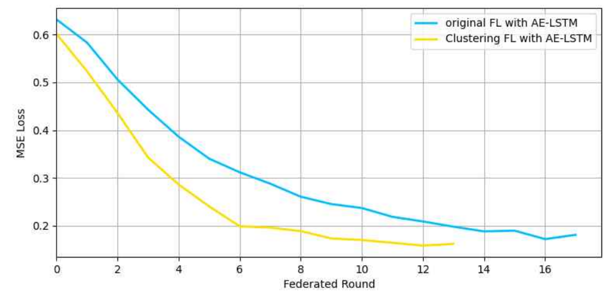


Figure 4. The model converges in our proposed method

V. Conclusions

This study proposed a novel method to detect anomalous on timeseries data using clustering Federated Learning with AE-LSTM approaches. Experimental results on this paper demonstrated our method’s ability to improve the results of a diverse of many clients in IoT systems, achieving much better performance compared to baseline methods. We also indicated the efficient of model when support clustering method for speed up model converges.

In the future, we consider providing an investigation with other technique in IoT system such as blockchain and generative adversarial network.

Acknowledgment

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2022-2018-0-01396) supervised by the IITP(Institute for Information & Communications Technology Planning & Evaluation).

References

[1] Alexander Geiger, Dongyu Liu, Sarah Alnegheimish, Alfredo Cuesta-Infante,Kalyan Veeramachaneni TadGAN: Time Series Anomaly Detection Using Generative Adversarial Networks, BigData-2020. *In Proceedings of IEEE International Conference on Big Data,* December 2020.

[2] Malhotra, Pankaj & Ramakrishnan, Anusha & Anand, Gaurangi & Vig, Lovekesh & Agarwal, Puneet & Shroff, Gautam. (2016). LSTM-based Encoder-Decoder for Multi-sensor Anomaly Detection.

[3] V. Mothukuri, P. Khare, R. M. Parizi, S. Pouriyeh, A. Dehghantanha and G. Srivastava, "Federated-Learning-Based Anomaly Detection for IoT Security Attacks," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2545-2554, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3077803.

[4] J. Konečný, H. B. McMahan, D. Ramage, and P. Richtárik, "Federated Optimization: Distributed Machine Learning for On-Device Intelligence," pp. 1–38, 2016.

[5] Li L., Fan Y., Tse M., Lin K.-Y. A review of applications in federated learning Comput. Ind. Eng., 149 (2020), Article 106854

[6] Lloyd, Stuart P. "Least squares quantization in PCM." Information Theory, IEEE Transactions on 28.2 (1982): 129-137.

[7] Pump_sensor_data open dataset available on Kaggle Dataset: https://www.kaggle.com/nphantawee /pump-sensor-data

[8] Chandola, V.; Banerjee, A.; Kumar, V. (2009). "Anomaly detection: A survey". *ACM Computing Surveys*. 41 (3): 1–58..Vapnik V.N. *The Nature of Statistical Learning Theory.* Springer; Berlin, Germany: 1995.

[9] Bui, V.; Pham, T.L.; Nguyen, H.; Jang, Y.M. Data Augmentation Using Generative Adversarial Network for Automatic Machine Fault Detection Based on Vibration Signals. Appl. Sci. 2021, 11, 2166

[10] McMahan H.B., Moore E., Ramage D., Hampson S., y Arcas B.A. Communication-efficient learning of deep networks from decentralized data (2017).