Anomaly Detection of Malicious Energy Usage in Smart Factories using Deep Neural Network

Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Jae Min Lee, Dong-Seong Kim
IT Convergence Engineering, *Kumoh National Institute of Technology* Gumi, South Korea
loveahakonye, cosmas.ifeanyi, ljmpaul, dskim@kumoh.ac.kr

***Abstract*—In Smart Factory, an extensive volume of data is generated daily by Advanced Metering Infrastructures (AMI) and Smart Sensors. One such data is the amount of energy usage and the need to keep track of normal and abnormal energy usage in the smart factory. This allows energy producers to uncover abnormal power consumption as well as realizing distinct malicious energy usage. Recognition of abnormal conducts is essential to predict the unusual occurrence and to enhance energy productivity. This work proposes the Long Short-Term Memory (LSTM) Network to accurately recognize malicious energy usage in a smart factory. The proposed system is implemented using Python on Google collaborate with Tanh activation function. The performance of the proposed scheme showed 99.92%, 99.98%, 99.92%, and 99.85% for accuracy, precision, F1-Score, and recall respectively.**

***Index Terms*—Machine Learning, Anomaly Detection, Smart Factory, Smart Grid**

I. Introduction

There has been a rise in research interest for energy grid monitoring. The increase is due to the need for significant, competent, accurate, and safe handling of the burden of anomaly detection for electricity consumption. By delivering virtually actual energy data utilization, Advanced Metering Infrastructures (AMIs) is used for examining power operation tendency to identify inconsistency asserting Smart Factories' protection and averting energy wastes [1], [2]. Moreover, anomaly detection [3] is a salient point to remit Smart Factories' returns and protection by applying constant survey of industries' operations.

This work introduces a Deep learning Neural Network approach for recognizing abnormal energy consumption in smart factory by leveraging on a public dataset comprising smart meter data clustered. Adopting deep neural network has enabled the effective handling and monitoring of the energy grid, otherwise known as smart grid system [4]. The means of controlling energy transmission balance between producer and consumer is the smart grid, managing the stability condition of energy for both parties [5]. Proposed approach uses Long Short-Term Memory Network (LSTM) to envisage power usage changes, and triggering anomalies when threshold is exceeded or changes in energy usage pattern. The contributions of this paper are:

1) Leveraging on existing datasets, and choice of ML algorithms, this work trained and tested dataset using LSTM Model for energy anomaly detection of malicious usage in Smart factories
2) The research also demonstrated the impact of activation function on the efficiency of the proposed LSTM.

The organization of this work is: following section I is section II where we gave background on Smart Factory, Malicious Energy Usage, and Anomaly Detection and techniques and related research. Section III method and design followed by section IV with the experimental result. The paper was concluded in section V.

II. Methodology

1) LSTM: This work proposed the use of LSTM because of its advantage in using large volume of time series data to stimulate decision-making in Smart Factory operations. LSTM is able to learn long-term constraint. It is one of the most accepted Recurrent Neural Networks (RNN).

In this research, an LSTM with three hidden layers was built. This LSTM was trained to predict the power consumption using Adam optimizer. To compare the proposed approach, various scenarios of possible activation function candidates were simulated. The activation functions compared were Relu, Sigmoid and Tanh respectively [6]. The overall system model is as shown in Fig. 1.

2) Dataset: Dataset is an augmented energy load data of the West Region of Electric Reliability Council of Texas (ERCOT) found on the National Renewable Energy Laboratory (NREL) website, for a period of 2012-2015 [7]. The choice of dataset stems from the fact that it is aggregated, however it was preprocessed accordingly for possible intricacies.

III. Performance Evaluation

The proposed LSTM with Tanh activation function performed better than LSTM with Relu and sigmoid functions respectively as shown in Table I. The proposed LSTM recorded 99.92%, 99.98%, 99.92% and 99.85% for accuracy, precision, F1-Score, and recall respectively. Similarly, Figs. 2, 3, and 4 show the accuracy, loss and confusion matrix of the proposed LSTM respectively.

IV. Conclusion

This work presented the use of LSTM with tanh activation as a preferred scheme for the anomaly detection of malicious usage of energy in a smart factory using Deep Neural Network. This is due to its outstanding performance when compared to other activation functions such Relu and Sigmoid. LSTM with

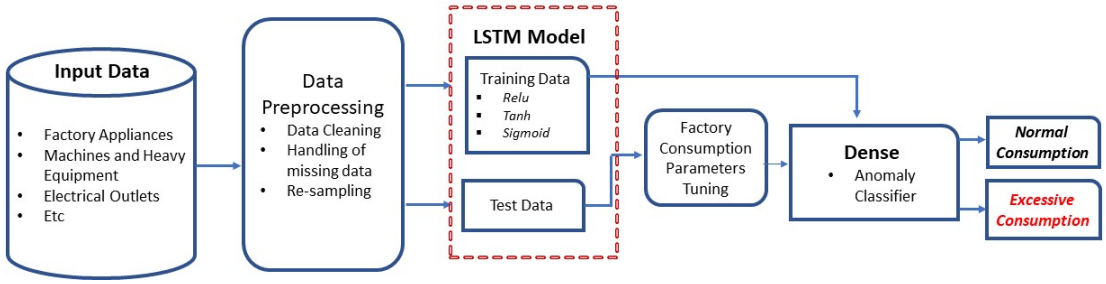

Fig. 1. Proposed Malicious Energy Usage Anomaly Detection Architecture

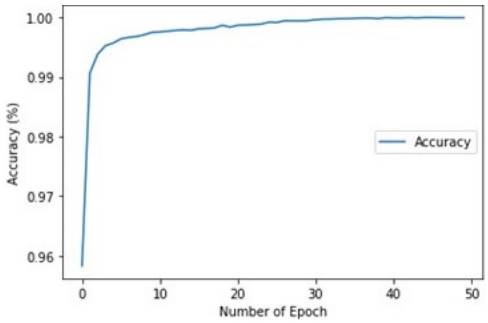

Fig. 2. Accuracy of the LSTM with tanh activation function

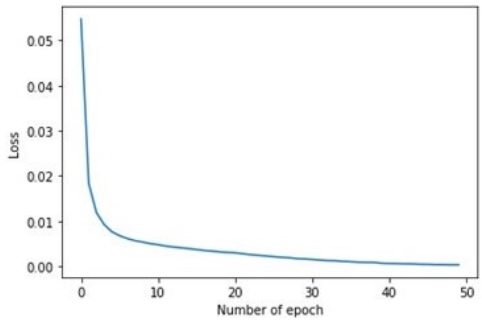

Fig. 3. Loss Performance of the LSTM over number of epoch

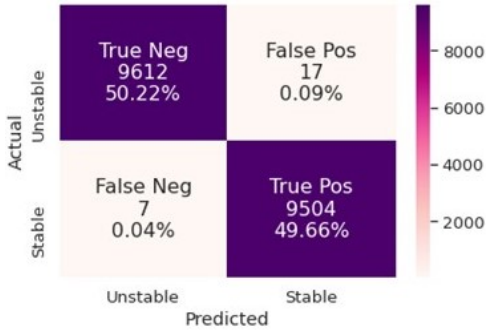

Fig. 4. Confusion matrix of the proposed malicious energy usage anomaly detection

TABLE I
COMPARING THE IMPACT OF ACTIVATION FUNCTIONS ON THE LSTM

Parameter Metrics/Activation Function	Relu	Sigmoid	Tanh
Accuracy (%)	99.87	99.74	99.92
Precision (%)	99.82	100.00	99.98
F1-Score (%)	99.87	99.74	99.92
Recall (%)	99.92	99.48	99.85

tanh activation function is presented high accuracy and minimal error loss. It is a future research direction to demonstrate the real time efficiency of the proposed scheme since time is a critical constraints in smart factories.

ACKNOWLEDGMENT

This research work was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003) and the Grand Information Technology Research Center support program (IITP-2021-2020-0-01612) supervised by the IITP by MSIT, Korea.

REFERENCES

[1] G. Fenza, M. Gallo, and V. Loia, "Drift-Aware Methodology for Anomaly Detection in Smart Grid," *IEEE Access*, vol. 7, pp. 9645–9657, 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2891315

[2] C. I. Nwakanma, F. B. Islam, M. P. Maharani, J.-M. Lee, and D.-S. Kim, "Detection and Classification of Human Activity for Emergency Response in Smart Factory Shop Floor," *Applied Sciences*, vol. 11, no. 8, 2021. [Online]. Available: https://www.mdpi.com/2076-3417/11/8/3662

[3] M. Zanetti, E. Jamhour, M. Pellenz, M. Penna, V. Zambenedetti, and I. Chueiri, "A Tunable Fraud Detection System for Advanced Metering Infrastructure Using Short-Lived Patterns," *IEEE Transactions on Smart Grid*, vol. 10, pp. 830–840, 2019. [Online]. Available: https://doi.org/10.1109/TSG.2017.2753738

[4] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based Smart Grid: Towards Sustainable Local Energy Markets," *Computer Science - Research and Development*, vol. 33, pp. 1–8, 2018. [Online]. Available: https://doi.org/10.1007/s00450-017-0360-9

[5] P. Zhuang and H. Liang, "Hierarchical and Decentralized Stochastic Energy Management for Smart Distribution Systems With High BESS Penetration," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6516–6527, 2019. [Online]. Available: https://doi.org/10.1109/TSG.2019.2906823

[6] C. I. Nwakanma, M. S. Hossain, J.-M. Lee, and D.-S. Kim, "Towards Machine Learning Based Analysis of Quality of User Experience (QoUE)," *International Journal of Machine Learning and Computing*, vol. 10, no. 6, pp. 752–758, 2020. [Online]. Available: https://doi.org/10.18178/ijmlc.2020.10.6.1001

[7] N. R. E. Laboratory, "Open Data Catalog: Smart Grid Dataset." [Online]. Available: https://www.smartgrid.gov/