# Cyber-Physical Data Fusion & Threat Detection with LSTM-Based Autoencoders in the Grid

Georgios Fragkos, Logan Blakely, Shamina Hossain-McKenzie, Adam Summers, Christopher Goes
*Sandia National Laboratories*
Albuquerque, NM, USA
gfragko@sandia.gov, lblakel@sandia.gov, shossai@sandia.gov, asummer@sandia.gov, cegoes@sandia.gov

***Abstract*—The power grid, traditionally perceived as an independent physical network has undergone a significant transformation in recent years due to its integration with cyber communication networks and modern digital components. Cyber situations, including cyber-attacks and network anomalies, can directly affect the physical operation of the grid; therefore, studying this intricate relationship between the physical and cyber systems is pivotal for enhancing the resilience and security of modern power systems. In this digest, a novel Long Short-Term Memory (LSTM)-based Autoencoder (AE) model for cyber-physical data fusion and threat detection is proposed. The scenario under consideration includes the effective detection of a physical disturbance and a Denial-of-Service (DoS) attack, which obstructs control commands during the physical disturbance in the power grid. Detailed analysis and quantitative results regarding the LSTM-based AE model's training and evaluation phases is provided, which highlight its key operation features and benefits for guaranteeing security and resilience in the power grid.**

***Index Terms*—cyber-physical, security, threat detection, machine learning, autoencoders, lstm, power grid**

## I. Introduction

In an era marked by the modernization of the electric grid, the high penetration of Distributed Energy Resources (DER) necessitates a paradigm shift in data management. Cyber-physical systems (CPS) integrate computation, networking, and physical processes that results in systems that are autonomous, intelligent, connected, and collaborative. The coexistence of cyber data and physical data in this evolving landscape underscores the importance of data fusion. According to [1], data fusion is defined as a "process dealing with association, correlation, and combination of data and information from single and multiple sources to achieve refined position and identity estimates, and complete and timely assessments of situations and threats, and their significance". As the grid transforms, understanding its state and ensuring its security requires power system measurements across the systems and seamlessly integrate them with the corresponding cyber data streams. This integration serves as the cornerstone for achieving enhanced situational awareness, enabling a comprehensive group of the grid's dynamic conditions [2].

Additionally, vast amounts of cyber and physical data are generated by the various DER communication types and interfaces within the grid, and a critical challenge emerges: the need for a robust mechanism to ingest and process this information [3]. For instance, processes such as IEEE 1547-2018 DER grid-support functions and communication-assisted protection schemes increase reliance on communications [4]. This is also enhanced by the extremely important need to fortify the grid against potential threats that can compromise its integrity and disrupt its functionality, as demonstrated by the Ukraine 2015 grid cyber-attack and 2013 Metcalf sniper attack [5]. Artificial Intelligence (AI) and Machine Learning (ML) can not only orchestrate seamless cyber-physical data fusion in order to get valuable data insights, but they can also play a crucial role in bolstering cyber-physical security. Through AI-driven mechanisms, the identification of potential cyber threats and physical disturbances in a CPS such as the modern power grid that generates high-fildelity information, can be executed with high accuracy [6]. This enables proactive mitigation strategies and reinforces the resilience of the electric grid against emerging challenges.

In this paper, we present a novel approach for a cyber-physical threat detection methodology through data fusion using a Long Short-Term Memory (LSTM)-based Autoencoder (AE). By integrating the temporal and structural patterns of the cyber-physical data into a lower-dimensional and high-informative feature space with data fusion, we are able to evaluate the accuracy in detecting potential cyber threats or physical disturbaces via the reconstruction loss of the trained LSTM-based AE. Specifically, by training the LSTM-based AE only on the normal cyber-physical data, we are able to define a reconstruction error threshold, which indicates if a new unseen data point is normal or abnormal. The model achieves a perfect accuracy in discriminating between normal and abnormal cyber-physical data, underscoring the critical role of data fusion in enhancing threat detection efficacy within the grid infrastructure.

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC (NTESS), a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration (DOE/NNSA) under contract DE-NA0003525. This written work is authored by an employee of NTESS. The employee, not NTESS, owns the right, title and interest in and to the written work and is responsible for its contents. Any subjective views or opinions that might be expressed in the written work do not necessarily represent the views of the U.S. Government. The publisher acknowledges that the U.S. Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this written work or allow others to do so, for U.S. Government purposes. The DOE will provide public access to results of federally sponsored research in accordance with the DOE Public Access Plan. 979-8-3503-7240-3/24/$31.00

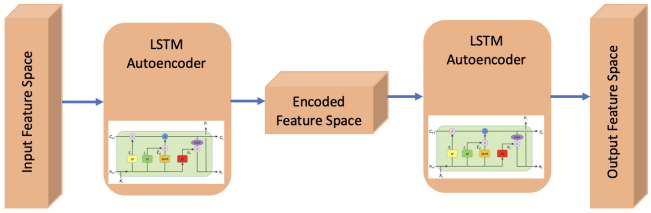


Fig. 1. LSTM-based AE model architecture

## II. Related Work

Considering the increased IEEE 1547-based connection capabilities of DER into the internet or private networks [7], cyber-physical situational awareness is needed to safeguard the electric power system against sophisticated adversaries and guarantee its safe and uninterrupted operation [8]. The fact that cyber-physical systems are highly interdependent necessitates the deeper understanding and exploitation of the valuable connections between the data features within the grid to further ensure its resilience. The majority of the existing techniques concentrate on the acquisition and fusion of physical data only, e.g., frequency, voltage, current, exclusively from geographically distributed physical sensors, supervisory control and data acquisition (SCADA) system, smart meters and phasor measurement units (PMU) [9]. Specifically, they focus on capturing the spatio-temporal correlations of the physical data for fault diagnosis through statistical-based or ML-based state estimation techniques, such as Bayesian inference [10] and deep neural networks (DNN) [11] respectively. Additionally, in [12] the authors propose a transformer model that is utilized in edge nodes in the grid, ingests electrical data and detects false data injection attacks by using federated learning. Similarly, the autors in [13] propose a wavelet transformation and singular value decomposition approach for detecting false data injection attacks. In [14] the authors developed a multi-souce multi-domain cyber-physical data fusion pipeline for classifying cyber attacks in the power systems.

Moreover, some initial research efforts utilize AEs for data fusion to perform threat detection using only cyber data. In particular, the authors in [15] utilize an AE to detect insider cyber-security threats from cyber-only data in an information technology (IT) environment without utilizing an architecture for capturing the temporal dependencies of the data. A hybrid two-stage deep learning architecture consisting of LSTM and AE is presented in [16], where cyber attacks, such as Denial of Service (DoS) and Port Scan, are effectively detected with high accuracy by utilizing cyber-only features (e.g., IP and MAC addresses). In [17], an intrusion detection system that utilizes multiple LSTM-based AE is presented, which uses diverse cyber-only features, such as transmission interval and payload value changes, to identify threats in an in-vehicle network.

Based on the aforementioned research works, we highlight that there is a significant research gap for blending the physical with the cyber data, utilizing cyber-physical data fusion techniques to gain valuable insights from this integration, and using it to perform threat detection to ensure the security of a system. Specifically, the question that we answer in this research paper is: "*How can we effectively fuse the cyber-physical data generated in the grid to ensure situational awareness and detect not only cyber threats but also physical disturbances?*". We present a LSTM-based AE architecture that fills this gap. This architecture performs temporal-based cyber-physical data fusion, taking advantage of the model's intrinsic structural properties and using the fused data to detect threats in the electric grid with high accuracy.

## III. Electric Grid Testbed, Dataset & Threat Model

In this work, the dataset we used is an emulated version of the Western System Coordinating Council (WSCC) 9-bus model [18]. The emulation environment used to generate the cyber-physical dataset in this research consists of a real-time digital simulator (RTDS) that enables streaming C37.118 data from PMUs in the RTDS WSCC 9-bus model and SCEPTRE$^{TM}$, a Sandia National Laboratories industrial control system (ICS) emulation tool [19]. Specifically, SCEPTRE$^{TM}$ facilitates the creation of ICS cyber/control network models and the implementation of real communication protocols, such as DNP3 and Modbus.

The emulated scenario begins with a generator and line outage event, followed by a Denial-of-Service (DoS) attack which impedes the load-shedding signal issued by the control center. This results in an unstable system as defined by frequency instability, which includes both normal and abnormal cyber-physical data. The physical data, which are collected from 8 different phasor measurement units (PMUs) in the WSCC 9-bus model, include the following features: *frequency, per-phase voltage, and per-phase current*. The cyber data, which are collected from 3 different relays in each of the three substations, include the following features: *packet roundtrip times (RTTs) and packet retransmissions*. The total number of features that characterize the data is 111. It should be noted that the time resolution on the PMU physical data is once per 33 milliseconds, while the resolution on the cyber data is once per second. As far as the DoS attack is concerned, it targeted the substation located at bus number 6 and as a result the load shedding command is unable to be executed and protect the 9-bus model from the physical disturbance.

## IV. Data Fusion & Threat Detection with a LSTM-Based AE Model

### A. AE & LSTM Preliminaries

Threat detection is a fundamental task in ensuring the security and resilience of the grid that involves identifying abnormal patterns in input data. However, as the dimensionality of the input space increases, the complexity of the ML-based threat detection task also increases, which leads to poor generalization. Consequently, there is a growing interest in fusing the cyber-physical input space and dealing with the multimodality of the collected data to enhance the predictive

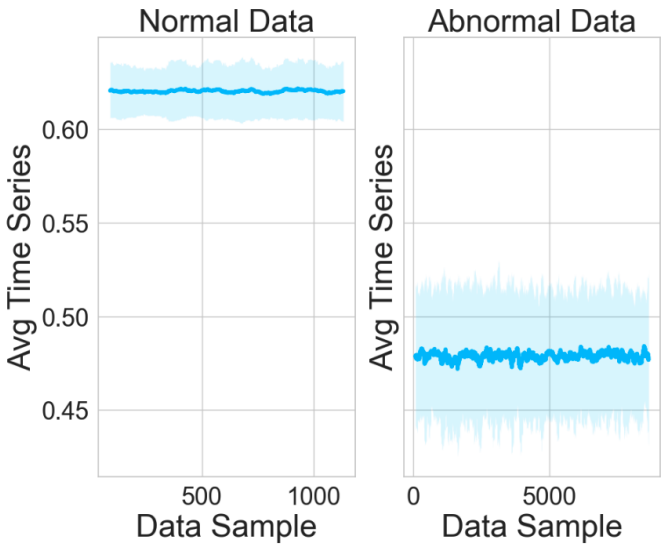


Fig. 2. Averaged normalized cyber-physical time series

performance of the classification models and provide situational awareness [20].

Autoencoders [21] represent one of the most fundamental data fusion techniques that can learn complex non-linear patterns in the data. They are artificial neural networks (ANN) whose structure is symmetrical consisting of an encoder and a decoder and fall in the category of unsupervised learning focusing on learning the optimal encoding-decoding scheme from data. Their symmetrical architecture is illustrated in Fig. 1. As data enters the AE, the encoder condenses it into a latent space, while the decoder expands the encoded representation back into the output layer. Subsequently, the reconstructed output is compared to the original data, and any discrepancies are back-propagated through the network to adjust the AE's weights. Specifically, given a set of input cyber-physical normal inputs $x = \{x_1, x_2, \ldots, x_t, \ldots\}$ from the WSCC 9-bus model, where $x_t \in \mathbb{R}^k$ denotes a $k$-dimensional vector of cyber-physical readings for $k$ features at time instance $t$ (e.g., RTT, voltage, frequency - see Section III), the encoder zips $x$ into a latent space $y = e(x) \in \mathbb{R}^n$, where $n$ is the reduced dimensionality of the latent space and $n < k$. Afterwards, the decoder reconstructs the latent space into the output $\hat{x} = d(y) \in \mathbb{R}^k$. The AE model is trained by minimizing the mean absolute error (MAE) of the reconstructed data as defined below:

$$MAE = \frac{1}{|x|} \sum_{x} ||x - \hat{x}|| \tag{1}$$

Additionally, we denote as $RE(x_i)$ the reconstruction error between the cyber-physical data vector $x_i$ and the reconstructed data vector $\hat{x_i}$, and it is formally defined below:

$$RE(x_i) = ||x_i - \hat{x_i}||, x_i \in x \tag{2}$$

Therefore, an AE is a perfect data-driven candidate model for cyber-physical data fusion in the grid, in terms of learning the most important features for threat detection.

However, plain AE might not be effective for processing time series data, e.g., cyber-physical data, where the temporal ordering of the data points is vital. LSTM-based AE, on the other hand, are a type of Recurrent Neural Networks (RNN) that can capture the temporal patterns in time series data. In particular, LSTM-based AE are composed of an encoder and a decoder, just like plain AE, but the encoder and decoder are built using RNN units instead of simple linear neural network layers [22]. The LSTM architecture enables memorizing past units and utilizing this memory to make predictions about future inputs. This makes the LSTM-based AE particularly effective for processing time series multimodal cyber-physical data. As a consequence, our methodology hinged on the intricate design and application of such a model (Fig. 1).

TABLE I
GRID-SEARCH VALUES THAT WERE USED FOR THE LSTM-BASED AE MODEL'S HYPERPARAMETERS OPTIMIZATION

| ***Hyperparameters*** | ***Grid-search values*** |
|---|---|
| Number of layers | [2, 3, 4] |
| Weight Decay | [0.01, 0.001, 0.0001, 0.00001] |
| Learning Rate | [0.1, 0.001, 0.0001] |
| Dropout Rate | [10%, 20%, 30%, 40%] |
| Batch Size | [32, 64, 128, 256, 512] |
| Optimizer | [Adam, Adadelta, Adagrad, SGD, RMSprop] |
| Latent Space Reduction | [35%, 55%, 75%] |

### *B. LSTM-Based AE Model's Specifics & Methodology*

The LSTM-based AE model is trained offline *only on the normal normalized cyber-physical data*, i.e., on data that was generated before the outages and DoS attack happened, trying to understand its inherent non-linear patterns and temporal dynamics and minimize the reconstruction error RE (Eq.2) between the encoder's input and decoder's output. Through this process, it learns how to perform cyber-physical data fusion and how to distill the salient temporal patterns into a low-dimensional information-rich representation.

The key idea of the cyber-physical threat detection lies on the exploitation of the RE metric, which quantifies the dissimilarity between the original and reconstructed data. Specifically, the higher the RE, the more pronounced the deviation from the normal data patterns; therefore, signifying a potential threat/anomaly in the electric grid. Thus, only after the model is optimized and fully trained, we analyze the reconstruction errors of the normal data points and find a threshold $th$ that indicates when a data point is normal or abnormal. In particular, the LSTM-based AE model learns how to fuse normal cyber-physical data into a lower-dimensional space and maintain the valuable insights at the same time. This results in the respective reconstruction errors being considerably lower than the ones of the abnormal data points, because the model never learned how to fuse and reconstruct data that include abnormalities (e.g., low/abnormal frequencies or high RTTs) during the training phase. Consequently, we can define a reconstruction error threshold $th$ that maximizes the

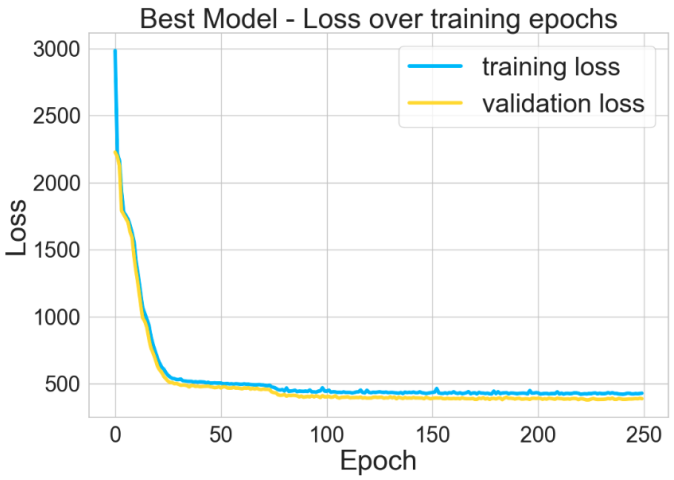


Fig. 3. Training & validation loss of the optimized LSTM-based AE model

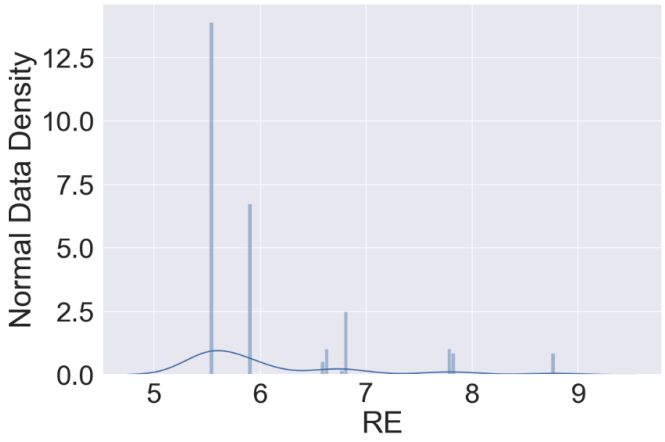


Fig. 4. Histogram of the reconstruction errors on the normal data of the trained LSTM-based AE model

reconstruction error distribution $d_x(RE)$ of the normal data points:

$$th = \arg\max_{RE} d_x(RE) \tag{3}$$

Finally, the trained LSTM-based AE can now operate as an effective cyber-physical binary classifier that determines if a new unseen data point $x_i'$ is abnormal based on the following rule:

$$Abormality(x_i') = \begin{cases} 1 & \text{if } RE(x_i') \geq th \\ 0 & \text{if } RE(x_i') < th \end{cases} \tag{4}$$

## V. Results

A detailed numerical evaluation is presented in this section in terms of both the LSTM-base AE model's offline training and online cyber-physical abnormality detection performance. The proposed framework's training and evaluation was conducted in a MacBook Pro M1 Laptop, with 16GB LPDDR3 RAM, and the PyTorch GPU functionality was used to perform distributed training [23].

Given the cyber-physical dataset that is described in Section III, we use $80\%$ for training and validating the developed LSTM-based AE model offline. Additionally, the remaining $20\%$ of the initial cyber-physical dataset is used as the test dataset to assess the accuracy of the trained model on unseen data and examine overfitting. However, we should note that the training and validation dataset is further split into $80\%$ for the actual training of the model, while the other $20\%$ will be used as a validation dataset during training for the hyperparameter optimization and fine-tuning of the model. To facilitate a smoother training process, the whole cyber-physical dataset was checked and scrubbed of any missing values. Also, each feature was translated individually such that it is in the range of $(0, 1)$ using the MinMaxScaler. In Fig. 2 we present an averaged version, i.e., smoothed out with one standard deviation on top and bottom of it, of a representative subset of the normalized cyber-physical data. The figure shows that the normal and abnormal data patterns differ distinctly. Specifically, the abnormal data is more noisy and has a higher standard deviation compared to the normal data, which should lead the trained LSTM-based AE model to capture these differences in the data and effectively perform threat detection through the data fusion process.

In order to determine the final LSTM-based AE model's architecture, a hyperparameters optimization via grid search was accomplished: we divided the domain of the hyperparameters that are used in the encoder and decoder into a discrete grid and afterwards by trying every combination of values in the grid we calculated both the MAE during training *on the normal data only* as well as the validation error. Specifically, in Table I, the hyperparameters that were optimized are presented: the a) number of layers in the encoder/decoder, b) weight decay, c) learning rate, d) dropout rate, e) batch size, f) pytorch optimizer, and e) the percentage of the initial feature space dimensionality reduction, i.e., the latent space reduction. After training the model for all the aforementioned combinations and observing the average training and validation loss in the last 50 epochs, i.e., when the model's training is converging, we selected the optimal hyperparameters which are highlighted with green color in the table. Fig. 3 shows the training and validation loss curves for the best hyperparameters, demonstrating a loss decrease and the convergence of the model. This also confirms the effectiveness of the training process on normal cyber-physical data and highlights the LSTM-based AE model's ability to learn and generalize well.

In Fig. 4 we present a histogram of the reconstruction errors on the *normal* data only of the optimized and trained LSTM-based AE model and we can discern that all of the errors values fall into the range of $(5, 9)$. This means that based on this reconstruction error distribution $d_x(RE)$, we can choose a value for the threshold, i.e., $th = 9$, which will drive the classification process for threat detection as described in Eq.4. Moreover, in Fig. 5 we show the histogram of the reconstruction errors on the *abnormal* data of the model, and we can clearly observe that the reconstruction errors values are much higher, i.e., in the range of $(30, 50)$. This is an expected behavior, since the LSTM-based AE model was

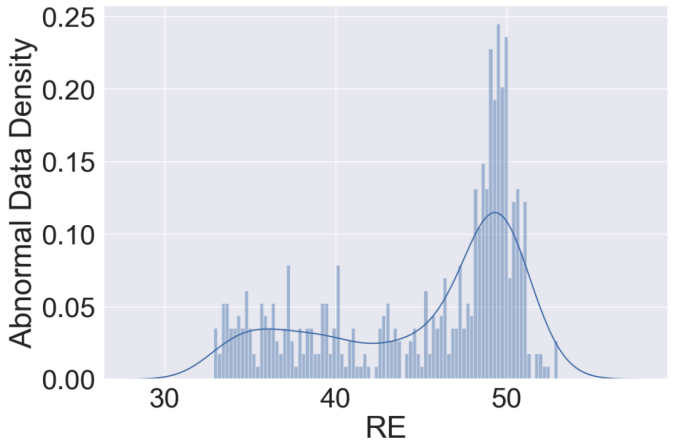


Fig. 5. Histogram of the reconstruction errors on the abnormal data of the trained LSTM-based AE model

trained on normal data only and as a result the previously unseen abnormal data patterns that exist in the dataset cause the model to perform an ineffective cyber-physical data fusion that is expressed with a high reconstruction error. However, this is actually the observation that helps the model to perform cyber-physical threat detection based on the value of the reconstruction error.

Fig. 6 illustrates two unseen normal cyber-physical data points (i.e., normal operating condition values) in the top row and two unseen abnormal ones (i.e., abnormal operating conditions values) in the bottom row, with the reconstruction error showing at the top of each panel. The blue line represents the original normalized feature values that were given to the trained model, whereas the orange line is what the model was able to reconstruct. It is obvious that the model is able to reconstruct almost perfectly the values of normal data points, whereas it shows a worse performance regarding the reconstruction of abnormal data points. Specifically, the abnormal data have an order of magnitude higher reconstruction error $RE$ than the one of the normal data points, i.e., $49.46$ vs $5.52$ and $48.07$ vs $6.63$. This difference between the reconstruction errors of the normal and abnormal data points enables the LSTM-based AE model to classify them accurately based on the chosen $th$ and Eq. 4.

In particular, the model achieved a $100\%$ accuracy in distinguishing normal from abnormal cyber-physical operating conditions, which highlights the potential of LSTM-based AE models in cyber-physical data fusion and threat detection in the electric grid for the protection of the critical infrastructure. Additionally, we followed the exact same methodology described in Section IV-B and developed cyber-only and physical-only models, which are trained only on cyber and physical data respectively. As a consequence, these two LSTM-based AE models can detect only cyber attacks, i.e., DoS attack, or physical disturbances correspondigly, i.e., generator and line outage event, correspondingly. In table II we present the accuracies for these different models as well as the average training and testing times. It is observed that the cyber-physical model has

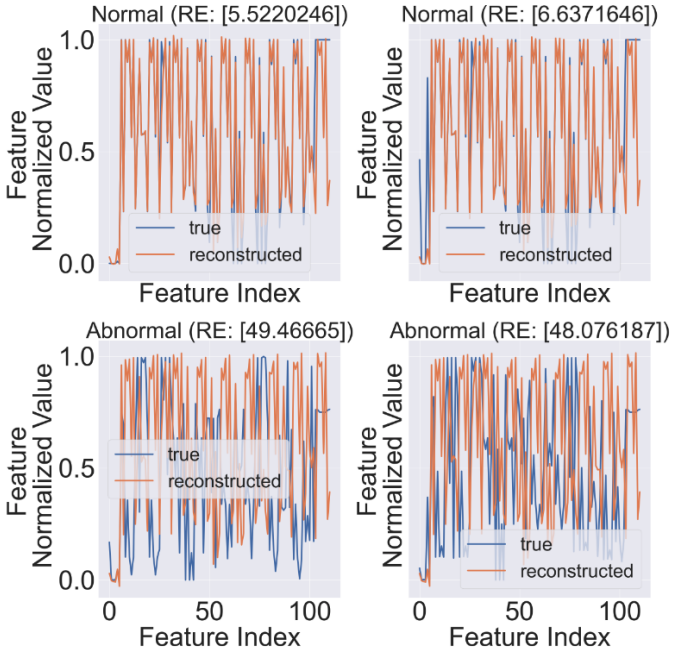


Fig. 6. LSTM-based AE model's feature input values, reconstructed feature values and errors for normal vs abnormal data

the highest/perfect accuracy among them, and this happens underlines the importance of cyber-physical data fusion in threat detection. Specifically, by fusing the cyber with the physical data, the model is able to facilitate the extraction and combination of salient features from high-dimensional data and map them into a lower-dimensional cyber-physical latent space, retaining at the same time the most crucial information and connections among the data. At this point, we should underline the fact that even in the case of the cyber-only and physical-only models, the threat detection is almost perfect, i.e., $96.19\%$ and $98\%$ respectively. Additionally, as far as the offline training time is concerned, the cyber-physical model takes the most time to be trained offline, because the number of features is the highest, i.e., $111$ features, and the data fusion is more complex. However, all the models are really fast when they are deployed online with less than $0.8$ second detection time.

## VI. Conclusion & Future Work

In this research work, we proposed a LSTM-based AE model for cyber-physical data fusion and threat detection in the electric grid. Specifically, we described the foundational theory behind LSTMs and AEs and we explained why a LSTM-based AE model can be particularly effective for processing and fusing time series multimodal cyber-physical data. Additionally, we formulated a methodology, based on which the model is optimized and trained only on the normal data, learns to effectively fuse and reconstruct cyber-physical data, and then a threshold that maximizes the reconstruction error distribution is chosen. After the model with the optimal hyperparameters is fully trained, it is deployed online in the

TABLE II
ACCURACY METRIC FOR THE CYBER-PHYSICAL, CYBER-ONLY, PHYSICAL-ONLY LSTM-BASED AE MODELS

| Model | Accuracy | Avg Training Time (∼10,000 data) | Avg Testing Time (1 data) |
|---|---|---|---|
| Cyber-Physical LSTM-based AE | 100% | ∼22 minutes | <0.8 sec |
| Cyber-only LSTM-based AE | 96.19% | ∼6 minutes | <0.4 sec |
| Physical-only LSTM-based AE | 98% | ∼17 minutes | <0.8 sec |

grid and performs threat detection through data fusion with perfect accuracy. A detailed numerical analysis is presented, as well as a comparative evaluation in terms of accuracy and time between the cyber-physical, cyber-only, and physical-only models.

Future work should investigate how the cyber-physical attack can be located within the grid via the per-feature reconstruction error as well as evaluating the combination of the LSTM-based AE model's learned latent space with other ML models, such as Random Forests, Single Value Decomposition, ARMA and others. Additionally, stealthier cyber-attacks, (e.g., man-in-the-middle or false data injection attack), where the cyber features will not contain a lot of information regarding these attacks, will be implemented and tested.

## REFERENCES


[1] F. E. White *et al.*, "Data fusion lexicon," *Joint Directors of Laboratories, Technical Panel for C*, vol. 3, p. 19, 1991.

[2] P. Cordeiro, A. Chavez, S. Hossain-McKenzie, A. Stenger, S. Bayless, R. Clark, S. Behrendt, J. Hawkins, and K. Davis, "Considerations for secure data exchange to achieve cyber-physical situational awareness in the electric grid," in *2023 IEEE Power and Energy Conference at Illinois (PECI)*, 2023, pp. 1–7.

[3] L. Xu, Q. Guo, Y. Sheng, S. Muyeen, and H. Sun, "On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective," *Renewable and Sustainable Energy Reviews*, vol. 152, p. 111642, 2021.

[4] J. Johnson, B. Fox, K. Kaur, and J. Anandan, "Evaluation of interoperable distributed energy resources to ieee 1547.1 using sunspec modbus, ieee 1815, and ieee 2030.5," *IEEE Access*, vol. 9, pp. 142 129–142 146, 2021.

[5] S. Hossain-McKenzie, N. Jacobs, A. Summers, B. Kolaczkowski, C. Goes, R. Fasano, Z. Mao, L. Al Homoud, K. Davis, and T. Overbye, "Harmonized automatic relay mitigation of nefarious intentional events (harmonie)-special protection scheme (sps)," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.

[6] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, "Electric power grid resilience to cyber adversaries: State of the art," *IEEE Access*, vol. 8, pp. 87 592–87 608, 2020.

[7] D. G. Photovoltaics and E. Storage, "Ieee standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE std*, vol. 1547, pp. 1547–2018, 2018.

[8] J. Johnson, C. B. Jones, A. Chavez, and S. Hossain-McKenzie, "Soar4der: security orchestration, automation, and response for distributed energy resources," in *Power Systems Cybersecurity: Methods, Concepts, and Best Practices*. Springer, 2023, pp. 387–411.

[9] S. Liu, Y. Zhang, S. Tian, Y. Fu, X. Su, and J. Shen, "A new method of data fusion with pmu and scada based on branch decomposition," in *2021 IEEE Sustainable Power and Energy Conference (iSPEC)*. IEEE, 2021, pp. 3982–3987.

[10] J. A. Massignan, J. B. London, M. Bessani, C. D. Maciel, R. Z. Fannucchi, and V. Miranda, "Bayesian inference approach for information fusion in distribution system state estimation," *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 526–540, 2021.

[11] M. Huang, Z. Wei, G. Sun, and H. Zang, "Hybrid state estimation for distribution systems with ami and scada measurements," *IEEE Access*, vol. 7, pp. 120 350–120 359, 2019.

[12] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of false data injection attacks in smart grid: A secure federated deep learning approach," *IEEE Transactions on Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022.

[13] M. Dehghani, T. Niknam, M. Ghiasi, N. Bayati, and M. Savaghebi, "Cyber-attack detection in dc microgrids based on deep machine learning and wavelet singular values approach," *Electronics*, vol. 10, no. 16, p. 1914, 2021.

[14] A. Sahu, Z. Mao, P. Wlazlo, H. Huang, K. Davis, A. Goulart, and S. Zonouz, "Multi-source multi-domain data fusion for cyberattack detection in power systems," *IEEE Access*, vol. 9, pp. 119 118–119 138, 2021.

[15] K. Saminathan, S. T. R. Mulka, S. Damodharan, R. Maheswar, and J. Lorincz, "An artificial neural network autoencoder for insider cyber security threat detection," *Future Internet*, vol. 15, no. 12, p. 373, 2023.

[16] V. Hnamte, H. Nhung-Nguyen, J. Hussain, and Y. Hwa-Kim, "A novel two-stage deep learning model for network intrusion detection: Lstm-ae," *IEEE Access*, 2023.

[17] T. Kim, J. Kim, and I. You, "An anomaly detection method based on multiple lstm-autoencoder models for in-vehicle network," *Electronics*, vol. 12, no. 17, p. 3543, 2023.

[18] A. Al-Hinai and M. Choudhry, "Voltage collapse prediction for interconnected power system," 10 2001.

[19] N. Jacobs, S. Hossain-McKenzie, S. Sun, E. Payne, A. Summers, L. Al-Homoud, A. Layton, K. Davis, and C. Goes, "Leveraging graph clustering techniques for cyber-physical system analysis to enhance disturbance characterisation," *IET Cyber-Physical Systems: Theory & Applications*, 2024.

[20] X. Wang, Y. Wang, J. Yang, X. Jia, L. Li, W. Ding, and F.-Y. Wang, "The survey on multi-source data fusion in cyber-physical-social systems: Foundational infrastructure for industrial metaverses and industries 5.0," *Information Fusion*, p. 102321, 2024.

[21] S. Chen and W. Guo, "Auto-encoders in deep learning—a review with new perspectives," *Mathematics*, vol. 11, no. 8, p. 1777, 2023.

[22] H. D. Nguyen, K. P. Tran, S. Thomassey, and M. Hamad, "Forecasting and anomaly detection approaches using lstm and lstm autoencoder techniques with the applications in supply chain management," *International Journal of Information Management*, vol. 57, p. 102282, 2021.

[23] A. Paszke, S. Gross, F. Massa, A. Lerer, J. Bradbury, G. Chanan, T. Killeen, Z. Lin, N. Gimelshein, L. Antiga *et al.*, "Pytorch: An imperative style, high-performance deep learning library," *Advances in neural information processing systems*, vol. 32, 2019.