ReAL: A New ResNet-ALSTM Based Intrusion Detection System for the Internet of Energy

Jiarui Song†, Beibei Li†, Yuhao Wu†, Yaxin Shi†, and Aohan Li‡
†College of Cybersecurity, Sichuan University, Chengdu, P.R. China 610065
‡Department of Electrical Engineering, Tokyo University of Science, Tokyo, Japan 162-8601
Email: libeibei@scu.edu.cn; {jiaruisong, wuyuhao, shiyaxin}@stu.scu.edu.cn; aohanli@ee.kagu.tus.ac.jp

2020 IEEE 45th Conference on Local Computer Networks (LCN) | 978-1-7281-7158-6/20/$31.00 ©2020 IEEE | DOI: 10.1109/LCN48667.2020.9314858

***Abstract*—The Internet of energy (IoE), envisioned to be a promising paradigm of the Internet of things (IoT), is characterized by the deep integration of various distributed energy systems. However, the fusion of heterogeneous IoE communication networks creates a new threat landscape. To thwart and mitigate various types of cyber threats to IoE networks, this paper proposes a novel intrusion detection system (IDS) based on a designed residual network with attention long short term memory (ReAL). Specifically, we design a light gradient boosting machine (LightGBM)-based feature selection method to identify the most useful features. Then, a residual network (ResNet) and a long short term memory neural network with an attention mechanism (ALSTM) are employed, to extract temporal patterns of network traffic events. After that, these patterns are orchestrated to identify the anomalies in IoE networks. The high effectiveness of the proposed IDS is validated on a real IoE dataset.**

***Index Terms*—Internet of energy (IoE), Internet of things (IoT), intrusion detection system (IDS), artificial intelligence**

I. Introduction

The Internet of energy (IoE) [1] is an emerging area in the Internet of things (IoT). It is defined as a networked system of various smart energy infrastructure components, including the control center, distributed renewable energy systems, decentralized energy storage, and energy consumers (e.g., industrial, commercial, and residential, etc.), as shown in Fig. 1. The vision of the IoE is to coordinate the existing distributed energy systems and, therefore, to optimize the energy efficiency of power generation, transmission, and consumption for all these energy systems [2].

Despite of these promising benefits, the IoE is facing an increasing number of cybersecurity challenges. The reason is that, the IoE integrates a line of heterogeneous and, possibly, vulnerable communication networks, making them desirable targets for attackers [3]. Besides, the widespread smart devices (e.g., smart meters, phasor measurement units, etc.), usually deployed in the fields where decent security protections are not often in place, create a lot of opportunities for malicious interceptions. In addition, the inherent vulnerabilities of legacy information technologies used in the traditional energy infrastructures, such as the supervisory control and data acquisition (SCADA) systems, may be exposed to the outside world without a hitch [4]. Unfortunately, the existing energy systems are not often equipped with advanced security protection solutions. It is, therefore, easy for powerful cyber attackers to bypass the existing security defenses. In this way, an effective intrusion detection system (IDS) against malicious penetrations is significantly demanded for the IoE.

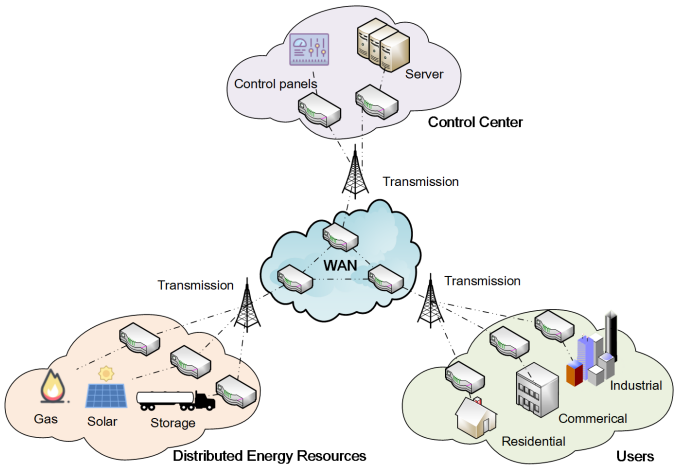

Fig. 1. The IoE infrastructure.

In this paper, we propose an effective IDS based on a **Re**sidual network with **A**ttention **L**ong short term memory (ReAL), to detect various types of cyberattacks on the IoE. Specifically, we conduct feature selection by using a designed light gradient boosting machine (LightGBM)-based method. Then, a residual network (ResNet) [5] and a long short term memory (LSTM) neural network [6] with an attention mechanism [7] are both employed to extract the temporal patterns of network traffic events. After that, the patterns are learned by the proposed ReAL model to identify the anomalies in IoE networks. The main contributions of this work are three-fold:

- First, a deep neural network is designed, called ReAL, by making use of the ResNet, the LSTM, and the attention mechanism, where temporal patterns of IoE network traffic events are effectively extracted and learned.
- Second, a novel feature selection method based on the LightGBM is also devised, which can reduce the dimension of features and, therefore, further improve the efficiency and accuracy of the proposed IDS.
- Last, we propose a ReAL-based IDS for the IoE, which is demonstrated on a real IoE dataset, and numerical results show that the proposed IDS is highly effective in detecting

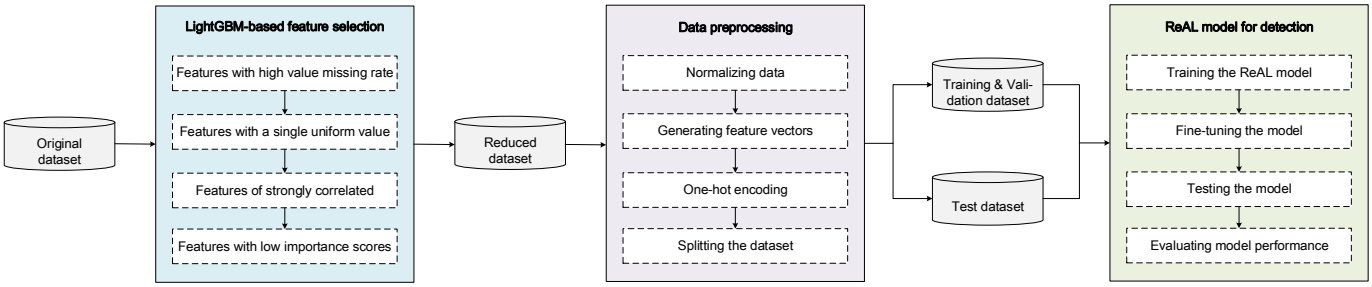

Fig. 2. The proposed ReAL-based IDS.

various cyber threats to the IoE and outperforms most of the existing IDSs.

The remainder of this paper is organized as follows. Section II reviews the recent studies on IDS techniques in IoE related areas. Section III elaborates on the proposed ReAL-based IDS, followed by the effectiveness and accuracy evaluation of the proposed IDS in Section IV. Finally, we draw our conclusions in Section V.

II. Related Work

In recent years, many researchers have presented their work focusing on IDS techniques in the IoT, power grids, etc., few work is undertaken on IoE. Moreover, most of state-of-the-art work placed priorities on machine learning- or deep learning-based intrusion detection approaches in recent years.

Machine learning-based approaches can handle high dimensional data. For example, in 2014, Nader *et al.* [8] investigated two types of machine learning-based one-class classification approaches for intrusion detection in SCADA systems. However, it can only detect one certain cyber threat. In 2018, Anton *et al.* [9] respectively used the support vector machine (SVM), random forest (RF), k-nearest neighbors (k-NN), and k-means clustering to identify malicious traffic events in a fictitious industrial scenario. Unfortunately, their model does not have good ability of generalization. In 2020, Rose *et al.* [10] presented a hybrid approach to detect attacks in IoE, which uses a combination of K-means and SVM. Nevertheless, the proposed IDS was not validated on a real IoE dataset.

Deep learning techniques are also a good candidate to develop IDSs, which can learn the inherent patterns of both the normal behavior and malicious behaviors, and is able to adaptively identify the anomalies. For instance, Yang *et al*. in 2014 [11] designed a knowledge-based multiattribute IDS using a heterogeneous whitelist and a protocol whitelist in smart grids. The weakness of this IDS is that it cannot detect potential attack operations, which exploit system vulnerabilities or conform to protocol specifications. In 2017, Aminanto *et al*. [12] proposed a sparse multi-layer auto encoders to detect cyber attacks in IoT networks. The fly in the ointment is that the classification model is not sufficient to deal with emerging attacks. In 2018, Kravchik *et al.* [13] utilized unsupervised convolutional neural networks (CNN) to detect cyber attacks in industrial control systems (ICSs). The limitation of their approach is that it can only identify naive attacks. We also notice that, in early 2020, Neha *et al* [14] presented a sine-cosine optimization based recurrent neural network (SCO-RNN) to detect cyber physical attacks against SCADA systems. The disadvantage is that this work does not reduce the dimension of the data, so the computational complexity of the model is relatively high.

III. The Proposed ReAL-Based IDS

In this section, we elaborate on the proposed IDS (see Fig. 2), which mainly comprises three phases: LightGBM-based feature selection, data preprocessing, and the ReAL for detection.

A. LightGBM-based Feature Selection

The network traffic data of the IoE, as well as most of the other IoT networks, are often imbalanced and heterogeneous. It is, therefore, necessary to remove unnecessary features prior to feeding them to the IDS model for cyber threats detection. In this work, we design a LightGBM-based feature selection method, which can effectively determine a set of features that is able to accelerate the training and detection phase of the proposed IDS, and also to optimize the detection accuracy. The designed LightGBM-based feature selection method is composed of four steps (see also in Algorithm 1):

- **Step 1**: Given an n-dimensional feature set, remove features having a value missing rate R^i_{miss} larger than a specified threshold R_{th}, where $i \in \mathcal{N} = \{1, 2, \cdots, n\}$.
- **Step 2**: Remove features with only a single uniform value.
- **Step 3**: Calculate the correlation coefficient $P^{i,j}_{corr}$ of each two features using the Pearson correlation coefficient, and identify the strongly correlated feature pairs with a correlation threshold of P_{th}. Then, remove one feature from each feature pair.
- **Step 4**: Measure the importance scores of all the features $\mathcal{I} = \{I_1, I_2, \cdots, I_m\}$ (m is the dimension of the reduced feature set), and order the features decreasingly as per their importance scores. Select the first k features and check the training accuracy of the IDS, until it no longer improves.

B. Data Preprocessing

Remove unnecessary columns of the IoE network traffic data, as per the reduced feature set $\mathcal{S}$. Then, a piece of traffic data vector is denoted by $\theta \in \mathbb{R}^k$ with a length k. To better suit the ReAL model, we normalize the data using the L_2 norm,

Algorithm 1 LightGBM-based Feature Selection

Input:

The full feature set $\mathcal{F} = \{F_1, F_2, \cdots, F_n\}$;
The threshold for value missing rate R_{th};
The threshold for feature correlation coefficient P_{th};
The feature importance score set $\mathcal{I}$.

Output:

A subset of features $\mathcal{S} \subseteq \mathcal{F}$;

Procedure:

Step 1:
for i in $\mathcal{N}$ **do**
  if $R^i_{miss} > R_{th}$ **then**
    $\mathcal{F} = \mathcal{F} \setminus \{F_i\}$.
  end if
end for

Step 2:
for i in $\mathcal{N}$ **do**
  if the i-th feature has only a uniform value **then**
    $\mathcal{F} = \mathcal{F} \setminus \{F_i\}$.
  end if
end for

Step 3:
for i in $\mathcal{N}$ **do**
  for j in $\mathcal{N}$ **do**
    if $P^{i,j}_{corr} > P_{th}$ **then**
      $\mathcal{F} = \mathcal{F} \setminus \{F_i\}$.
    end if
  end for
end for

Step 4:
Calculate $\mathcal{I}$=LightGBM($\mathcal{F}$), and order the features in $\mathcal{F}$ decreasingly as per their importance scores;
Select the first k features in $\mathcal{F}$, and calculate the training accuracy until it no longer improves;
$\mathcal{S} = \{F_1, F_2, \cdots, F_k\}$;
return $\mathcal{S}$.

without disrupting the linear relationship between the original data. The normalized traffic data vector $x \in \mathbb{R}^k$ (also called the feature vector) is given by

$$x_i = \frac{\theta_i}{\sqrt{\sum_{i=1}^{k} \theta_i^2}},\ i \in \{1, 2, \cdots, k\}. \tag{1}$$

Then, the label for each class in the given dataset is quantized to facilitate the one-hot encoding of the labels. After that, the dataset is split into training dataset, validation dataset, and test dataset.

C. The Novel ReAL Model for Intrusion Detection

In this part, we introduce the architecture of the proposed ReAL model and how it can be used to achieve intrusion detection.

1) The Architecture of ReAL Model: The proposed ReAL model is mainly composed by a ResNet module and an ALSTM (LSTM with an attention mechanism) module, followed by an MLP (multilayer perceptron) module, and then a softmax layer (see Fig. 3), which are respectively described as below:

- **ResNet module**: The ResNet module involves three residual blocks (ResBlock) and a global average pooling (GAP) layer. A residual block is composed of three convolutional blocks with a shortcut connection, and each convolutional block comprises a temporal convolutional layer, a batch normalization (BN) layer, and a ReLU activation function.
- **ALSTM module**: The ALSTM module is composed of two LSTM layers and an attention mechanism (used to focus on important features).
- **MLP module**: The MLP module involves a fully connected layer and a dropout layer. It is used to prevent the model from overfitting.
- **Softmax layer**: The softmax layer is exploited to map the non-normalized output of the MLP module to a probability distribution over predicted classes.

Given the network traffic feature vector x being the input, the ALSTM module and ResNet module process x in different ways. The ALSTM module regards a feature vector as a multivariate time series with a single time step, while the ResNet module treats a feature vector as a univariate time series with multiple time steps. Concretely, prior to the ALSTM module, a dimension shuffle layer is implemented, which transposes the temporal dimension of the feature vector. It is given by

$$\tilde{x} = \mathrm{Shuffle}(x). \tag{2}$$

Then, the ALSTM module processes $\tilde{x}$ in the following ways in purpose of extracting the temporal patterns:

$$\begin{aligned} \tilde{h_1} &= \mathrm{LSTM}_1(\tilde{x}) \\ \tilde{h_2} &= \mathrm{LSTM}_2(\tilde{h_1}) \\ \nu &= \mathrm{Attention}(\tilde{h_2}), \end{aligned} \tag{3}$$

where $\mathrm{LSTM}_i,\ i \in \{1, 2\}$, represents the i^{th} LSTM layer, Attention denotes the attention mechanism, $\tilde{h_1}$ and $\tilde{h_2}$ are two hidden vectors, and ν is the final output of the ALSTM module.

When it comes to the ResNet module, each residual block processes x by (taking the first residual block as an example)

$$\begin{aligned} h_1 &= \mathrm{ConvBlock}_1(x) \\ h_2 &= \mathrm{ConvBlock}_2(h_1) \\ h_3 &= \mathrm{ConvBlock}_3(h_2) \\ h' &= h_3 + x \\ y' &= \mathrm{ReLU}(h'), \end{aligned} \tag{4}$$

where the $\mathrm{ConvBlock}_i,\ i \in \{1, 2, 3\}$, represents the i-th convolutional block in the first residual block, $h_1, h_2, h_3 \in \mathbb{R}^k$ are hidden vectors, and h' is the hidden state after the shortcut connection and element-wise addition. After that, y' is delivered to the subsequent residual blocks. Then, the output of these residual blocks is transferred to the GAP layer in purpose of reducing the number of parameters, the result of which is μ.

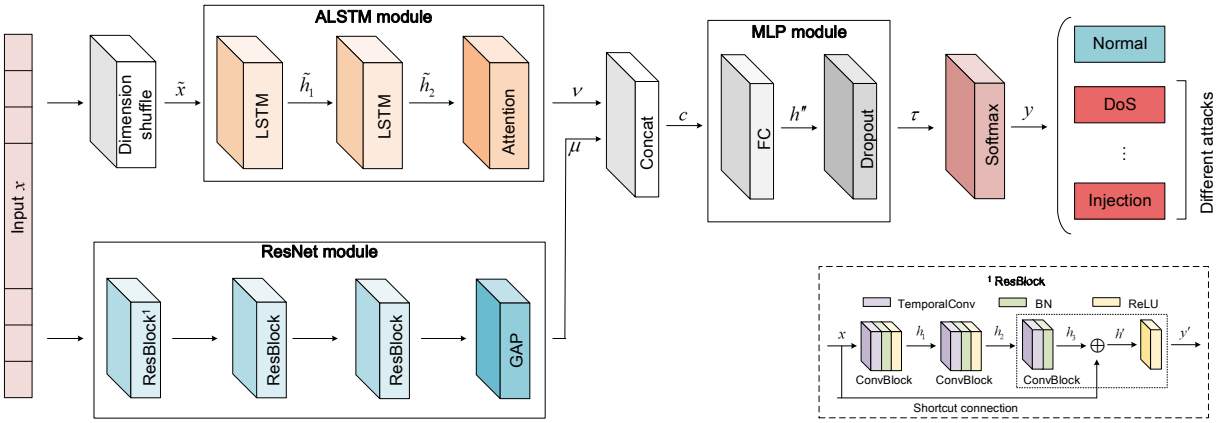

Fig. 3. The architecture of ReAL model.

Following the ResNet module and ALSTM module, μ and ν are concatenated and then fed into the MLP module, which is described by

$$\begin{aligned} c &= \mathrm{Concate}(\mu, \nu) \\ h'' &= \mathrm{FC}(c) \\ \tau &= \mathrm{Dropout}(h''), \end{aligned} \tag{5}$$

where $\mathrm{Concate}$ represents the concatenation operation, c is the concatenated result, FC and $\mathrm{Dropout}$ respectively denotes the fully connected layer and the Dropout layer, and h'' and τ is the output of the fully connected layer and the Dropout layer, respectively.

At last, the softmax layer provides the final classification result by

$$y = \mathrm{Softmax}(\tau), \tag{6}$$

where $\mathrm{Softmax}$ represents the softmax layer and y is the final classification result of the network traffic data.

2) Intrusion Detection Using ReAL Model: To detect cyber attacks using ReAL, the ReAL model needs to be trained first. In order to obtain the appropriate hyperparameters, we need to pre-train the model to adjust hyperparameters. Then formally train the model using these hyperparameters. After training, the model needs to be fine-tuned to achieve better performance. Finally, the best performing model can be used for intrusion detection, that is, to input the feature vectors of network traffic and output the detection results.

IV. Performance Evaluation

In this section, we evaluate the performance of the proposed ReAL-based IDS. The ReAL model is implemented using the Keras API[1], on a platform with an Intel Xeon E5-2618L v3 CPU and a NVIDIA GeForce RTX 2080TI GPU (64GB RAM). We conduct experiments not only on the proposed ReAL-based IDS but also on some widely used detection models, such as the SVM, linear regression (LR), MLP, LSTM, and CNN, etc. The settings of the hyperparameters used in our ReAL model, determined after a set of preliminary experiments, are shown in TABLE I.

[1]Keras: The Python deep learning library (http://keras.io/).

TABLE I
Hyperparameters Configuration

Configuration	***Value***
Optimization function	Adam
Epoch	100
Batch size	32
Learning rate	0.001
ReduceLROnPlateau	monitor='val_acc', factor=0.5, patience=10
EarlyStopping	monitor='val_acc', patience=20
ModelCheckpoint	monitor='val_acc', save_best_only=True

In the numerical results analysis, four metrics are taken into consideration to evaluate the performance of IDSs, i.e., the accuracy, precision, recall, and F1-score. Note that, the macro average is utilized to comprehensively evaluate the global performance of the IDSs. Each group of experiments are repeated ten times and the macro average results are presented.

A. Dataset Description

The gas pipeline system is one of the most significant energy systems in the IoE. In this paper, we use a real gas pipeline dataset [15] to evaluate the IDS performance. In this dataset, one class of network traffic data under normal operations and seven classes under various cyber attacks are respectively collected (see TABLE II). Each sample in this dataset contains 26 features (note that each dimension of network traffic data is defined as a feature) and 1 label. In our experiments, the dataset is randomly split into three parts, i.e., 80% for training, 10% for validation, and the remaining 10% for testing.

B. Numerical Results for Feature Selection

There are totally 26 features in the gas pipeline dataset. We use the designed feature selection method (as shown in Section III-A) to select the most important features for cyber attacks detection.

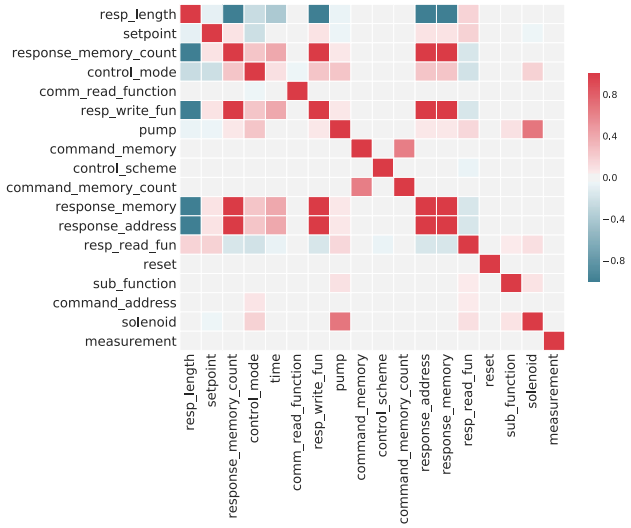

Fig. 4. The correlation matrix of features.

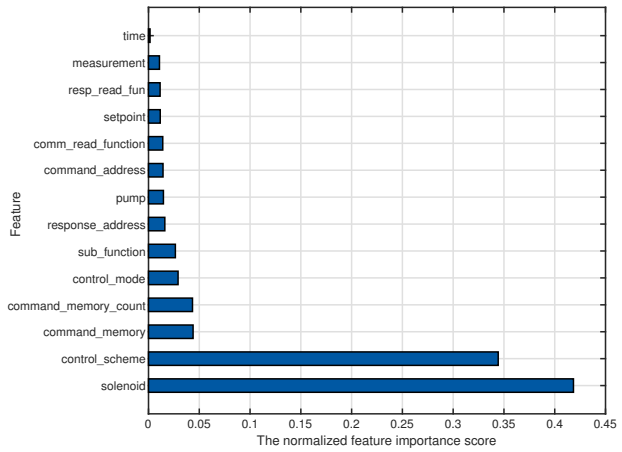

Fig. 5. The importance score of features.

- The threshold for the value missing rate R_{th} is 0.60;
- The threshold for the feature correlation coefficient H_{th} is set to 0.99.

In the first place, no features with a value missing rate greater than 0.60 are identified and then removed. Next, 8 features with a single unique value in the gas pipeline dataset are removed. In particular, they are: *crc_rate*, *cycletime*, *rate*, *comm_write_fun*, *deadband*, *reset*, *command_length*, *gain*. The correlation matrix of the remaining features is shown in Fig. 4. It can be seen that many features are strongly correlated. For feature pairs with strong correlation, we only keep one of them. Therefore, we remove four features, which are *response_memory*, *response_memory_count*, *resp_write_fun*, and *resp_length*. Last but not least, we use the LightGBM classifier to score the importance of the remaining features. The importance score of each feature is shown in Fig. 5. Based on importance scores, we explore the optimal number of features required by ReAL.

Figure 6 shows how the performance of ReAL varies with the number of features (i.e., the first k features). It is obvious that as the number of features ranges from 1 to 12, all metrics are steadily rising and most importantly, they all reach a peak when using the first 12 features, where the accuracy achieves 99.10%. Nevertheless, the performance suffered a slight decrease if more than 12 features are utilized, which means that features after the first 12 no longer contributes to the IDS performance any more. In this case, all the experiments thereafter are conducted using the first 12 features.

TABLE II
THE GAS PIPELINE DATASET DESCRIPTION

Label	***Amount***	***Description***
Normal	61156	Instance is not part of an attack
NMRI	2763	Naive malicious response injection
CMRI	15466	Complex malicious response injection
MSCI	782	Malicious state command injection
MPCI	7637	Malicious parameter command injection
MFCI	573	Malicious function command injection
DoS	1837	Denial-of-service attack
Reconnaissance	6805	Reconnaissance attack

TABLE III
THE PERFORMANCE OF REAL-BASED IDS FOR VARIOUS CYBER ATTACKS

Category	***Precision***	***Recall***	***F1-score***
NMRI	0.9593	0.9384	0.9487
CMRI	0.9904	0.9994	0.9949
MSCI	0.9610	0.9487	0.9548
MPCI	0.9728	0.9817	0.9772
MFCI	1.0000	0.9298	0.9636
DoS	1.0000	0.9946	0.9973
Reconnaissance	1.0000	0.9853	0.9926

C. Performance Comparison of IDS Models

In this part, we evaluate the performance of our ReAL-based IDS under various cyber attacks, and compare the results with other IDS models, including SVM, LR, MLP, CNN, and LSTM. It is worth noting that all detection models undertake experiments on the same training and test datasets with the best combination of features.

The performance of the ReAL-based IDS for various cyber attacks is illustrated in Table III. It can be seen that in the detection of CMRI, DoS and Reconnaissance, the proposed IDS has a higher F1-score. In the relatively small number of attacks in the dataset (NMRI, MSCI, MPCI, MFCI), the performance of the ReAL-based IDS is slightly worse. However, despite the class imbalance, the ReAL-base IDS has achieved excellent detection results. Figure 7 and Table IV show the numerical results of all the considered IDS models in terms of the accuracy, precision, recall, and F1-score. As can be easily seen that for each of the considered metrics, the proposed ReAL-based IDS achieves the best performance over all of the other IDS models. Therefore, it can be concluded that the proposed

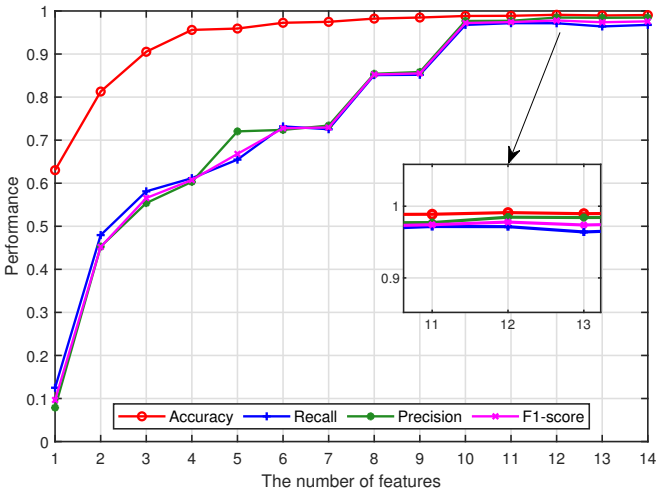

Fig. 6. The ReAL performance changes with the number of features.

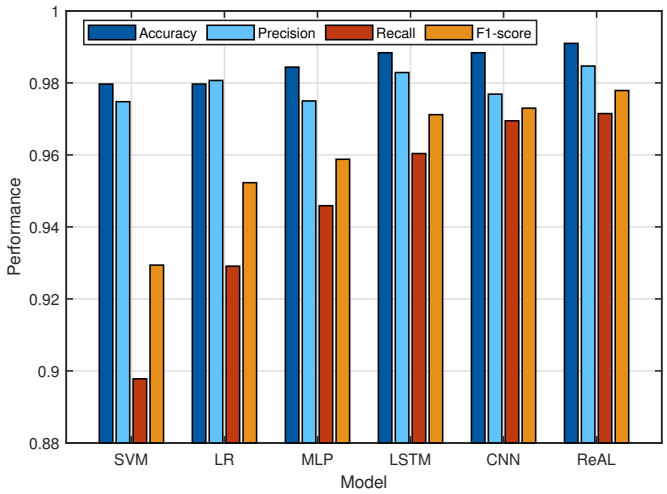

Fig. 7. Comparison between ReAL and other detection models.

TABLE IV
THE PERFORMANCE COMPARISON WITH OTHER DETECTION MODELS

Model	*Accuracy*	*Precision*	*Recall*	*F1-score*
LR	0.9797	0.9807	0.9291	0.9523
SVM	0.9797	0.9748	0.8978	0.9294
MLP	0.9844	0.9750	0.9460	0.9588
CNN	0.9884	0.9769	0.9695	0.9730
LSTM	0.9884	0.9829	0.9604	0.9712
ReAL	**0.9910**	**0.9847**	**0.9715**	**0.9779**

ReAL-based IDS can effectively detect various cyber attacks in IoE networks and outperforms many widely used IDS models.

V. Conclusion

In this paper, we have proposed a novel ReAL-based IDS for the IoE networks, which can achieve significantly high performance in detecting various cyber attacks against the IoE. More specifically, we designed a new LightGBM-based feature selection method to identify the most important features for intrusion detection. Also, both the ResNet and the LSTM with an attention mechanism were employed to extract the temporal patterns of IoE network traffic events. Importantly, these patterns were then orchestrated by a designed ReAL model for cyber attack detection. Extensive experiments on a real IoE dataset showed that, compared with some most widely used IDS models, the proposed ReAL-based IDS is superior in terms of the accuracy, precision, recall, and F1-score.

Future work will focus on more IoE datasets to further verify and tune our IDS model.

References

[1] N. Bui, A. P. Castellani, P. Casari, and M. Zorzi, "The Internet of energy: A web-enabled smart grid system," *IEEE Netw.*, vol. 26, pp. 39–45, July 2012.

[2] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng, S. Guo, Y. Xiang, and J. Wu, "A survey on energy Internet: Architecture, approach, and emerging technologies," *IEEE Syst. J.*, vol. 12, pp. 2403–2416, Sept. 2018.

[3] Q. Sun, Y. Zhang, H. He, D. Ma, and H. Zhang, "A novel energy function-based stability evaluation and nonlinear control approach for energy Internet," *IEEE Trans. Smart Grid*, vol. 8, pp. 1195–1210, May 2017.

[4] B. Li, Y. Wu, J. Song, R. Lu, T. Li, and L. Zhao, "DeepFed: Federated deep learning for intrusion detection in industrial cyber-physical systems," *IEEE Trans. Industr. Inform.*, 2020. DOI: 10.1109/TII.2020.3023430.

[5] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, June 2016, pp. 770-778.

[6] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Comput*, vol. 9, pp. 1735–1780, Nov. 1997.

[7] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," [Online]. Available: https://arxiv.org/abs/1409.0473.

[8] P. Nader, P. Honeine, and P. Beauseroy, "l_p-norms in one-class classification for intrusion detection in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 10, pp. 2308–2317, Nov. 2014.

[9] S. D. Anton, S. Kanoor, D. Fraunholz, and H. D. Schotten, "Evaluation of machine learning-based anomaly detection algorithms on an industrial Modbus/TCP data set," in *Proc. International Conference on Availability, Reliability and Security (ARES)*, Hamburg, Germany, Aug. 2018, pp. 1-9.

[10] T. Rose, K. Kifayat, S. Abbas, and M. Asim, "A hybrid anomaly-based intrusion detection system to improve time complexity in the Internet of energy environment," *J. Parallel Distrib. Comput.*, vol. 145, pp. 124–139, June 2020.

[11] Y. Yang, K. McLaughlin, S. Sezer, T. Littler, E. G. Im, B. Pranggono, and H. F. Wang, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans. Power Deliv.*, vol. 29, pp. 1092–1102, June 2014.

[12] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi impersonation detection," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, pp. 621–636, Mar. 2018.

[13] M. Kravchik and A. Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks," in *Proc. Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC)*, Toronto, ON, Canada, Oct. 2018, pp. 72-83.

[14] N. Neha, S. Priyanga, S. Seshan, R. Senthilnathan, and V. S. Sriram, "SCO-RNN: A behavioral-based intrusion detection approach for cyber physical attacks in SCADA systems," in *Proc. Inventive Communication and Computational Technologies (ICICCT)*, Namakkal, TN, India, Apr. 2019, pp. 911-919.

[15] T. Morris and W. Gao, "Industrial control system traffic data sets for intrusion detection research," in *Proc. International Conference on Critical Infrastructure Protection (ICCIP)*, Arlington, TX, USA, Mar. 2014, pp. 65-78.