Cluster Computing
https://doi.org/10.1007/s10586-022-03659-3

When explainable AI meets IoT applications for supervised learning

Youcef Djenouri[1] · Asma Belhadi[2] · Gautam Srivastava[3,4] · Jerry Chun-Wei Lin[5]

Received: 11 December 2021 / Revised: 10 April 2022 / Accepted: 17 June 2022
© The Author(s) 2022

Abstract

This paper introduces a novel and complete framework for solving different Internet of Things (IoT) applications, which explores eXplainable AI (XAI), deep learning, and evolutionary computation. The IoT data coming from different sensors is first converted into an image database using the Gamian angular field. The images are trained using VGG16, where XAI technology and hyper-parameter optimization are introduced. Thus, analyzing the impact of the different input values in the output and understanding the different weights of a deep learning model used in the learning process helps us to increase interpretation of the overall process of IoT systems. Extensive testing was conducted to demonstrate the performance of our developed model on two separate IoT datasets. Results show the efficiency of the proposed approach compared to the baseline approaches in terms of both runtime and accuracy.

Keywords XAI · Deep learning · IoT applications · Genetic algorithm

1 Introduction

The Internet of Things (IoT) has been largely used in the last decade in many instances from smart city applications to multimedia applications [16, 24, 30]. Various types of sensors deployed in IoT settings yields the generation of massive data that needs to be analyzed. Deep learning based solutions [1, 18, 32] performed well for solving IoT problems such as intrusion detection, and prediction. However, they suffer from two main challenges:

1. Hyper-parameter settings: the deep learning models provide various hyper-parameters that can be tuned such as the number of epochs, the activation function, the loss function, the number of batches, and so on. To achieve good performance of the deep learning models, we need to find the optimal values for the different hyper-parameters. Several strategies based on genetic algorithms have been developed in the literature to optimize the hyperparameters [3, 21, 31]. They transform the possible combinations of the hyperparameter values into the solution space and then intelligently explore the solution space with the goal of finding the best values of the hyperparameters that yield the best accuracy of the deep learning model.
2. Interpretation: Deep learning architectures are black box based models. These black-box models are created by a training algorithm directly from data, which means that humans, including those who develop them, have no idea how the factors are combined to produce the given results. Recently, a new class of artificial intelligence solutions has emerged called eXplainable Artificial Intelligence (XAI) [17, 29, 37]. It enables efficient mapping between input features and model results to make deep learning architectures understandable to industrial users.

✉ Jerry Chun-Wei Lin
jerrylin@ieee.org

Youcef Djenouri
Youcef.Djenouri@sintef.no

Asma Belhadi
asma.belhadi@kristiania.no

Gautam Srivastava
SRIVASTAVAG@brandonu.ca

[1] SINTEF Digital, Oslo, Norway

[2] Kristiania University College, Oslo, Norway

[3] Brandon University, Brandon, Canada

[4] China Medical University, Taichung, Taiwan

[5] Western Norway University of Applied Sciences, Bergen, Norway

Published online: 17 August 2022

This paper presents a new framework for handling IoT challenges. The framework explores different correlations among the features of sensor data, and then applies deep learning to learn both prediction, and intrusion detection tasks (the most challenging problems in IoT applications). In addition, XAI is used for better understanding the contribution of each feature in both the prediction, and the detection output. The main contributions of the presented work can be summarized as follows:

1. We propose an adapted Gamian angular strategy to convert the time series collected by the different sensors into visual features that can then be easily represented by a series of images. This allows us to adopt the promising VGG16 architecture to learn the various correlations of sensor data from a set of images.
2. We introduce XAI for IoT applications by analyzing the impact of input values on the output, understanding the different weights of the deep learning model used in the learning process, and calculating the contribution of each feature to the model output. This is done by studying the shape value and learning the deep architecture hyperparameters using the genetic algorithm.
3. We perform intensive experiments on two IoT collections for solving both prediction, and detection problems. According to a series of experiments, the designed method outperforms the baseline algorithms in both runtime and accuracy.

The following is the structure of the rest of the paper. An overview of the most commonly used intrusion detection and prediction methods are studied in Sect. 2. Our approach is described in detail in Sect. 3. Section 4 contains the performance evaluation. The paper is concluded in Sect. 5.

2 Related work

Intrusion detection is one of the challenging problems in IoT settings [15, 22]. Chaabouni et al. [6] study the existing solutions for intrusion detection from IoT data. It suggested an architecture of IoT system composed of perception, network, and application layers. It also surveys both traditional and deep learning works for intrusion detection. Wu et al. [38] deal with heterogeneity issue in IoT, and develop a federated learning based framework in cloud-edge system. The global model is trained by aggregating the local models. Alsaedi et al. [2] introduced a new dataset collection for both industrial internet of things for evaluating intrusion detection systems. It provides different anomalous events for various industrial platforms. The authors also evaluated the well-known machine and deep learning algorithms such as random forest [7], support vector machine [23], and long-short term memory [25] by selecting different views of the proposed dataset. Khraisat et al. [20] proposed a taxonomy of different intrusion detection systems applied on IoT environments. It considers algorithms based on deployment strategy whether the deployment is decentralized, distributed or hybrid. It also considers algorithms with different validation strategy, whether the validation is done by simulation, theoretical, or empirical. It groups the intrusion detection algorithms on supervised and unsupervised models, reinforcement based solutions, and deep learning based solutions. Ullah et al. [36] created a convolution neural network for detecting anomalies in IoT traffic data. The solution is able to identify outliers from 1D, 2D, and also 3D data. Transfer learning is also integrated by using a pre-trained convolution neural network based model for multi-classification problem

Prediction from the IoT data is also a challenging problem in recent decades [10, 42]. Dami et al. [9] predicted the arterial events captured in several months from IoT devices. The authors used the long short term memory with the deep belief network to learn the medical features. The data were periodically collected from wearable heart rate monitoring sensors, and stored as time series where the values are separated by 5 min timestamps. Xu et al. [39] developed prediction model for vehicular data deployed in IoT settings. The Elman neural network with the improved grey wolf optimization is investigated to ensure better solution exploration. The grey wolf optimization is integrated to derive the optimal parameters of the deep learning network used in the prediction process. Sharma et al. [34] predict the situation of COVID disease in Saudi Arabia from data captured by IoT devices. The novel system consists of the study of the IoT variation and the different kinds of symptoms for real COVID cases. Bhat et al. [5] studied the correlation between indoor and the outdoor sensors to predict the Asthma risk from IoT sensor data. The convolutional neural network is trained to learn the matching among both the indoor observation, the outdoor observation, and the prediction values.

However, the above algorithms ignore interpretation of the results and only focus on the model output. This reduces the deployment of such solutions in IoT settings. This paper explores and studies the XAI in both intrusion detection and prediction on IoT devices. The next section presents the new architecture and details about its main components.

3 XD-IoT-based framework

3.1 Principle

This section presents our XD-IoT (eXplainable Deep learning for Internet of Things) framework. The purpose is to first solve IoT problems using deep learning technologies and then to understand in detail of the various components that contribute greatly to IoT outputs. Both deep learning and XAI technologies are used to determine which features are involved in IoT outputs. As explained in Fig. 1, the process begins by collecting data from various IoT sensors. The extracted data is then converted into images using the Gramian angular field. Deep learning, specifically VGG16, is applied to the images created to solve IoT problems such as intrusion detection and flow prediction. Since VGG16 contains a large number of hyperparameters to be optimized, the genetic algorithm is used to find the best parameters of the VGG16 model. Explainability is introduced throughout the process by calculating the importance of each input function to the final output. In the remaining of this section, we show how to use all these concepts in the XD-IoT framework.

1. Gamian angular field: It is a strategy highly used to convert time series data to the set of images in a non-Cartesian system [19]. The sensor data can be viewed as a set of time series, where the time is set to the sensor acquisition period. The sensor is explored one by one and transformed to the images by considering the acquisition period as the pixel coordinates, and the sensor value as pixel value.
2. Deep learning: Our deep learning approach uses the images derived in the previous step, and learns the set of features. To learn the collection of IoT features, we employed VGG16. It is a well-known deep learning architectures highly used in many applications [8, 35, 41]. In order to extract the visual features from the generated images depending on the location of reference, VGG16 uses convolutional layers. Filters of window sizes 3, 5, and 7 are applied in parallel to input features in our network. Feature maps of three convolutional blocks are combined and fed successively to the 1024 and 256 neurons in the hidden Fully Connected (FC) layer. The `softmax` layer receives the output of the FC layer. Overfitting is countered by using dropout in both FC layers.
3. XAI: eXplainable AI (XAI) is introduced for IoT by analyzing the impact of the input values in the output and understanding the different weights of the deep learning models used in the learning process as:

    (a) *Variable Explanation*: The input IoT variables are analyzed by extracting visual features of the

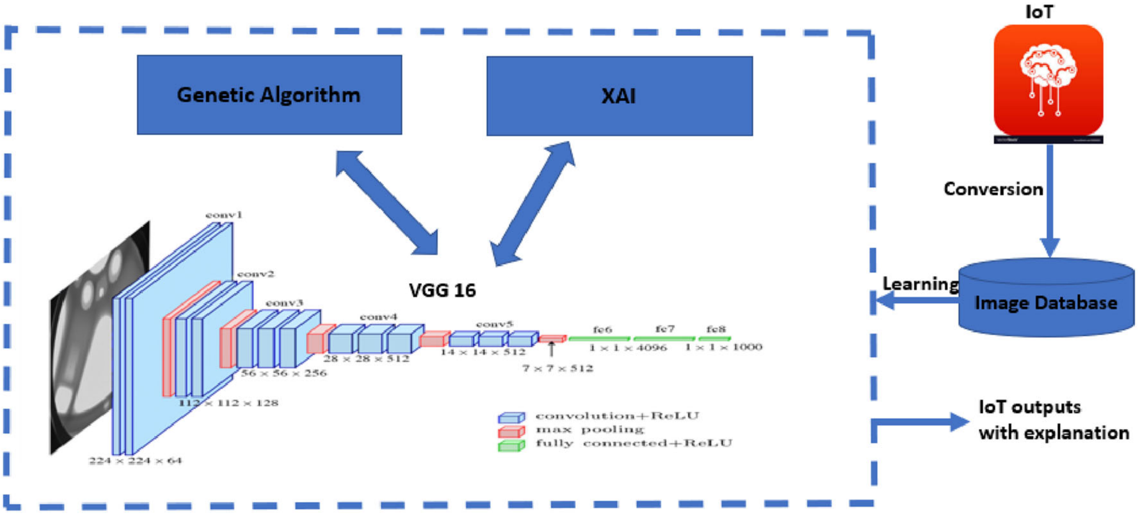


Fig. 1 Developed XDIoT Framework

users. Correlation between the extracted features from CNN, and the features trained by Word2-VEc is determined. The obtained correlation is transformed to the matrix, where it is fed it into the layers. The Shapely value is also applied on extracted features to compute the importance of each feature in the output [27].

(b) *Hyper-parameters-optimization*: The network generated requires high number of parameters to be fixed, such as the number of epochs, the learning rate, the activation functions of each layers, and the dropout rate. Therefore, an optimization strategy to set these parameters is needed. The genetic algorithm [12] is successfully applied for the hyper-parameter optimization in solving real world problems [13, 26]. Therefore, we adopt genetic algorithm in finding the optimal parameters of the learning architecture. The set of population is initialized, where each individual is represented by the set of values of each parameter of the learning architecture. Afterwards, the crossover, the mutation, and the selection operators are applied on the current population in order to generate more relevant individuals. The evaluation of each individual is determined using the fitness function. It calculates the accuracy of the generated results. This depends on the particular IoT problem. For example, if the problem is intrusion detection, the fitness function gives the number of intrusions correctly detected by the proposed system. This process is applied for a maximum number of generations iteratively until the termination criteria is achieved.

Algorithm 1 presents the pseudo-code of the developed XDIoT algorithm. The process starts by transforming the sensor data into an image database (lines 4–11). We scan all sensor data, for each value in the given sensor, we associate its value to 1, in its corresponding image. A deep learning model is designed by defining the convolution and max pooling operators. Afterwards, the genetic algorithm is applied to optimize the hyper-parameters of the deep learning model by performing the training phase on the transferred images. These two steps are then executed (lines 13-15). The prediction phase is then launched on the trained model in order to retrieve the IoT outputs (line 16), which highly depends on the problem. For instance, if we aim at solving the intrusion detection, the output will be the set abnormal behaviours retrieved from the IoT sensors. The XAI technology is finally performed to understand the mapping between the IoT features and the derived outputs (line 17). The output of the algorithm is the set of outputs O with their explanation O_{XAI}, which represent the contribution value of each input in the output (line 18).

Algorithm 1 XDIoT Algorithm

```
1: Input: $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_m\}$: the set of sensors.
2: Output: $< O, O_{XAI} >$: the set of the IoT outputs with their explainability.
3: ************Gamian Angular Field*****************
4: I $\leftarrow \emptyset$;
5: for $i$=1 to $m$ do
6:     for $j$=1 to $|Time(S_m)|$ do
7:         for $k$=1 to $|Values(S_j)|$ do
8:             $I \leftarrow I \cup Values(S_j)$;
9:         end for
10:    end for
11: end for
12: ************Deep Learning and XAI*****************
13: $Batches \leftarrow CreatingBatches(I)$;
14: $model \leftarrow VGG16()$;
15: $Hyper\_Param \leftarrow GA(fit(model, Batches))$;
16: $O \leftarrow Inference(S_{new}, model, Hyper\_Param)$;
17: $O_{XAI} \leftarrow XAI(S_{new}, O, model, Hyper\_Param)$;
18: return $< O, O_{XAI} >$.
```

4 Performance evaluation

4.1 Experimental environment

Extensive experiments have been carried out to evaluate the performance of the proposed approach using benchmark IoT collections targeting two use cases flow prediction, and intrusion detection. All algorithms have been implemented in Python 3.7 using Keras library for deep learning models. We also implement XAI library to visualize XAI output. The implemented library is based on Bioinfokit.[1] Both computational time and accuracy are calculated and evaluated in the experiments. The runtime is measured in seconds, and the accuracy is determined by *prediction rate* (PR) and intrusion detection rate (IR) measures, which are respectively defined as:

$$PR = \frac{CorrectedPredicted(\{S_i \in S_{test}\})}{|S_{test}|} \tag{1}$$

and,

$$IR = \frac{Detected(\{S_i \in S_{test}\})}{|S_{test}|}, \tag{2}$$

where $CorrectPredicted(\{S_i \in S_{test}\})$ is the number of corrected predicted sensor data in the testing sensors, and $Detected(\{S_i \in S_{test}\})$ is the number of corrected detected anomaly sensor data in the testing sensors.

Two IoT collections are used in the experiments as follows:

1. IPFlow [33]: It contains 87 features for flow generated by IoT network devices. It is collected over 6 days (April 26, 27, 28 and May 9, 11 and 15) of 2017. A total of 3, 577, 296 time series values are generated.
2. N-BaIoT [28]: This dataset deals with the IoT botnet anomalies. It contains data collected from 9 IoT sensor devices. It represents a set of 7, 062, 606 multivariate time series with 115 features.

The baseline algorithms used in these experiments are RNN-LF [4], and Tripres [40] for flow prediction, and kNN-TF [11], and LOF-TF [14] for intrusion detection, which are all the state-of-the-art models for comparisons.

4.2 Parameters setting

Intensive experiments have been carried to tune the best parameters using the genetic algorithm of XD-IoT. We varied the maximum number of iterations *IMAX*, and population size is set from 10 to 200, and the best values are given in Table 1. In the remaining experiments, the best parameters described in Table 1 are used.

4.3 XD-IoT versus state-of-the-art flow prediction solutions

This experiment compares the performance of XD-IoT with the baseline algorithms for solving the flow prediction problem, RNN-LF and Tripres, using the IPFFlow.

Figure 2 compares the runtime of XD-IoT with the baseline flow prediction algorithms by varying both the number of features and the number of time series values respectively. The results shows the superiority of XD-IoT against Tripres algorithm, and it is very competitive to the RNN-LF. By varying the percentage of features from 20 to 100%, the runtime of the proposed solution is less than the two baseline approaches, where a clear superiority against Tripres is observed. For instance, with 100% of features, the runtime of Tripres exceeds 4 seconds, whereas the runtime of XDP-IoT does not exceed 2 seconds. In addition, XD-HR outperforms RNN-LF when varying the number of features, and RNN-LF outperforms XD-IoT while varying the number of time series values. These results are achieved thanks to the efficient transformation, and deep learning pattern strategies used to predict the flow.

Figure 3 compares the accuracy of XD-IoT with the baseline flow prediction algorithms by varying both the number of features and the number of time series values respectively. By varying the percentage of features and the percentage of time series values from 20 to 100%, the prediction rate of the proposed solution is greater than the two baseline approaches. These results are achieved thanks to the use of the genetic algorithm for finding the optimal hyper-parameters of the deep learning architecture.

4.4 XD-IoT vs state-of-the-art intrusion detection solutions

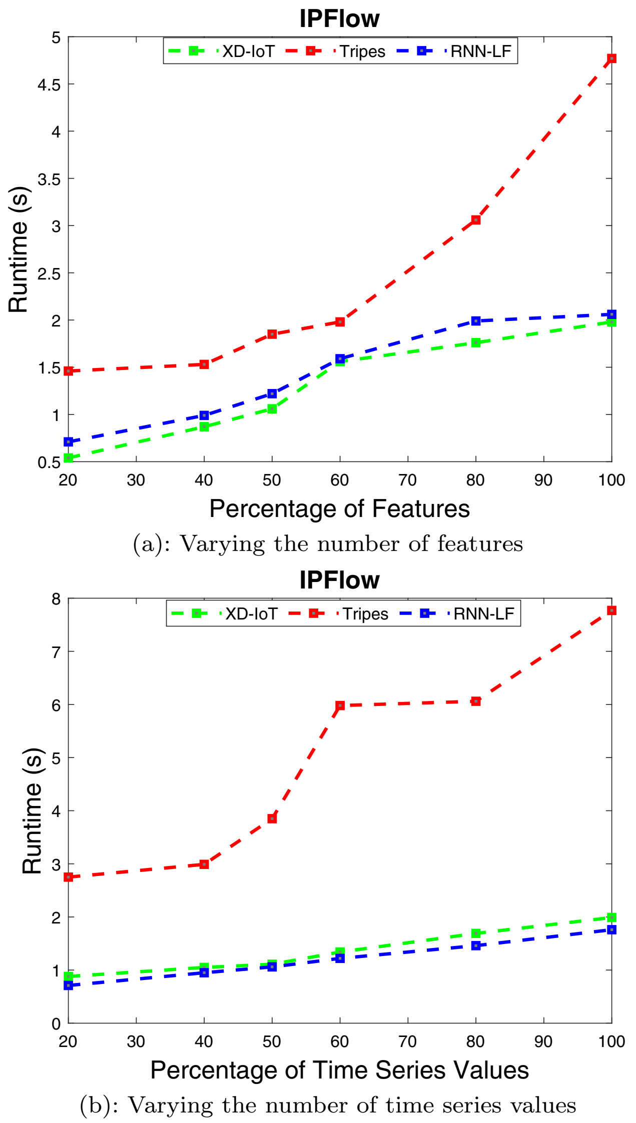
The next experiment aims at evaluating another XD-IoT problem, which is intrusion detection. The baseline algorithms are kNN-TF and LOF-TF for further comparisons.

Figures 4 and 5 compare both the runtime, and the accuracy of XD-IoT with the baseline intrusion detection algorithms by varying both the number of features and the

Table 1 Parameter setting of the genetic algorithm

IoT collection	Maximum number of iteration *IMAX*	The population size |*P*|
IPFlow	86	140
N-BaIoT	45	165

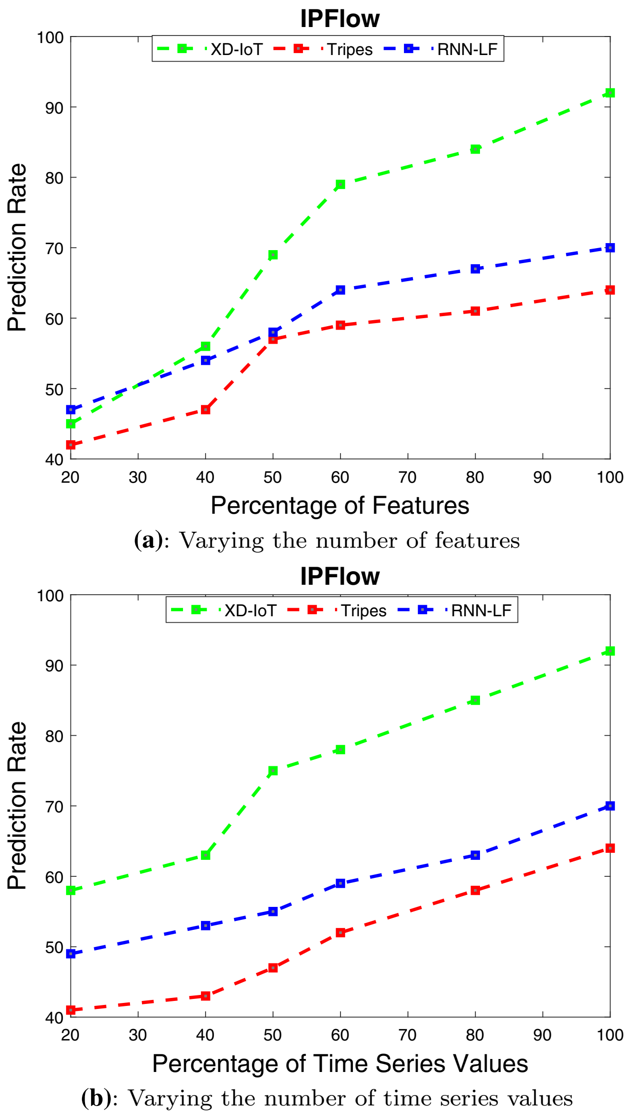
[1] https://github.com/reneshbedre/bioinfokit.



(a): Varying the number of features

(b): Varying the number of time series values

Fig. 2 XD-IoT versus State-of-the-art Flow Prediction Solution: Runtime



(a): Varying the number of features

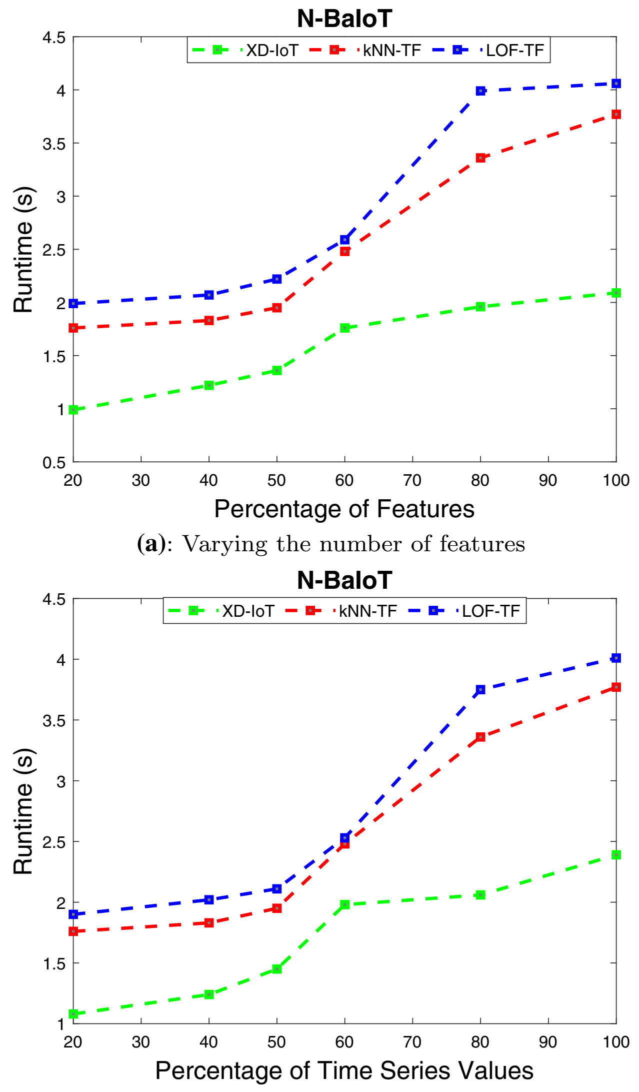
(b): Varying the number of time series values

Fig. 3 XD-IoT vs state-of-the-art flow prediction solution: accuracy

number of time series values respectively. The results show that the XD-IoT algorithm outperforms both baseline algorithms in terms of runtime and accuracy. These results confirmed again the applicability of the developed XD-IoT for solving IoT applications.

4.5 Explainibility

The last experiment aims to show the interpretation of key results obtained by the XAI process. Both prediction and detection have been performed, and the importance of each input feature is determined. Figures 6 and 7 present the results of the XAI tool developed in the XD-IoT framework. In Fig. 6, our XAI tool is able to visualize the importance of 20 input features collected from the six selected IoT sensors of the IPFlow data, and in Fig. 7, our XAI tool is able to visualize the importance of 50 input features collected from six selected IoT sensors of the N-BaIoT data. These results show that the contribution of the features varied from prediction task to detection task. For instance, 20 important features are identified for the

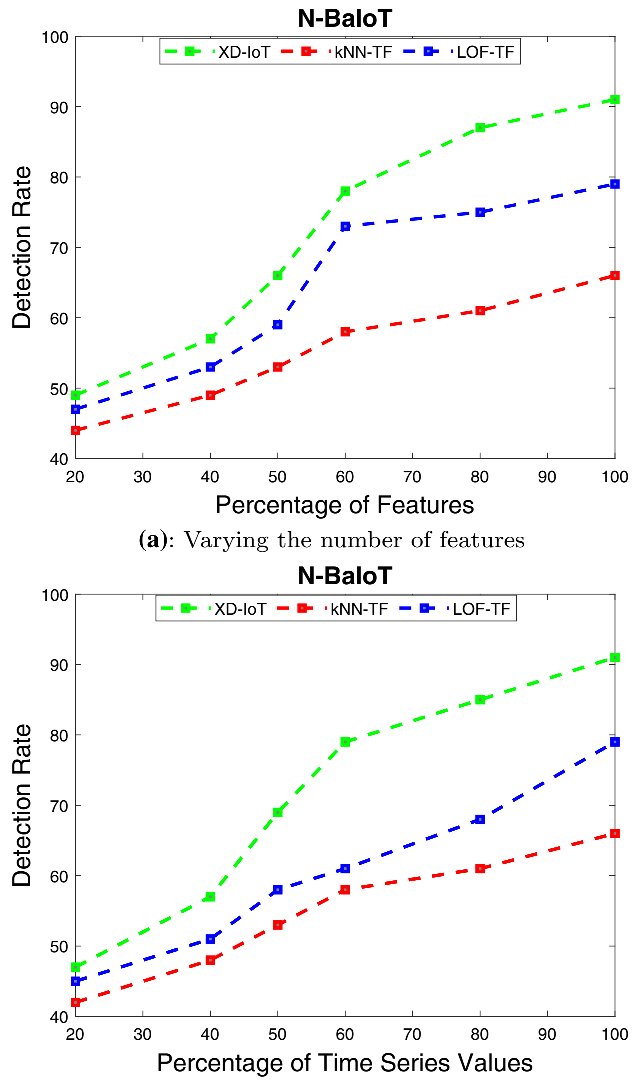


(a): Varying the number of features

(b): Varying the number of time series values

Fig. 4 XD-IoT vs state-of-the-art intrusion detection solution: runtime

prediction task where 50 features are derived for the detection task. This reveals that the detection task in IoT is much more complicated than the prediction task. Thus, the security issue in IoT is much more challenging than prediction. From these results, we encourage companies and stakeholders to investigate more on security and privacy issues for IoT sensor devices.



(a): Varying the number of features

(b): Varying the number of time series values

Fig. 5 XD-IoT vs state-of-the-art intrusion detection solution: accuracy

5 Conclusion and future work

In this paper, we propose a novel approach that not only processes IoT data using deep learning models, but also improves the interpretation of the results. Initially, IoT data is collected from various sensors. To efficiently process IoT data, the Gamian angular field is used to transform the

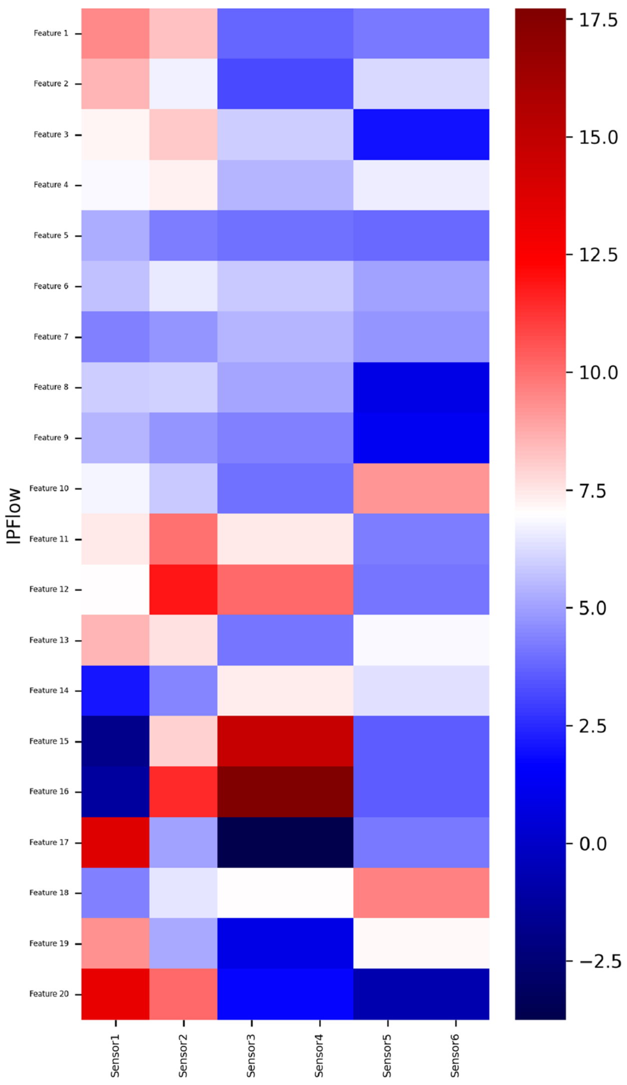


Fig. 6 XD-IoT: explainability on IPFlow

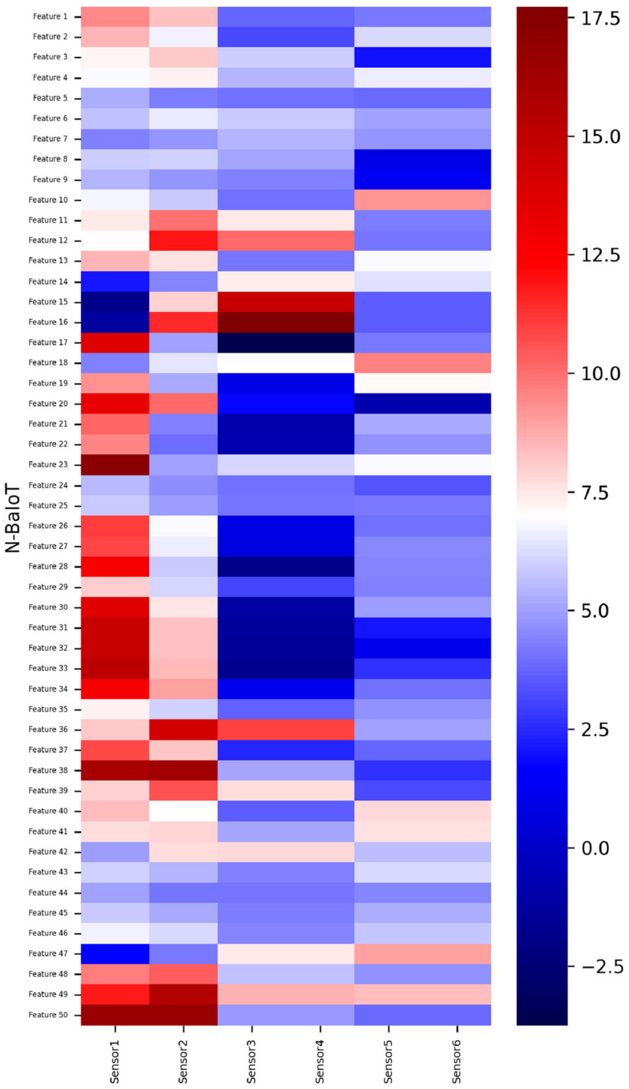


Fig. 7 XD-IoT: explainability on N-BaIoT

signal data into a set of images. The latter are trained by a VGG16 model that incorporates XAI, and hyperparameter optimization. Extensive experiments have been conducted to thoroughly demonstrate the usefulness of our method in two different use cases such as stream prediction and intrusion detection. The experimental results show the efficiency of the proposed approach compared to the baseline approaches in terms of both runtime and accuracy. In the future, we plan to investigate the processing of signals represented by time series data. Therefore, the use of a recurrent neural network with an attention mechanism for processing time series data is crucial. Another perspective of this research is to investigate other genetic algorithms for hyperparameter optimization. Optimizing the shapely value of the whole XAI process is also on our future agenda.

Author contributions YD handles the conceptualization and writing—original draft; AB handles formal analysis; GS handles writing—review & editing; and JC-WL handles conceptualization, writing—review & editing, and investigation.

Funding Open access funding provided by Western Norway University Of Applied Sciences. This research was supported by the Western Norway University of Applied Sciences, Bergen, Norway.

Data availibility The used data in the experiments can be accessed from https://github.com/reneshbedre/bioinfokit.

Declarations

Conflict of interest The authors declare that there are no conflicts of interest in this paper.

Ethical approval This article does not contain any studies with human participants performed by any of the authors.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Abbasi, J.S., Bashir, F., Qureshi, K.N., ul Islam, M.N., Jeon, G.: Deep learning-based feature extraction and optimizing pattern matching for intrusion detection using finite state machine. Comput. Electr. Eng. **92**, 107094 (2021)
2. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A.: Ton_IoT telemetry dataset: a new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access **8**, 165130–165150 (2020)
3. Balaha, H.M., Saif, M., Tamer, A., Abdelhay, E.H.: Hybrid deep learning and genetic algorithms approach (HMB-DLGAHA) for the early ultrasound diagnoses of breast cancer. Neural Comput. Appl. **34**, 8671–8695 (2022)
4. Belhadi, A., Djenouri, Y., Djenouri, D., Lin, J.C.W.: A recurrent neural network for urban long-term traffic flow forecasting. Appl. Intell. **50**, 3252–3265 (2020)
5. Bhat, G.S., Shankar, N., Kim, D., Song, D.J., Seo, S., Panahi, I.M., Tamil, L.: Machine learning-based asthma risk prediction using IoT and smartphone applications. IEEE Access **9**, 118708–118715 (2021)
6. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutor. **21**(3), 2671–2701 (2019)
7. Chen, Y., Zheng, W., Li, W., Huang, Y.: Large group activity security risk assessment and risk early warning based on random forest algorithm. Pattern Recognit. Lett. **144**, 1–5 (2021)
8. Choi, H., Yang, H., Lee, S., Seong, W.: Type/position classification of inter-floor noise in residential buildings with a single microphone via supervised learning. In: 2020 28th European signal processing conference (EUSIPCO), pp. 86–90. IEEE (2021)
9. Dami, S., Yahaghizadeh, M.: Predicting cardiovascular events with deep learning approach in the context of the internet of things. Neural Comput. Appl. **33**, 7979–7996 (2021)
10. Delnevo, G., Girau, R., Ceccarini, C., Prandi, C.: A deep learning and social IoT approach for plants disease prediction toward a sustainable agriculture. IEEE Internet Things J. **9**, 7243–7250 (2021)
11. Djenouri, Y., Belhadi, A., Lin, J.C.W., Cano, A.: Adapted k-nearest neighbors for detecting anomalies on spatio-temporal traffic flow. IEEE Access **7**, 10015–10027 (2019)
12. Djenouri, Y., Comuzzi, M.: Combining apriori heuristic and bio-inspired algorithms for solving the frequent itemsets mining problem. Inf. Sci. **420**, 1–15 (2017)
13. Djenouri, Y., Srivastava, G., Lin, J.C.W.: Fast and accurate convolution neural network for detecting manufacturing data. IEEE Trans. Ind. Inform. **17**(4), 2947–2955 (2020)
14. Djenouri, Y., Zimek, A., Chiarandini, M.: Outlier detection in urban traffic flow distributions. In: 2018 IEEE international conference on data mining (ICDM), pp. 935–940. IEEE (2018)
15. Ge, M., Syed, N.F., Fu, X., Baig, Z., Robles-Kelly, A.: Towards a deep learning-driven intrusion detection approach for internet of things. Comput. Netw. **186**, 107784 (2021)
16. Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S.: Recent security trends in internet of things: A comprehensive survey. IEEE Access (2021)
17. Ivanovs, M., Kadikis, R., Ozols, K.: Perturbation-based methods for explaining deep neural networks: a survey. Pattern Recognit. Lett. **150**, 228–234 (2021)
18. Jan, B., Farman, H., Khan, M., Imran, M., Islam, I.U., Ahmad, A., Ali, S., Jeon, G.: Deep learning in big data analytics: a comparative study. Comput. Electr. Eng. **75**, 275–287 (2019)
19. Kan, C.N.E., Povinelli, R.J., Ye, D.H.: Enhancing multi-channel eeg classification with gramian temporal generative adversarial networks. In: ICASSP 2021-2021 IEEE international conference on acoustics, speech and signal processing (ICASSP), pp. 1260–1264. IEEE (2021)
20. Khraisat, A., Alazab, A.: A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity **4**(1), 1–27 (2021)
21. Kilicarslan, S., Celik, M., Sahin, Ş: Hybrid models based on genetic algorithm and deep learning algorithms for nutritional anemia disease classification. Biomed. Signal Process. Control **63**, 102231 (2021)
22. Kumar, V., Das, A.K., Sinha, D.: Uids: a unified intrusion detection system for IoT environment. Evolut. Intell. **14**(1), 47–59 (2021)
23. Le, D.N., Parvathy, V.S., Gupta, D., Khanna, A., Rodrigues, J.J., Shankar, K.: IoT enabled depthwise separable convolution neural network with deep support vector machine for covid-19 diagnosis and classification. Int. J. Mach. Learn. Cybern. **12**(11), 3235–3248 (2021)
24. Li, S., Da Xu, L., Zhao, S.: The internet of things: a survey. Inf. Syst. Front. **17**(2), 243–259 (2015)
25. Lin, J.C.W., Shao, Y., Djenouri, Y., Yun, U.: ASRNN: a recurrent neural network with an attention model for sequence labeling. Knowl.-Based Syst. **212**, 106548 (2021)
26. Lin, J.C.W., Srivastava, G., Zhang, Y., Djenouri, Y., Aloqaily, M.: Privacy-preserving multiobjective sanitization model in 6g IoT environments. IEEE Internet Things J. **8**(7), 5340–5349 (2020)

27. Ma, S., Tourani, R.: Predictive and causal implications of using shapley value for model interpretation. In: Proceedings of the 2020 KDD workshop on causal discovery, pp. 23–38. PMLR (2020)
28. Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., Elovici, Y.: N-baiot: network-based detection of iot botnet attacks using deep autoencoders. IEEE Pervasive Comput. **17**(3), 12–22 (2018)
29. Mohseni, S., Zarei, N., Ragan, E.D.: A multidisciplinary survey and framework for design and evaluation of explainable AI systems. ACM Trans. Interact. Intell. Syst. (TiiS) **11**(3–4), 1–45 (2021)
30. Nauman, A., Qadri, Y.A., Amjad, M., Zikria, Y.B., Afzal, M.K., Kim, S.W.: Multimedia internet of things: a comprehensive survey. IEEE Access **8**, 8202–8250 (2020)
31. Pan, Y., Yang, Y., Li, W.: A deep learning trained by genetic algorithm to improve the efficiency of path planning for data collection with multi-uav. IEEE Access **9**, 7994–8005 (2021)
32. Prates, R.M., Cruz, R., Marotta, A.P., Ramos, R.P., Simas Filho, E.F., Cardoso, J.S.: Insulator visual non-conformity detection in overhead power distribution lines using deep learning. Comput. Electr. Eng. **78**, 343–355 (2019)
33. Rojas, J.S., Pekar, A., Rendón, Á., Corrales, J.C.: Smart user consumption profiling: incremental learning-based ott service degradation. IEEE Access **8**, 207426–207442 (2020)
34. Sharma, S.K., Ahmed, S.S.: Iot-based analysis for controlling & spreading prediction of covid-19 in Saudi Arabia. Soft Comput. **25**, 12551–12563 (2021)
35. Sundararajan, K., Woodard, D.L.: Deep learning for biometrics: a survey. ACM Comput. Surv. (CSUR) **51**(3), 1–34 (2018)
36. Ullah, I., Mahmoud, Q.H.: Design and development of a deep learning-based model for anomaly detection in iot networks. IEEE Access **9**, 103906–103926 (2021)
37. Vassiliades, A., Bassiliades, N., Patkos, T.: Argumentation and explainable artificial intelligence: a survey. Knowl. Eng. Rev. (2021). https://doi.org/10.1017/S0269888921000011
38. Wu, Q., He, K., Chen, X.: Personalized federated learning for intelligent iot applications: a cloud-edge based framework. IEEE Open J. Comput. Soc. **1**, 35–44 (2020)
39. Xu, L., Yu, X., Gulliver, T.A.: Intelligent outage probability prediction for mobile iot networks based on an igwo-elman neural network. IEEE Trans. Veh. Technol. **70**(2), 1365–1375 (2021)
40. Xu, X., Fang, Z., Qi, L., Zhang, X., He, Q., Zhou, X.: Tripres: traffic flow prediction driven resource reservation for multimedia iov with edge computing. ACM Trans. Multimed. Comput. Commun. Appl. (TOMM) **17**(2), 1–21 (2021)
41. Zhang, M., Zhou, Y., Zhao, J., Man, Y., Liu, B., Yao, R.: A survey of semi-and weakly supervised semantic segmentation of images. Artif. Intell. Rev. **53**(6), 4259–4288 (2020)
42. Zhang, Y., Pan, J., Qi, L., He, Q.: Privacy-preserving quality prediction for edge-based iot services. Future Gener. Comput. Syst. **114**, 336–348 (2021)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Youcef Djenouri obtained the PhD in Computer Engineering from the University of Science and Technology USTHB, Algiers, Algeria, in 2014. He is currently a research scientist at SINTEF Digital in Oslo, Norway. He is working on topics related to artificial intelligence and data mining, with focus on association rules mining, frequent itemsets mining, parallel computing, swarm and evolutionary algorithms and pruning association rules. Dr. Djenouri has published more than 70 refereed research papers, in the areas of data mining, parallel computing and artificial intelligence.

Asma Belhadi obtained the PhD in Computer Engineering from the University of Science and Technology USTHB Algiers, Algeria, in 2016. She is a postdoctoral researcher at Kristiania University College in Oslo, Norway. She is working on topics related to artificial intelligence and data mining, with focus on logic programming. Dr. Belhadi has published over 25 refereed research articles in the areas of artificial intelligence, and smart city applications.

Gautam Srivastava was awarded his B.Sc. degree from Briar Cliff University in the U.S.A. in the year 2004, followed by his M.Sc. and Ph.D. degrees from the University of Victoria in Victoria, British Columbia, Canada in the years 2006 and 2012, respectively. Dr. G, as he is popularly known, is active in research in the field of Cryptography, Data Mining, Security and Privacy, and Blockchain Technology. In his 5 years as a research academic, he has published a total of 90 papers in high-impact conferences in many countries and in high-status journals (SCI, SCIE). He is an IEEE Senior Member.

Jerry Chun-Wei Lin received his Ph.D. in Computer Science and Information Engineering from National Cheng Kung University, Tainan, Taiwan, in 2010. He is now working as a full Professor at the Department of Computer Science, Electrical Engineering and Mathematical Sciences, Western Norway University of Applied Sciences, Bergen, Norway. His research interests include data mining, privacy-preserving and security, Big Data analytics, and social networks. He has published more than 350 research papers in peer-reviewed international conferences and journals. He is the Senior Member of both IEEE and ACM, and also the Fellow of IET (FIET).