Network Anomaly Detection using Federated Learning for the Internet of Things

Ana Cholakoska
Ss. Cyril and Methodius University in Skopje
Faculty of Electrical Engineering and Information Technologies
Skopje, North Macedonia
acholak@feit.ukim.edu.mk

Bojan Jakimovski
Ss. Cyril and Methodius University in Skopje
Faculty of Electrical Engineering and Information Technologies
Skopje, North Macedonia
kti1562018@feit.ukim.edu.mk

Bjarne Pfitzner
Hasso Plattner Institute
Digital Health — Connected Healthcare
Potsdam, Germany
bjarne.pfitzner@hpi.de

Hristijan Gjoreski
Ss. Cyril and Methodius University in Skopje
Faculty of Electrical Engineering and Information Technologies
Skopje, North Macedonia
hristijang@feit.ukim.edu.mk

Bert Arnrich
Hasso Plattner Institute
Digital Health — Connected Healthcare
Potsdam, Germany
bert.arnrich@hpi.de

Marija Kalendar
Ss. Cyril and Methodius University in Skopje
Faculty of Electrical Engineering and Information Technologies
Skopje, North Macedonia
marijaka@feit.ukim.edu.mk

Danijela Efnusheva
Ss. Cyril and Methodius University in Skopje
Faculty of Electrical Engineering and Information Technologies
Skopje, North Macedonia
danijela@feit.ukim.edu.mk

ABSTRACT

The widespread use of IoT devices has contributed greatly to the continuous digitisation and modernisation of areas such as healthcare, facility management, transportation, and household. These devices allow for real-time mobile sensing, use input and then simplify and automate everyday tasks. However, like all other devices connected to a network, IoT devices are also subject to anomalous behaviour primarily due to security vulnerabilities or malfunction. Apart from this, they have limited resources and can hardly cope with such anomalies and attacks. Therefore, early detection of anomalies is of great importance for the proper functioning of the network and the protection of users' personal data above all. In this paper, deep learning and federated learning algorithms are applied in order to detect anomalies in IoT network traffic. The results obtained show that all the models achieve high accuracy, with the FL models providing slight worse results compared to the DL models. However, with the increase in the amount of user data, the model based on federated learning is expected to have better results over time.

KEYWORDS

federated learning; deep learning; malware; internet of things; anomaly detection

1 INTRODUCTION

In the last decade, a significant increase in the usage of Internet of Things (IoT) devices has been observed. The ability to connect various kinds of devices from different manufacturers to a network wirelessly and share data has proven beneficial to nearly every domain where this technology is involved, including household, industry, infrastructure, transportation, and healthcare[3]. Additionally, the actions that end users can take are increasing everyday and vary from changing ambient parameters of a home or car setting easily and on-the-go to remotely and securely controlling a manufacturing process inside a smart factory setting. Implementing these devices into an ambient assisted living (AAL) setting has proven to be beneficial both for the patients and for the medical staff, as it can improve monitoring and medical assistance (if needed), as well as medication dose adjustment[7].

However, the diversity of IoT devices, accompanied by wireless networking and a slow standardisation process, have led to many issues regarding the privacy and security of data and also the processes based on that data. The occurrence of various cyber attacks on networks composed of IoT devices, but also on individual IoT devices performing specific tasks, is becoming more common [8]. By disabling, reconfiguring or reprogramming such devices, attackers can manipulate the network, obtain private data illegally and maybe even induce a life-threatening situation, especially in the e-health domain. Therefore, it is significantly important to detect potential attacks and anomalies that occur in an IoT setting.

This paper examines the detection of anomalies in IoT network traffic by using deep learning and federated learning algorithms. The remainder of this paper is structured as follows. Section

Information Society 2022, 10–14 October 2022, Ljubljana, Slovenia

2 gives an overview of the approaches tackling IoT network anomaly detection using deep and federated learning algorithms. Section 3 describes the used dataset and gives an insight into the importance of the features. The experiments done in this research and the discussion of the results obtained are presented in Section 4, while Section 5 gives a brief summary and provides further research directions.

2 RELATED WORK

One of the most popular approaches when tackling network anomaly detection is the usage of network intrusion detection systems (NIDS). By examining network data flow patterns (signatures), the NIDS can track inconsistencies (also called anomalies) and resolve them in a timely manner. However, directly analysing the behaviour of the IoT devices has proven to be more beneficial in detecting newer and unknown types of attacks, in spite of the overall lower detection accuracy and higher computational cost [6].

Using machine learning (ML) techniques has had a big impact on the development of NIDS and malware anomaly detection systems in general. Lin et al. [9] propose a combination of Support Vector Machines (SVMs) and Artificial Fish Swarm algorithms for IoT botnet detection. A combination [5] using different ML algorithms, also including an SVM has been done to evaluate the accuracy in detecting Mirai DDoS attacks. The authors in [16] used Convolutional Neural Networks (CNN) with binary visualisation to provide fast zero-day malware detection. However, some of the datasets used in these research papers provide only network traffic flow from conventional networks and have little to do with the attacks which target IoT networks. A further issue is that using traditional ML techniques increases the security risk, as data has to be moved away from the network and the data source to a powerful system performing the ML training.

Federated learning (FL) has emerged as a new decentralised way of training models on privately held datasets that can or should not be shared for security and privacy reasons. The training process consists of a central server and several clients, where the former facilitates the training and the latter possess the private data. In each round of federated training, the server randomly selects a subset of clients who receive the current model parameters. Then, local training is performed by each of the clients, keeping the local data on-site. The updated model parameters are then sent back to the server, where the global server model is updated. Opposed to centralised ML or classical decentralised techniques, FL can work with both independent and identically distributed (IID) and non-IID datasets. [10]

Several approaches have been using this decentralised technique in order to detect anomalies in IoT networks. The DIoT approach [2] uses federated learning to aggregate profiles of IoT network behaviour. It was evaluated in real-world conditions and reported no false alarms. Saharkhizan et al. [14] used a recurrent neural network with ensemble learning to detect cyberattacks on IoT devices. The evaluation of the model was performed on a Modbus dataset of network traffic. Some of the approaches even used a combination of FL and a distributed ledger (blockchain) [12, 17] in order to detect anomalies in networks. In [13], the federated deep learning model created for zero-day botnet attacks on IoT devices outperformed traditional decentralised approaches, as well as both localised deep learning (DL) and distributed DL methods. In [15], a novel privacy-by-design FL model using a stacked long short-time memory (LSTM) model is introduced for tackling anomaly detection in smart buildings. The results showed twice as fast convergence during training, compared to the centralised LSTM.

3 DATASET AND EXPLORATORY DATA ANALYSIS

For the purpose of this research we used the publicly available dataset N-BaIoT [11]. It is a dataset created by a group of researchers from the University of California, Irvine, School of Information and Computer Sciences in the USA. The dataset addresses the lack of public botnet datasets, especially for the IoT domain. It is composed of real-time network traffic data gathered from nine commercial IoT devices, including a baby monitor, security cameras, a webcam, doorbells, and a thermostat, which have been infected by the most common families of botnet attacks: Mirai and Bashlite [1].

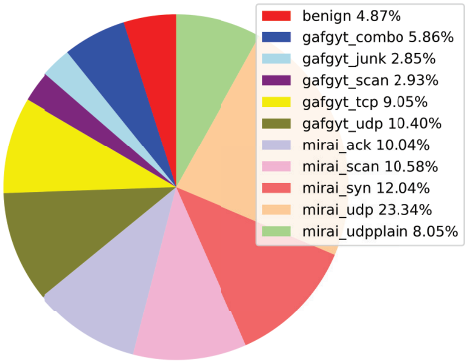

Figure 1: N-BaIoT dataset distribution by class

The N-BaIoT dataset consists of 7,062,606 entries with 115 different features, which are further divided into 10 attack categories: gafgyt_combo, gafgyt_junk, gafgyt_scan, gafgyt_tcp, gafgyt_udp, mirai_ack, mirai_scan, mirai_syn, mirai_udp, mirai_udpplain and one benign category, which contains the normal traffic flow of the observed devices. As it can be seen from Figure 1, which shows the distribution of the dataset used in the upcoming experiments, only a portion (509,149 entries) is considered for the model training in both DL and FL experiments. For the DL experiments, the dataset is further divided into a train and test partition including 80% and 20% of the data, while maintaining the distribution intact. As for the FL experiments, the data is divided into 50 IID datasets which include a train and test subsets. They represent the 50 clients which will take part in the FL process.

Table 1: Most important dataset features

Number	Feature
1	H L0.01_mean
2	Ml_dir_L0.01_mean
3	Ml_dir_L0.01_variance
4	H_L0.01_variance
5	H_L0.1_mean

After preprocessing the data, an exploratory analysis was done in order to obtain the features which have the greatest

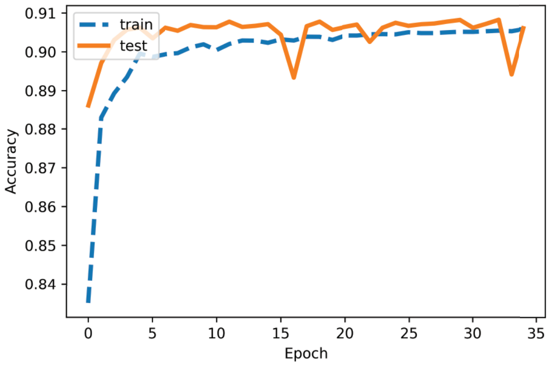

Figure 2: DL model using the five layer NN - accuracy

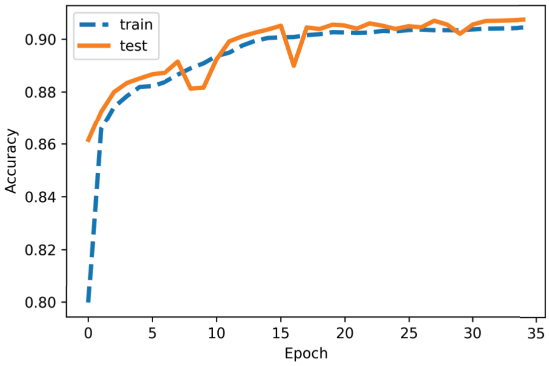

Figure 3: DL model using the three layer NN - accuracy

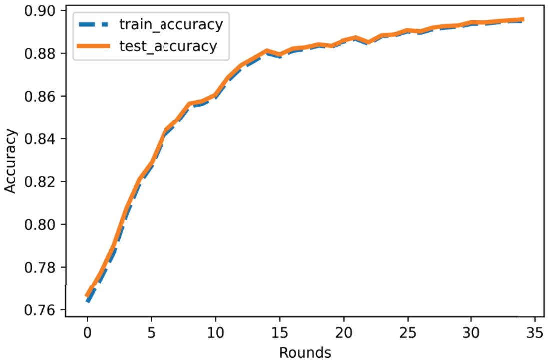

Figure 4: FL model using the five layer NN - accuracy

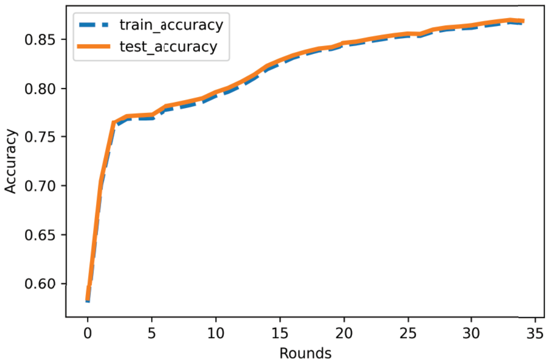

Figure 5: FL model using the three layer NN - accuracy

influence. The mutual dependence between the features and the class was determined with the help of Mutual Information Gain. From Table 1, it can be noticed that the five features with the greatest importance are H L0.01_mean, Ml_dir_L0.01_mean, Ml_dir_L0.01_variance, H_L0.01_variance and H_L0.1_mean.

4 EXPERIMENTS AND DISCUSSION

This paper compares two DL and two FL models for network anomaly detection, which are able to distinguish anomalous behaviour or a deviation from the normal traffic flow of IoT devices. After performing the training, all models were evaluated in order to see their accuracy in detecting anomalies. In the first experiment, a feed-forward neural network with 5 layers, an input layer, 3 hidden layers and an output layer was used. In the second experiment, a simple feed-forward neural network with one hidden layer was used. In both cases, the output layer has 11 neurons, which represent all the classes in the dataset.

Both models have the same hyperparameters. We used the Adam optimiser with a learning rate of 0.001, which works well for many use cases and models. Since the model performs a multi-class prediction task, we minimised the categorical cross entropy loss during training. The DL experiments were performed using the TensorFlow framework and the FL experiments were performed using the Flower [4] framework and TensorFlow Federated, applying the FedAvg aggregation strategy [10] on the server. In the FL experiments 35 rounds were performed, which corresponds to approximately 35 epochs in the DL experiments.

As previously mentioned, two DL models, the first one using a NN with multiple layers and the second one using a simple NN were trained and tested. From Figures 2 and 3 we can notice that the accuracy between the two models is very similar - the first model obtained an accuracy of 90.75% on the test data, while the second model obtained an accuracy of 90.18%. Furthermore, if the confusion matrices of both DL models are analysed, it can be noted that both models make the same mistake - predicting class 4 (gafgyt_scan) as class 5 (gafgyt_tcp).

When it comes to the results obtained from the FL process after 35 rounds it can be seen that the first model obtained an accuracy of 88% (Figure 4). As for the second simplified model, the accuracy is 86% (Figure 5). This means that even though a simpler NN was used, the second model actually performed similarly in terms of FL. We can also observe the minor differences in accuracy (1-5%) between the DL and FL models, which means that although the DL models performed slightly better, the FL models can also accurately predict anomalies.

From Figures 6 and 7 we can analyse the SHAP (SHapley Additive exPlanations) force plot, which shows the contribution of each feature in making a prediction. We can see that the features 69, 25, 75, 87, 56 and 101 (HH_jit_L3_mean, H_L0.1_mean, HH_jit_L0.1_mean, HpHp_L3_weight, HH_L0._covariance and HpHp_L0.1_weight) have the greatest influence in making the prediction. The features 69, 25 and 75 have a positive impact on

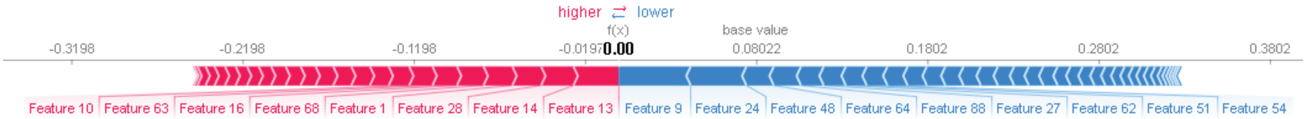

Figure 6: SHAP force plot for DL model using the five layer NN.

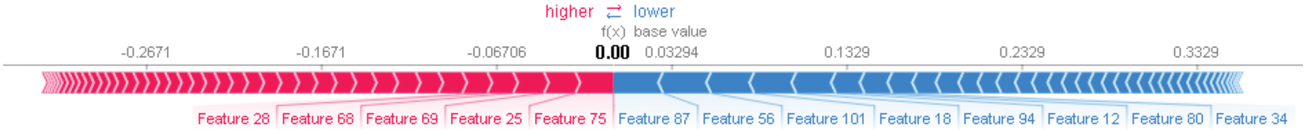

Figure 7: SHAP force plot for DL model using the three layer NN.

decision-making, i.e. prediction, while the features 87, 56 and 101 affect negatively on the performance. When we compare Figures 6 & 7 and Table 1, we can see that the most important features are different. This is because the SHAP method deals with the model and its output, while Mutual Information Gain deals with the preprocessed data.

5 CONCLUSION AND FUTURE WORK

This paper compares two models of DL and FL for accurate anomaly detection purposes in IoT networks. The FL model distributes the learning process to several clients, thus preserving data privacy and security. Both models achieve high accuracy, with the FL models providing similar results to the DL models.

Future work will include implementing some security mechanisms to the FL models and evaluating the trade-off between privacy and accuracy. Also, these models can be further tested and improved by being provided with new substantial datasets which may combine similar categories of attacks and/or include novel attacks on IoT networks. New federated learning algorithms can also be tested and evaluated on the same and new datasets, which can lead to a novel federated learning algorithm for anomaly detection purposes.

ACKNOWLEDGMENTS

The authors would like to thank Daniel Denkovski and Valentin Rakovic for the useful discussions on the research topic. This work has been supported by the WideHealth project - European Union's Horizon 2020 research and innovation programme under grant agreement No. 952279.

REFERENCES

[1] Abdelmuttlib Ibrahim Abdalla Ahmed. 2020. Systematic Literature Review on IoT-Based Botnet Attack. *IEEE Access* 8 (12 2020). https://doi.org/10.1109/ACCESS.2020.3039985

[2] Ulrich Matchi Aïvodji, Sébastien Gambs, and Alexandre Martin. 2019. IOTFLA : A Secured and Privacy-Preserving Smart Home Architecture Implementing Federated Learning. In *2019 IEEE Security and Privacy Workshops (SPW)*. 175–180. https://doi.org/10.1109/SPW.2019.00041

[3] Saurabh Bagchi, Tarek F. Abdelzaher, Ramesh Govindan, Prashant Shenoy, Akanksha Atrey, Pradipta Ghosh, and Ran Xu. 2020. New Frontiers in IoT: Networking, Systems, Reliability, and Security Challenges. *IEEE Internet of Things Journal* 7, 12 (2020), 11330–11346. https://doi.org/10.1109/JIOT.2020.3007690

[4] Daniel J. Beutel, Taner Topal, Akhil Mathur, Xinchi Qiu, Javier Fernandez-Marques, Yan Gao, Lorenzo Sani, Kwing Hei Li, Titouan Parcollet, Pedro Porto Buarque de Gusmão, and Nicholas D. Lane. 2020. Flower: A Friendly Federated Learning Research Framework. https://doi.org/10.48550/ARXIV.2007.14390

[5] Rohan Doshi, Noah Apthorpe, and Nick Feamster. 2018. Machine Learning DDoS Detection for Consumer Internet of Things Devices. In *2018 IEEE Security and Privacy Workshops (SPW)*. 29–35. https://doi.org/10.1109/SPW.2018.00013

[6] Satish Kumar, Sunanda Gupta, and Sakshi Arora. 2021. Research Trends in Network-Based Intrusion Detection Systems: A Review. *IEEE Access* 9 (2021), 157761–157779. https://doi.org/10.1109/ACCESS.2021.3129775

[7] Isabel Laranjo, Joaquim Macedo, and Alexandre Santos. 2012. Internet of Things for Medication Control: Service Implementation and Testing. *Elsevier Procedia Technology* 5 (10 2012), 777–786. https://doi.org/10.1016/j.protcy.2012.09.086

[8] In Lee. 2020. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. *Future Internet* 12 (09 2020), 157. https://doi.org/10.3390/fi12090157

[9] Kuan-Cheng Lin, Sih-Yang Chen, and Jason Hung. 2014. Botnet Detection Using Support Vector Machines with Artificial Fish Swarm Algorithm. *Journal of Applied Mathematics* 2014 (04 2014), 1–9. https://doi.org/10.1155/2014/986428

[10] H. Brendan McMahan, Daniel Ramage, Kunal Talwar, and Li Zhang. 2017. Learning Differentially Private Language Models Without Losing Accuracy. *CoRR* abs/1710.06963 (2017). arXiv:1710.06963 http://arxiv.org/abs/1710.06963

[11] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. 2018. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Computing* 17, 3 (2018), 12–22. https://doi.org/10.1109/MPRV.2018.03367731

[12] Yisroel Mirsky, Tomer Golomb, and Yuval Elovici. 2020. Lightweight collaborative anomaly detection for the IoT using blockchain. *J. Parallel and Distrib. Comput.* 145 (06 2020). https://doi.org/10.1016/j.jpdc.2020.06.008

[13] Segun I. Popoola, Ruth Ande, Bamidele Adebisi, Guan Gui, Mohammad Hammoudeh, and Olamide Jogunola. 2022. Federated Deep Learning for Zero-Day Botnet Attack Detection in IoT-Edge Devices. *IEEE Internet of Things Journal* 9, 5 (2022), 3930–3944. https://doi.org/10.1109/JIOT.2021.3100755

[14] Mahdis Saharkhizan, Amin Azmoodeh, Ali Dehghantanha, Kim-Kwang Raymond Choo, and Reza M. Parizi. 2020. An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic. *IEEE Internet of Things Journal* 7, 9 (2020), 8852–8859. https://doi.org/10.1109/JIOT.2020.2996425

[15] Raed Abdel Sater and A. Ben Hamza. 2021. A Federated Learning Approach to Anomaly Detection in Smart Buildings. *ACM Trans. Internet Things* 2, 4, Article 28 (aug 2021), 23 pages. https://doi.org/10.1145/3467981

[16] Robert Shire, Stavros Shiaeles, Keltoum Bendiab, Bogdan Ghita, and Nicholas Kolokotronis. 2019. Malware Squid: A Novel IoT Malware Traffic Analysis Framework Using Convolutional Neural Network and Binary Visualisation. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Olga Galinina, Sergey Andreev, Sergey Balandin, and Yevgeni Koucheryavy (Eds.). Springer International Publishing, Cham, 65–76.

[17] Devrim Unal, Mohammad Hammoudeh, Muhammad Asif Khan, Abdelrahman Abuarqoub, Gregory Epiphaniou, and Ridha Hamila. 2021. Integration of Federated Machine Learning and Blockchain for the Provision of Secure Big Data Analytics for Internet of Things. *Comput. Secur.* 109, C (oct 2021), 14. https://doi.org/10.1016/j.cose.2021.102393