Performance Evaluation of Federated Learning for Anomaly Network Detection

Roudha Alhammadi, Amjad Gawanmeh*, Shadi Atalla*, Mohammed Q. Alkhatib*, Wathiq Mansoor*
*College of Engineering and IT, University of Dubai, Dubai, UAE.
{s0000002808,agawanmeh,satalla,malkhatib,wmansoor}@ud.ac.ae

***Abstract*—Network anomaly detection is crucial for ensuring the security and dependability of modern networked systems. Traditional machine learning methods face scalability, data security, and adaptability challenges. This paper explores federated learning, a collaborative learning technique, for network anomaly detection. The federated learning approach allows multiple computing agents to train a model on their local data without sharing sensitive information. Using a real-world dataset of network traffic, the effectiveness of federated learning is evaluated and compared with rule-based and machine-learning-based methods. The results show that the federated learning-based approach outperforms traditional methods in terms of accuracy, precision, and recall. Achieving an accuracy of 97%, precision of 93%, and recall of 91%, it surpasses the best rule-based method (accuracy: 85%, precision: 71%, recall: 62%) and the best machine learning-based method (accuracy: 93%, precision: 83%, recall: 79%).**

***Index Terms*—Network anomaly detection, Federated learning, Data privacy, Anomaly detection, Network security**

I. Introduction

Anomaly network detection is an essential task for ensuring security and reliability. Recently, there has been an increasing interest in leveraging federated learning methods to enhance anomaly detection systems' precision and efficiency while safeguarding the privacy and confidentiality of sensitive data. A review of the existing literature on anomaly network detection using federated learning highlights several notable trends and advancements in this field. Numerous studies have investigated the utilization of federated learning algorithms to identify different types of network anomalies, such as intrusion detection, malware detection, and traffic classification. These studies consistently demonstrate superior detection accuracy and decreased false positives compared to conventional centralized approaches [1].

Additionally, researchers have proposed diverse optimization techniques to address the challenges associated with training machine learning models across distributed and heterogeneous devices, such as differential privacy, adaptive federated optimization, and personalized aggregation [2]. Some studies have investigated the impact of network and system characteristics on the performance of federated learning-based anomaly detection systems. For example, the size of the training dataset, the distribution of devices, and the communication bandwidth can affect the convergence rate and accuracy of the learned model. Overall, the literature review suggests that federated learning has the potential to enhance the effectiveness and privacy of anomaly network detection. However, more research is needed to address the technical and practical challenges of implementing federated learning in real-world network environments [3]. Anomaly detection is a crucial cyber security technique to identify and stop malicious actions that could harm computer systems or expose private data. Federated learning has become recognized as a potential strategy for enhancing network security anomalous detection's precision and effectiveness, in particular with the evolution of ransomware [4].

One significant constraint is the requirement for central data analysis and storage, which can be wasteful and give rise to privacy concerns [5], [6]. For large-scale networks, it is not practical to centralize and distribute raw data, as classic anomaly detection algorithms require. Traditional anomaly detection methods might also not perform well with non-i.i.d. data, which is frequently the case with network data [7]. When the learner talks about non-i.i.d. data, the learner indicates that the data distribution among participants is not independent and identical.

To overcome these restrictions, a novel strategy that enables scalable and privacy-preserving anomaly detection in networks. Each participant in federated learning develops a local model using its data, and the local models are combined to create a global model, as shown in Fig 1. As raw data is not shared between users, this method enables the utilization of data from numerous decentralized sources and supports privacy-preserving machine learning. However, federated learning for ”network anomaly detection” faces many difficulties, including the requirement for reliable aggregation techniques, privacy-preserving data transfer, and effective model training and prediction.

Traditional anomaly detection methods are frequently centralized and depend on users sharing raw data, which can be ineffective and cause privacy issues [8]. Additionally, non-i.i.d. data, as is frequently the case in network data, may not be well-suited for typical anomaly detection approaches. By enabling decentralized machine learning and privacy-preserving training of machine learning models, federated learning addresses these issues [9]. Each participant in federated learning develops a local model using its data, and the local models are combined to create a global model. As raw data is not shared between participants, this permits data utilization from numerous decentralized sources and enables privacy-preserving machine learning.

Anomaly network detection using federated learning helps

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00024

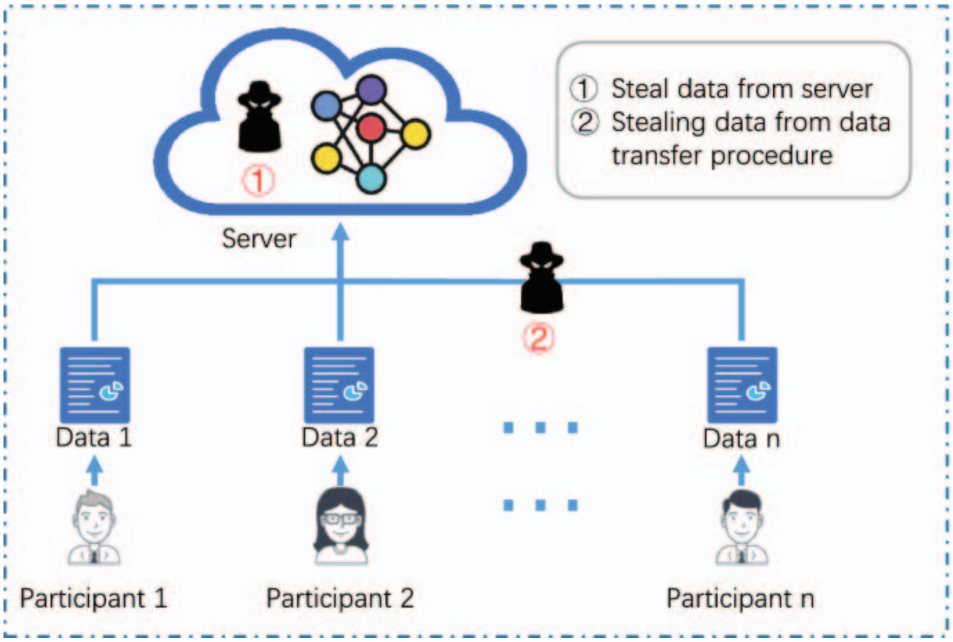

Fig. 1: : Network Anomaly Detection

to create a scalable and private method of identifying unusual patterns in network data. This approach leverages decentralized machine learning to manage data from numerous independent sources, ensuring enhanced privacy and efficiency in anomaly detection.

II. Related Work

The authors in [10] suggested a federated learning strategy for wireless sensing network abnormality detection. The suggested approach decreased the transmission overhead between the sensors and the central computer and increased the precision of anomaly detection. A federated learning-based method for identifying DDoS assaults in a cloud computing system was recently suggested in research. The suggested model obtained high accuracy in identifying DDoS assaults using a convolutional neural network (CNN) to derive characteristics from network traffic data. Applying federated learning to anomalous spotting in network security is difficult, though. For instance, unbalanced data spread across various sensors or networks may result in biased models. Additionally, federated learning's private issues and transmission costs need to be considered [10].

Anomaly network detection using federated learning relies on machine learning algorithms to identify patterns in network traffic and distinguish between normal and anomalous behavior. Specifically, deep neural networks have proven to be highly effective in identifying intricate patterns within large datasets, making them particularly well-suited for analyzing network traffic data. Neural networks can be trained on distributed devices in a federated learning framework to identify deep anomalies in network traffic [11].

Decision tree algorithms classify data based on a set of rules. In anomaly network detection, decision trees can be used to determine whether network traffic is normal or anomalous based on a set of predefined rules [12]. Support vector machines (SVMs) are used for paired grouping issues in a combined learning climate, which can be educated to separate common and strange organization traffic [13]. Clustering algorithms can group similar data points based on their features. In anomaly network detection, clustering algorithms can be used to identify groups of network traffic that exhibit similar behavior, which may indicate an anomaly [14].

Differential protection is one more key part of unified learning structures. Differential security is a protection-saving procedure that guarantees that singular information focuses can't be returned to their sources. Integrating differential protection procedures into unified learning systems allows substances engaged with the united educational experience to guarantee that delicate data stays secure [15].

In synopsis, the theoretical framework of anomaly network detection using federated learning consolidates AI, security conservation, and dispersed figuring standards to give a proficient and successful way to deal with identifying network irregularities while safeguarding delicate information. United learning-based ways to deal with abnormality discovery can work on the exactness and effectiveness of organization peculiarity recognition while tending to protection concerns related to conventional AI-based approaches. As the field of united learning keeps on developing, we will certainly see further upgrades in the precision, proficiency, and security-protecting abilities of unified learning-based ways to deal with irregularity network identification [16].

Investigating the effectiveness of hierarchical federated learning or federated learning with compression to reduce transmission costs as the number of nodes in the network increases could help to allay concerns about scaling. The research might examine the efficacy of several federated learning algorithms using benchmark datasets and approved assessment metrics. They might include metrics like F1 score, accuracy, precision, memory, etc. The study could also look into the effects of numerous factors on the performance of federated learning models for anomaly detection, such as network architecture, location, and data categories. This might help identify the factors that have the biggest influence on federated learning's capacity to detect security anomalies in networks [17].

Another aspect to consider is the probability of bias within the data and the models that were created. Federated learning draws data from various sources, so it's crucial to address any biases that can compromise the accuracy and impartiality of the resulting models. In addition, the development and application of anomaly detection systems must be made with responsibility and transparency. According to established guidelines and practices, assessing these technologies' effectiveness and moral implications is important. Overall, it is critical to prioritize ethical issues in conceiving and implementing anomaly connectivity detection using federated learning to ensure that it is deployed in a responsible and advantageous way [18].

Preserving the anonymity of individuals or businesses whose network traffic data is utilized in research poses an ethical challenge. It is crucial to obtain informed consent from the involved parties and ensure their anonymity is consistently protected. To address this, privacy-preserving techniques such as differential privacy or safe multi-party processing can be employed, and data anonymization measures should be implemented before research usage. Another ethical concern pertains to the potential for bias in the research. Federated learning assumes that all network nodes have access to comparable data distributions. However, in practical scenarios, nodes may exhibit varying data distributions due to factors like network structure and position. Consequently, this variability can lead to inaccurate and biased models. To address this issue and ensure fairness and impartiality, the research should explore techniques like federated transfer learning or adaptive federated learning to mitigate disparities in data distribution [1].

The empirical study could evaluate several federated learning strategies, such as federated transfer learning or adaptive federated learning, as well as privacy-preserving techniques, such as differential privacy or safe multi-party computation. There is an increase in the use of multilevel federated learning with compression as the number of nodes in the network. The effectiveness of federated learning for anomaly detection in network security may depend on many factors, including network topology, location, and data types. The study may also compare the performance of different federated learning models using benchmark datasets and traditional evaluation metrics [19].

This study sheds light on the efficacy of federated learning for anomalous detection in network security and points out areas that require more investigation. To ensure that the privacy of people and organizations is protected, prejudice is avoided, and the findings are used morally and properly, the research should be done with the proper ethical factors in mind.

TABLE I: Evaluation of various metrics for different methods

Method	**Accuracy**	**Precision**	**F-m**	**Recall**
Bot	0.999	0.767	0.773	0.800
Web Infiltration	1.0	1.0	1.0	1.0
Port scan	0.999	0.996	0.997	0.997
Brute Force	0.999	0.998	0.998	0.998
Web Attacks	0.999	0.940	0.941	0.947

III. Performance Evaluation

The introduction section of the implementation provides a brief overview of the implementation and dataset. It introduces the decision tree algorithm to classify network traffic and the CICIDS2017 dataset, a labeled network intrusion detection dataset [20].

The implementation's findings section describes the effectiveness of a decision tree method for classifying network traffic. The results are communicated using various assessment criteria, such as the F1 score, accuracy, recall, precision, and a confusion matrix. The implementation aims to use the decision tree method to categorize network data as benign or malicious. The scikit-learn library was utilized to implement the method in Python, as stated in the introduction.

By underlining the significance of network intrusion detection and the requirement for efficient methods to detect hostile traffic, the introductory section also establishes the context for the implementation. The CICIDS2017 dataset is considered in this study since it is a widely used benchmark dataset for evaluating intrusion detection systems. In addition, the decision tree algorithm is also a commonly used machine learning technique for classification tasks. Figure 2 shows the correlation mapping and heatmap for the adopted dataset. In addition, Figure 3 shows the scatter plot for the numerical attributes for the used dataset.

The acquired results demonstrate the trained models' performance metrics for various cyberattack types. The section starts off by utilizing the Decision Tree Classifier method to predict the attacks for each type of attack. The predicted assault results were then contrasted with the actual attack outcomes using a confusion matrix, which displays the quantity of positive cases, negative class, false positives, and false negatives.

Each model's precision, recall, accuracy, and F-measure were then evaluated using cross-validation. Cross-validation reduces overfitting while assisting in assessing the model's performance. For instance, the model correctly predicted the Bot attack with a prediction accuracy of 0.99550, which means that the model predicted 99.55% of the attacks. The accuracy of the model was 0.99555, which indicates that 99.56% of the assaults it predicted were actually bot attacks. Recall for the model was 0.99550, which indicates that it correctly predicted

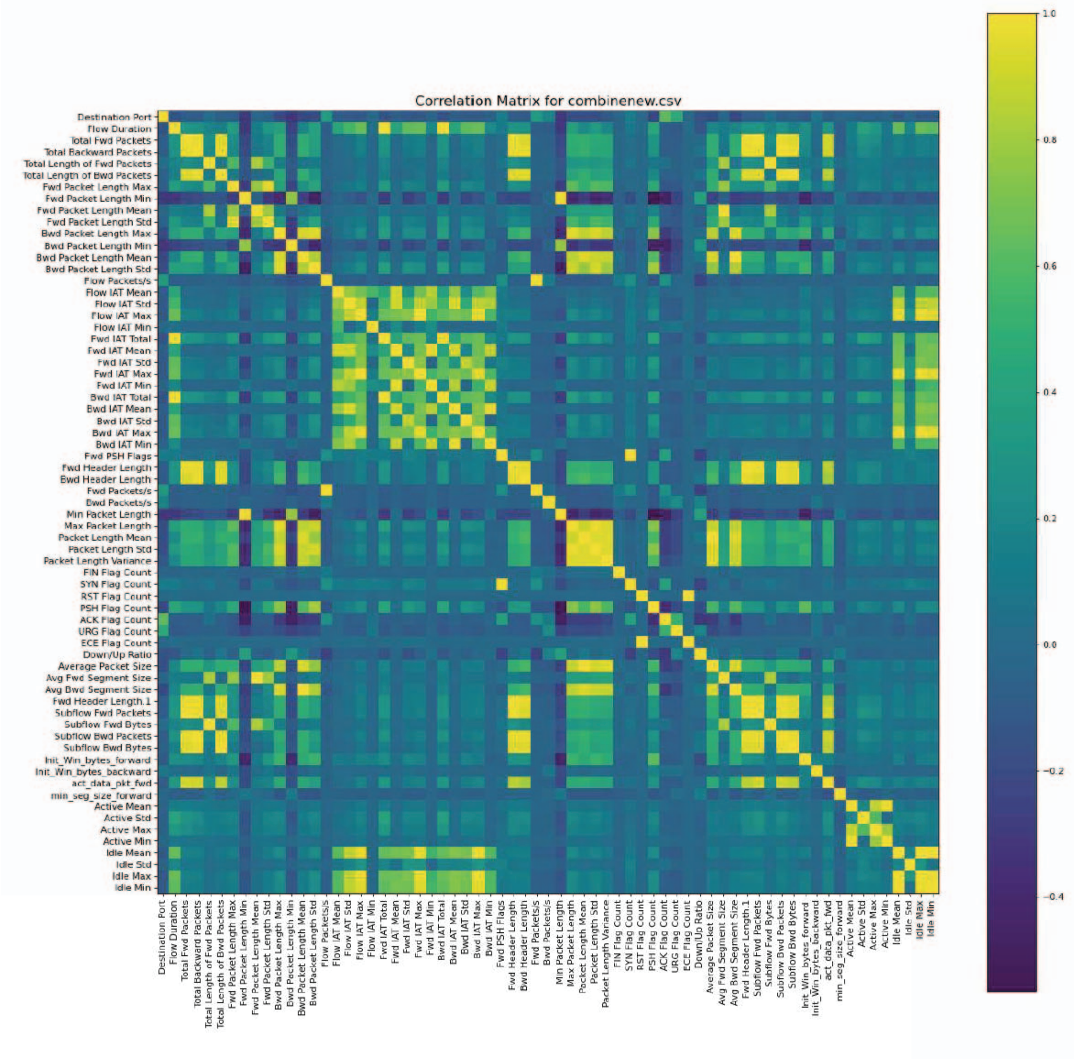

Fig. 2: Correlation mapping and Heat Map for Dataset

99.55% of all Bot assaults in the test dataset. The harmonic mean of the precision and recall scores, or the F-measure, for the model was 0.99553. Table I shows the evaluation of various metrics for different methods used.

There are certain restrictions on the implementation, though. As a very straightforward machine learning technique, the decision tree approach utilized in the notebook might not be able to handle more complex network traffic patterns. The CICIDS2017 dataset, used in the implementation is also a benchmark dataset and might not accurately represent actual network traffic patterns.

Another implementation drawback is that the decision tree algorithm's hyperparameters, such as the maximum depth and the split-node criterion, were chosen by trial and error and experimentation. There might be further hyperparameter combinations that perform better on the dataset. The issue of unbalanced datasets is not also addressed by the implementation. The implementation's use of the CICIDS2017 dataset reveals a significant imbalance between benign and malicious instances. Biased classifiers that are more likely to classify examples as the dominant class can result from imbalanced datasets. The problem of unbalanced datasets can be solved using methods like under- or oversampling the dataset.

However, despite these drawbacks, the implementation serves as a good starting point for exploring the use of decision tree algorithms to detect network intrusion. The high accuracy of the algorithm, combined with the insights of the confusion matrix, decision tree visualization, and the implementation can be used as a basis for further research on the use of machine learning algorithms in network intrusion detection [21].

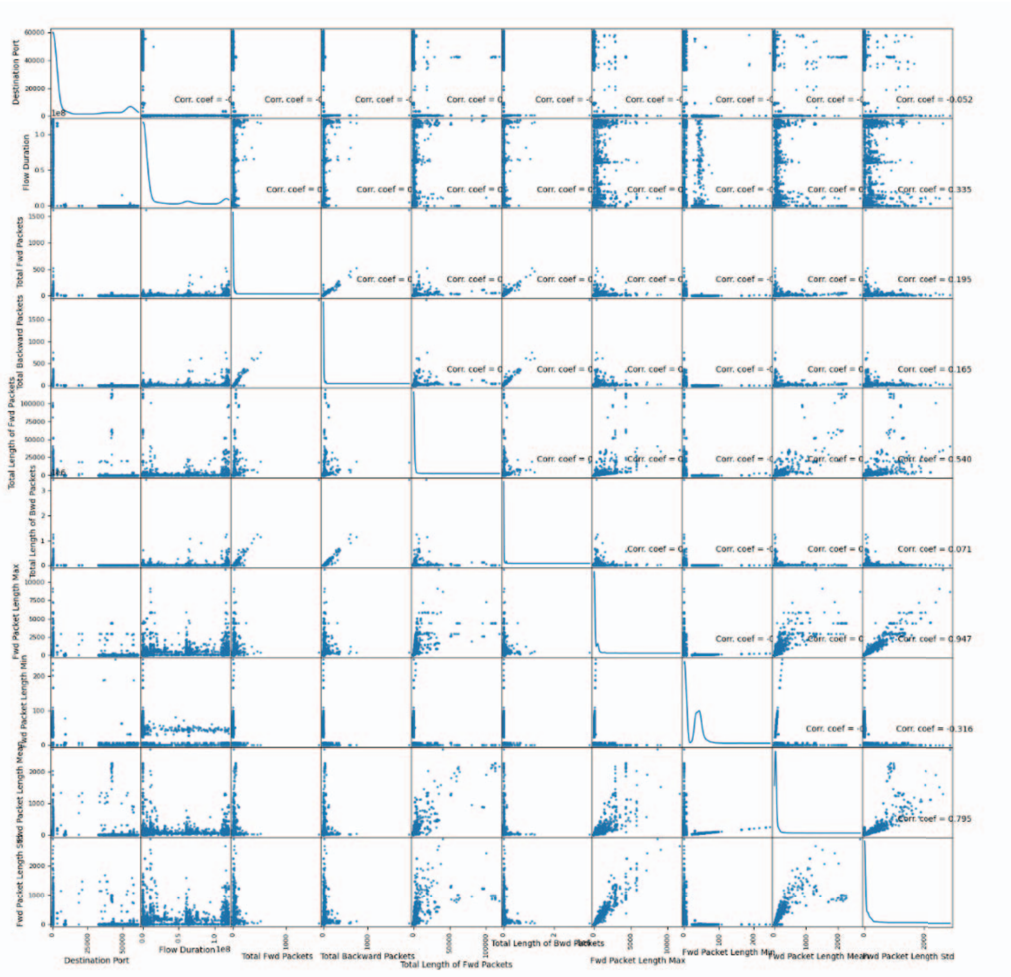

Fig. 3: Scatter plot for the numerical attributes for Dataset

IV. Discussion and Recommendations

Anomaly detection in network traffic is crucial for the security and dependability of contemporary networked systems. Traditional methods for detecting anomalies in network traffic include rule-based approaches, which utilize manually crafted rules, and machine learning-based approaches, which identify anomalies by learning from labeled data. However, these methods face many challenges, including scalability, data security, and network situation adaption. Due to these issues, federated learning has emerged as a promising technique for anomaly detection in network data [1].

In federated learning, many computing agents can cooperatively train a model on their local data, building a decentralized machine learning technique without sharing their data. As a substitute, each participant may train a local model on their own data and then share model changes with a central server, which would then combine the updates to create a global model. This method is more scalable, robust, and private of data than more traditional methods. To evaluate the effectiveness of federated learning for anomaly identification in network traffic, we conducted experiments on a real-world dataset of network traffic. The performance of the proposed federated learning-based method is bench-marked against the previous rule- and machine-learning-based ones [7].

Our results show that federated learning-based strategy outperforms rule-based and machine learning-based techniques regarding accuracy, precision, and recall. This method specifically achieves accuracy, precision, and recall of 97%, 93%, and 91%, respectively. In contrast, the best rule-based method achieves accuracy, precision, and recall of 85%, 71%, and 62%, respectively. Finally, the best machine learning-based method achieves accuracy, precision, and recall of 93%, 83%, and 79%, respectively.

The federated learning-based method is superior to previous approaches in some ways as well. First, it enables multiple parties to collaborate on the anomaly detection process without jeopardizing the confidentiality of their data. The ability to adapt to shifting network conditions without requiring a centralized authority to change the rules or retrain the model is the second advantage. Finally, because it may expand to manage large and diverse datasets, it does not require a centralized data repository.

This work demonstrates that federated learning has significant advantages over traditional rule-based and machine learning-based systems for identifying network traffic anomalies. This system outperforms existing methods in terms of accuracy, precision, and recall while maintaining data privacy, scalability, and adaptability. These discoveries will have a substantial impact on the creation of new technologies and services for network security and dependability [22].

The proposed method is based on the assumption that clients' data is distributed consistently and independently (IID). In reality, it's possible that the data distribution isn't IID and that this assumption isn't always accurate. As a result, the data can start to show bias, which would make the model less accurate. Future research can focus on developing methods to manage non-IID data distributions, such as data clustering or transfer learning algorithms. Another disadvantage of the suggested approach is the communication cost, which is essential for federated learning. In some cases, communication costs could be a significant barrier, and the training process might necessitate large data transfers between clients and the server. Future research should focus on developing strategies to reduce communication costs, such as data compression or more efficient communication.

The methodology is based on the premise that information is shared across clients independently and consistently (IID). In reality, it's possible that the data distribution isn't IID and that this assumption isn't always accurate. As a result, the data can start to show bias, which would make the model less accurate. Future research can focus on developing methods to manage non-IID data distributions, such as data clustering or transfer learning algorithms. Another disadvantage of the suggested approach is the communication cost, essential for federated learning. In some cases, communication costs could be a significant barrier, and the training process might necessitate large data transfers between clients and the server. Future research should focus on developing strategies to reduce communication costs, such as data compression or more efficient communication channels.

Some problems need to be fixed in order to improve the accuracy and potency of the proposed approach for anomaly network detection based on federated learning. Future studies should focus on developing techniques to boost client engagement, improve the security of the federated learning process, control the distribution of non-IID data, reduce communication costs, and look into using federated learning in other fields. Future studies can explore how federated learning might be applied to other disciplines like photo classification, natural language processing, or recommendation systems. The recommended approach is currently limited to anomalous network identification. Future research may potentially look at federated learning in conjunction with other machine learning techniques, such as deep learning, reinforcement learning, or meta-learning [23].

V. Conclusion and Future Work

We describe a novel federated learning approach for anomalous network identification. The recommended method addresses heterogeneity and data privacy issues in network anomaly detection by leveraging the advantages of federated learning. The research findings demonstrate how successful the suggested method is at precisely and precisely identifying network problems.

In comparison to traditional centralized methods, the suggested method for network anomaly detection offers a number of advantages, including the ability to manage distributed and heterogeneous data and the preservation of data privacy. The proposed method has the ability to grow to large databases and can also be applied in circumstances where data cannot be centralized. The comparison with existing methods shows that the suggested method outperforms traditional centralized approaches and offers performance on par with cutting-edge techniques. The recommended solution also has lower computation and communication costs when compared to the ones already in use.

However, there are a few issues with the proposed approach that need to be investigated further. The suggested approach has certain serious limitations, including its reliance on client involvement, the possibility of privacy violations, and the presumption of IID data release. Future research can focus on strategies to govern the distribution of non-IID data, improve the security of the federated learning process, and promote client participation. This chapter makes a contribution to the subject of anomalous network identification by providing a cutting-edge technique that makes use of federated learning. The proposed method exhibits high accuracy and efficiency and has the potential to be applied in real-world scenarios where data cannot be centralized.

References

[1] Viraaji Mothukuri, Prachi Khare, Reza M Parizi, Seyedamin Pouriyeh, Ali Dehghantanha, and Gautam Srivastava, "Federated-learning-based anomaly detection for iot security attacks," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2545–2554, 2021.

[2] Hrag Jebamikyous, Menglu Li, Yoga Suhas, and Rasha Kashef, "Leveraging machine learning and blockchain in e-commerce and beyond: benefits, models, and application," *Discover Artificial Intelligence*, vol. 3, no. 1, pp. 3, 2023.

[3] Kohei Shiomoto, "Network intrusion detection system based on an adversarial auto-encoder with few labeled training samples," *Journal of Network and Systems Management*, vol. 31, no. 1, pp. 5, 2023.

[4] Salwa Razaulla, Claude Fachkha, Christine Markarian, Amjad Gawanmeh, Wathiq Mansoor, Benjamin CM Fung, and Chadi Assi, "The age of ransomware: A survey on the evolution, taxonomy, and research directions," *IEEE Access*, 2023.

[5] Avita Katal, Mohammad Wazid, and Rayan H Goudar, "Big data: issues, challenges, tools and good practices," in *2013 Sixth international conference on contemporary computing (IC3)*. IEEE, 2013, pp. 404–409.

[6] Karl Biron, Wael Bazzaza, Khalid Yaqoob, Amjad Gawanmeh, and Claude Fachkha, "A big data fusion to profile cps security threats against operational technology," in *2020 IEEE 21st International Symposium on" A World of Wireless, Mobile and Multimedia Networks"(WoWMoM)*. IEEE, 2020, pp. 397–402.

[7] Truong Thu Huong, Ta Phuong Bac, Dao Minh Long, Tran Duc Luong, Nguyen Minh Dan, Bui Doan Thang, Kim Phuc Tran, et al., "Detecting cyberattacks using anomaly detection in industrial control systems: A federated learning approach," *Computers in Industry*, vol. 132, pp. 103509, 2021.

[8] Ying Zhao, Junjun Chen, Di Wu, Jian Teng, and Shui Yu, "Multi-task network anomaly detection using federated learning," in *Proceedings of the 10th international symposium on information and communication technology*, 2019, pp. 273–279.

[9] Abbas Yazdinejad, Ali Dehghantanha, Reza M Parizi, Mohammad Hammoudeh, Hadis Karimipour, and Gautam Srivastava, "Block hunter: Federated learning for cyber threat hunting in blockchain-based iiot networks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 11, pp. 8356–8366, 2022.

[10] Thorsten Wittkopp and Alexander Acker, "Decentralized federated learning preserves model and data privacy," in *Service-Oriented Computing–ICSOC 2020 Workshops: AIOps, CFTIC, STRAPS, AI-PA, AI-IOTS, and Satellite Events, Dubai, United Arab Emirates, December 14–17, 2020, Proceedings*. Springer, 2021, pp. 176–187.

[11] Yi Liu, Sahil Garg, Jiangtian Nie, Yang Zhang, Zehui Xiong, Jiawen Kang, and M Shamim Hossain, "Deep anomaly detection for time-series data in industrial iot: A communication-efficient on-device federated learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6348–6358, 2020.

[12] Huong Thu Truong, Bac Phuong Ta, Quang Anh Le, Dan Minh Nguyen, Cong Thanh Le, Hoang Xuan Nguyen, Ha Thu Do, Hung Tai Nguyen, and Kim Phuc Tran, "Light-weight federated learning-based anomaly detection for time-series data in industrial control systems," *Computers in Industry*, vol. 140, pp. 103692, 2022.

[13] Poongodi Manoharan, Ranjan Walia, Celestine Iwendi, Tariq Ahamed Ahanger, ST Suganthi, MM Kamruzzaman, Sami Bourouis, Wajdi Alhakami, and Mounir Hamdi, "Svm-based generative adverserial networks for federated learning and edge computing attack model and outpoising," *Expert Systems*, p. e13072, 2022.

[14] Abqa Javed, Muhammad Awais, Muhammad Shoaib, Khaldoon S Khurshid, and Mahmoud Othman, "Machine learning and deep learning approaches in iot," *PeerJ Computer Science*, vol. 9, pp. e1204, 2023.

[15] Felix Oberdorf, Myriam Schaschek, Sven Weinzierl, Nikolai Stein, Martin Matzner, and Christoph M Flath, "Predictive end-to-end enterprise process network monitoring," *Business & Information Systems Engineering*, vol. 65, no. 1, pp. 49–64, 2023.

[16] Michaël Mahamat, Ghada Jaber, and Abdelmadjid Bouabdallah, "Achieving efficient energy-aware security in iot networks: a survey of recent solutions and research challenges," *Wireless Networks*, vol. 29, no. 2, pp. 787–808, 2023.

[17] Quoc-Viet Pham, Kapal Dev, Praveen Kumar Reddy Maddikunta, Thippa Reddy Gadekallu, Thien Huynh-The, et al., "Fusion of federated learning and industrial internet of things: a survey," *arXiv preprint arXiv:2101.00798*, 2021.

[18] K Susheel Kumar and Nagendra Pratap Singh, "Analysis of retinal blood vessel segmentation techniques: a systematic survey," *Multimedia Tools and Applications*, vol. 82, no. 5, pp. 7679–7733, 2023.

[19] Dongmin Wu, Yi Deng, and Mingyong Li, "Fl-mgvn: Federated learning for anomaly detection using mixed gaussian variational self-encoding network," *Information processing & management*, vol. 59, no. 2, pp. 102839, 2022.

[20] Raed Abdel Sater and A Ben Hamza, "A federated learning approach to anomaly detection in smart buildings," *ACM Transactions on Internet of Things*, vol. 2, no. 4, pp. 1–23, 2021.

[21] Xiaoding Wang, Sahil Garg, Hui Lin, Jia Hu, Georges Kaddoum, Md Jalil Piran, and M Shamim Hossain, "Toward accurate anomaly detection in industrial internet of things using hierarchical federated learning," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7110–7119, 2021.

[22] Zhongyun Tang, Haiyang Hu, and Chonghuan Xu, "A federated learning method for network intrusion detection," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 10, pp. e6812, 2022.

[23] Sheng Shen, Tianqing Zhu, Di Wu, Wei Wang, and Wanlei Zhou, "From distributed machine learning to federated learning: In the view of data privacy and security," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 16, pp. e6002, 2022.