Advancing Security in 5G Core Networks through Unsupervised Federated Time Series Modeling

Saeid Sheikhi and Panos Kostakos
Center for Ubiquitous Computing
Faculty of Information Technology and Electrical Engineering
University of Oulu, Oulu, Finland,90014
Email: Saeid.Sheikhi@oulu.fi

2024 IEEE International Conference on Cyber Security and Resilience (CSR) | 979-8-3503-7536-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/CSR61664.2024.10679491

***Abstract*—The rapid development of fifth-generation (5G) mobile communication technology poses fresh challenges for cybersecurity defense systems. Current intrusion detection mechanisms in 5G networks have shortcomings, particularly in identifying sophisticated cyber attacks. Our study presents a novel approach combining Federated Learning with Long Short-Term Memory (LSTM) networks to enhance cyber threat detection on the GTP protocol within 5G infrastructures. Our approach leverages the collective analytical power of multiple devices to identify cyber threats more effectively. The model validated against two major cyber threats, Distributed Packet Forwarding Control Protocol (PFCP) and IP address spoofing emulated within a specially constructed 5G test environment that mirrors a complex public network infrastructure. The findings demonstrate that our unsupervised FL-LSTM model effectively identifies 5G cyber threats while preserving individual network traffic privacy, highlighting Federated Learning's potential to strengthen 5G and beyond network security.**

***Index Terms*—5G security, cyber-security, LSTM, intrusion detection systems**

I. Introduction

Wireless communication networks are rapidly progressing with the emergence of fifth-generation (5G) technology standard [1]. These advancements demand a diverse range of requirements, such as high bandwidth, low latency, stability, and reliability [2]. Among the various concerns in networking and telecommunications research, security stands out as a critical area of focus [3]. As the complexity of emerging networks and the number of connected devices continue to grow, prioritizing their security has become paramount. This involves safeguarding the principles of the CIA triad: Confidentiality, Integrity, and Availability, to maintain a robust and secure infrastructure. Looking towards the future, envisioning a mobile network that surpasses the functionalities of 5G or 6G implies the integration of intelligent security protocols and automated security management [4], [5]. Therefore, there is an urgent requirement for an automated security system capable of safeguarding the 5G infrastructure, ensuring the protection of users' privacy and security. Deploying automated security solutions, which function with limited human oversight yet meet high-performance standards, may introduce new challenges, even as they resolve existing security issues.

Machine learning techniques could offer viable solutions to tackle these emerging challenges. Machine learning-based intrusion detection systems (ML-IDS) have the potential to significantly contribute to safeguarding large-scale systems [6]. These systems excel at precisely identifying intrusions and can generalize this acquired knowledge to effectively detect previously unknown threats. However, the proposed ML methods often come with certain drawbacks, notably their high demand for processing power and extensive data collection [7]. In contrast, Federated Learning (FL) offers a relatively novel approach in machine learning that utilizes decentralized processing to enhance privacy and efficiency [8]. Under the Federated Learning paradigm, models are trained on distributed devices, and the results are then aggregated to achieve the final output. This innovative strategy enables multiple devices distributed throughout the network to collectively learn without exposing their local data, thereby greatly enhancing the overall network's security and privacy.

Consequently, in this research, we leverage the Federated Learning approach to create a distributed anomaly detection system within the GPRS Tunneling Protocol (GTP) of a 5G core network to enhance its security and trustworthiness. Specifically, we assess the effectiveness of a Federated Learning Intrusion Detection System (FL-IDS) in detecting two significant attacks: distributed Packet Forwarding Control Protocol (PFCP) and distributed IP spoofing attacks across 5G core networks. These two attacks present substantial threats to the GTP, potentially compromising the system's data integrity, confidentiality, and availability of resources. GTP plays a crucial role in performing essential functions, such as session management and data transmission, making it vulnerable to the impact of these attacks [9]. The proposed approach employs the Long Short-Term Memory (LSTM) model to build the FL-IDS, utilizing collaborative learning techniques. The method harnesses the strength of unsupervised learning, allowing it to learn without requiring labeled data for training. By employing clustering techniques and learning from data patterns, the system categorizes records into two clusters: benign and anomaly. This enables the effective detection of anomalies within the 5G core network without relying on labeled data. The main contribution of this study is summarised as follows:

- Introducing an advanced unsupervised FL-LSTM approach for autonomously identifying cyber attacks aimed at the GTP within 5G core networks.

- Executing simulated scenarios involving distributed PFCP and distributed IP spoofing attacks within a practical 5G core environment, followed by data collection and feature extraction for training.
- Enhancing the model's effectiveness through deployment on a dedicated testing environment and carrying out trials using datasets that reflect real-life conditions and scenarios.

The structure of the paper is as follows. In Section II, you will find a summary of previous research and studies that have used different methods. Section III describes how the testbed was created and how datasets were gathered for the experiment. In Section IV, an unsupervised Federated Learning LSTM model for identifying cyber threats in the 5G network is presented. Section V provides details of the experiment setup and an analysis of the outcomes achieved by the developed model. Finally, Section VI includes our summarizations and recommendations for future work.

II. Related works

Recently, there has been a significant increase in attention towards security issues and potential vulnerabilities within 5G networks. Previous studies have investigated different techniques, including centralized and Federated Learning, to improve anomaly detection efficacy in 5G networks. Thus, this section presents an overview of the advancements made in 5G network security based on recent literature.

Amponis et al. [10] investigated denial-of-service attacks targeting the PFCP within the 5G core infrastructure. Their research unveiled a method involving the transmission of unauthorized session control packets capable of disrupting established 5G tunnels without affecting subscriber connectivity. The paper comprehensively analyzes these identified PFCP DoS attacks and shows their substantial impact. This research also features the implementation of various PFCP-based DoS attack scenarios within the 5G core. Additionally, it offers an intrusion detection dataset that captures network traffic during these attacks, a valuable resource for developing AI/ML-based IDS for the 5G core environment. Park et al. [11] introduce an ML-based approach for detecting signaling DDoS attacks on 5G standalone core networks. The authors analyze 5G signaling characteristics, create labeled datasets using actual and simulated data, and extract statistical features, such as signaling message counts and timing metrics. After feature selection and dimensionality reduction, they evaluate three ML classifiers (support vector machine, random forest, Naive Bayes), with the random forest algorithm achieving over 99% accuracy, recall, and precision in 10-fold cross-validation. However, it acknowledges potential overfitting and dynamic feature engineering requirements while highlighting the system's potential to enhance 5G core security through real-time monitoring. Tian et al. [12] introduce ADSeq-5GCN, a novel framework for detecting anomalies in the 5G Core Network's control plane. ADSeq-5GCN employs sequential data processing and Bi-LSTM sequence modeling to effectively identify anomalies in the network's control plane. Evaluated on a 5GCN testbed with realistic threat scenarios, ADSeq-5GCN's Bi-LSTM model outperforms baseline methods in anomaly detection. However, detection performance is sensitive to the length of the service sequence. Sheikhi and Kostakos [13] proposed an unsupervised Federated Learning approach for identifying DDoS attacks on the 5G core network, specifically aimed at the GTP protocol. The authors utilized an Autoencoder model and designed a 5G testbed architecture to conduct experiments, demonstrating the model's effective identification of DDoS packets with a high detection rate while preserving individual network data privacy. Maimo et al. [14] introduced a 5G-centric framework employing deep learning (DL) for cyber-attack detection. The authors utilized the 5G network infrastructure, specifically ETSI-NFV, and analyzed the botnet dataset CTU to explore anomaly detection in 5G. The Long Short-Term Memory (LSTM) model was used as the DL technique, achieving promising outcomes in effectively classifying traffic within 5G settings.

Consequently, recent studies have highlighted the potential of machine learning approaches in addressing security challenges within 5G networks. However, traditional centralized ML techniques have some limitations that restrict their efficacy on a large scale. To overcome these challenges, distributed learning strategies, like the Federated Learning (FL) framework, have emerged as promising solutions that outperform centralized models in detecting cyber attacks within 5G networks. This study introduces an unsupervised Federated LSTM model specifically designed to identify cyber-attacks in 5G core networks. This model utilizes data generated within the network itself instead of relying on historical datasets. The proposed model shows considerable promise for deployment and utilization in protecting the 5G network infrastructure against cyber threats.

III. Methodology

A. The 5G testing environment

We have created an advanced distributed cyber testing environment that can be used to assess the efficiency of Federated Learning in practical 5G settings. To set up this testing range, we utilized Open5GS and UERANSIM to develop 5G networks. These networks were designed to replicate the functionality of the core 5G infrastructure, which provides a critical structure for implementing the proposed model. Additionally, we can use these networks to simulate potential security breach scenarios and collect GTP data packets.

B. GPRS Tunneling Protocol

GPRS Tunneling Protocol (GTP) is a critical communication protocol for mobile networks, enabling data traffic between eNB/gNB and the 5G core network through GTP tunnels using IP [15]. It supports wireless internet access for mobile subscribers on the move. It is widely used in various network deployments, offering control plane (GTP-C), user plane (GTP-U), and charging traffic capabilities. In

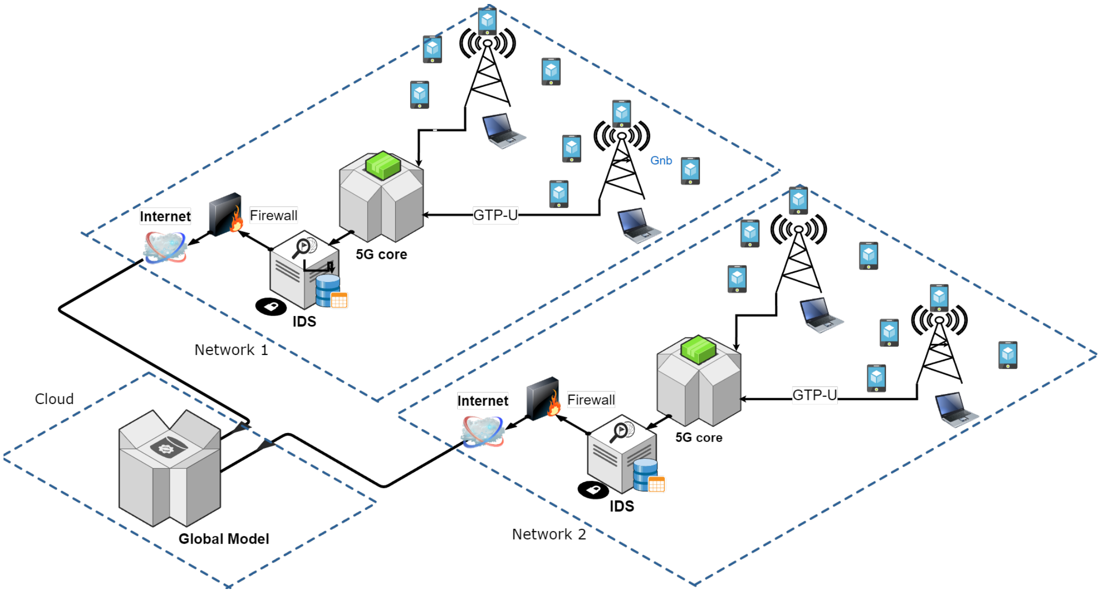

Fig. 1. Environment Architecture for the Development and Deployment of the Proposed Model

this protocol, the client's packets are wrapped in the GTP-U (GTP User Plane) header by the gNB (base station) and sent to the UPF (User Plane Function) via a GTP tunnel [16]. The G-protocol data unit (G-PDU) is constructed with the encapsulated packet and the GTP-U header [17]. In the GTP, upon receiving packets, the system evaluates the most suitable route to the Internet by comparing the destination IP address with entries in the routing table.

C. Simulation of Attack Scenarios

Distributed PFCP attacks and distributed IP spoofing attacks pose significant threats to the security and reliability of 5G networks. In our research, we simulated these attacks in a test environment using three nodes within each 5G core network. As illustrated in Figure 1, our federated prototype consists of three base stations in each 5G, with User Equipment (UE) connected to the core through these stations. To automate the network attacks, we created three malicious nodes and linked each to a different gNB within every 5G core. The simulation was launched three times, employing all three malicious nodes for each specific attack simulation. The list of automated attacks is as follows:

Distributed Packet Forwarding Control Protocol: The Packet Forwarding Control Protocol (PFCP) is important in the 5G core network. Its primary role is to manage packet processing and facilitate the coordination among various functional elements. PFCP mainly operates on the Sx/N4 interface, enabling the initiation, alteration, and termination of Protocol Data Unit (PDU) sessions across the user plane [18]. As outlined in 3GPP, PFCP supports communication between the Session Management Function (SMF) and the User Plane Function (UPF) in the 5G core network [19]. However, there is an imminent threat in the form of distributed PFCP attacks, a variant of Distributed Denial of Service (DDoS) attacks that specifically target the PFCP protocol [20]. These attacks employ multiple sources to flood PFCP interfaces, potentially resulting in service deterioration, loss of connectivity, and disruption to essential network operations.

Distributed IPSpofing: IP spoofing stands as a network attack technique where an attacker hides their actual IP address by modifying the source IP address within network packets [21]. This alteration provides the impression that the traffic originates from a different source. This scheme finds common usage in a variety of attacks, including DDoS attacks [22]. In the 5G core network, IP spoofing involves misrepresenting the source IP address in IP packets exchanged between network components. Attackers employ this tactic to obscure their identity or to bypass security measures that rely on filtering IP addresses [23]. A Distributed IP Spoofing attack on the 5G core network involves multiple assailants falsifying their IP addresses to overwhelm the network with malicious traffic. This is a significant threat because it disrupts regular operations, leads to service interruptions, degrades network performance, and potentially introduces security vulnerabilities.

D. Feature extraction

The initial feature extraction phase begins by gathering GTP packets from the 5G core within the established 5G network testbed, as discussed in the preceding subsection. We harvested raw GTP packets with the Tcpdump tool, used Tshark to extract their features, and then labeled and converted these features into the CSV format for usage. The packets contain various features, some of which are not sufficiently valuable to use for the experiments. Therefore, following the approach of other studies [13], [24], [25], we conducted a thorough analysis of the extracted features to identify the optimal set. This feature selection process aims to enhance model performance while minimizing processing time [26]. The list of features is reported in Table I.

TABLE I
LIST OF NETWORK FEATURES EXTRACTED FOR THE MODEL EVALUATION AND EXPERIMENTS

Feature Category	Specific Features
IP	ip.len,ip.flags.mf ,ip.flags.df , ip.fragment.count, ip.ttl, ip.proto
TCP	tcp.port, tcp.window$_{s}ize, tcp.ack\_raw, tcp.seq$, tcp.len, tcp.stream, tcp.urgent_pointer, tcp.flags, tcp.analysis.ack_rtt, tcp.segments, tcp.ack, tcp.reassembled.length, tcp.time_relative, tcp.time_delta
GTP	gtp.ext_hdr, gtp.ext_hdr.length, gtp.ext_hdr.pdu_type, ,gtp.flags.e, gtp.flags ,gtp.flags.pn, gtp.ext_hdr.pdu gtp.flags.payload, gtp.flags.reserved, gtp.flags.s, gtp.message, gtp.teid ,gtp.flags.version,gtp.length
Quality of Service	qos_flow_id
Session Continuity	pdu_ses_cont.ppp
Timing	frame.time_delta, frame.time_relative
UDP	udp.port, udp.length

E. Data collection and Pre-processing

After extracting and processing the features, we saved them in CSV format, ready to be used in our proposed model.As our study involved a 5G testbed environment comprising two 5G cores, we accordingly partitioned the gathered data for each core. The DDoS data gathered for the distributed PFCP attack were used in the model deployed on the first 5G core, while the distributed IP spoofing attack dataset was prepared for use on the second 5G core. However, we evaluated the federated model's efficiency using test data containing both distributed PFCP and distributed IP spoofing attacks. The summarized information of the collected data is reported in Table II.

TABLE II
DISTRIBUTION OF CLASSES WITHIN THE NETWORK TRAFFIC DATASET

Class	Records	Percentage
Benign	14,932	59.89%
PFCP	4,000	16.04%
IP-spoofing	4,000	16.04%
Total	24,932	100%

IV. PROPOSED MODEL

In the proposed method, we leverage an LSTM, an unsupervised model, for the detection of network anomalies. LSTM models have the ability to capture long-range dependencies and temporal patterns, making them useful for tasks such as Natural Language Processing (NLP), time series prediction, and anomaly detection. A significant advantage of using unsupervised LSTM for anomaly detection is that it eliminates the need for labeled data during training and effectively captures the inherent patterns and structures within the network data. This is particularly crucial for detecting distributed PFCP and distributed IP spoofing, where collecting labeled data might not always be feasible or could involve high costs.

A. Model Architecture

The model integrates an unsupervised LSTM into a Federated Learning structure, enabling distributed training across multiple clients while preserving data confidentiality. Federated Learning ensures that data remains local to each client, enhancing privacy and reducing data transfer overhead. The key steps are:

1) **Local Training:** Each client (e.g., a 5G core) trains its local LSTM model on private data, capturing temporal patterns in network traffic.
2) **Parameter Sharing:** Clients securely send updated model parameters to a central server.
3) **Global Aggregation:** The server aggregates these parameters to update the global model.
4) **Model Distribution:** The updated global model is sent back to clients for further training.
5) **Iteration:** This cycle repeats until the model converges, indicated by a predefined loss threshold.

The network architecture and distribution of IDS components are illustrated in Figure1.

B. Clustering and Anomaly Detection

The proposed LSTM model employs clustering techniques to group similar data points based on their characteristics. During training, it identifies patterns representing normal network behavior. Anomalies are detected as data points that do not fit into these established clusters. The anomaly detection mechanism consists of two main steps:

- **Pattern Recognition:** The LSTM captures long-range dependencies and temporal patterns by analyzing the timing and order of data points, extracting features that characterize normal network behavior.
- **Clustering:** The model groups similar data points into clusters representing normal behavior and flags data points that do not fit into any cluster as anomalies, indicating potential network issues.

The proposed approach combines LSTM's temporal pattern recognition with the privacy-preserving advantages of Federated Learning, providing an efficient and secure method for 5G network anomaly detection.

V. EXPERIMENT AND RESULTS ANALYSIS

This section aims to provide a comprehensive overview of the experimental framework and the outcomes achieved through the suggested methodology. It details the procedural steps of the experiment, the configuration of the test environment, and the metrics used to validate the performance. It also provides an analysis of the results obtained. The information presented in this section will shed light on the effectiveness of the methodology and provide valuable insights for future research endeavors.

A. Experiment setup

The construction of the proposed model and its preliminary processing phases were carried out using the Python-based Keras and TensorFlow frameworks. For the experiments,

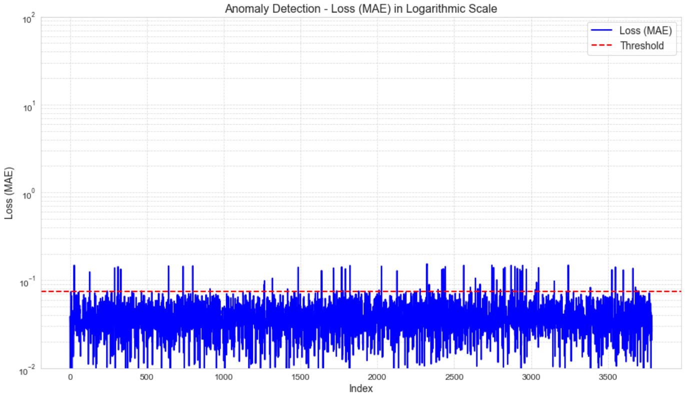

Fig. 2. The clustered records over the threshold.

we adopted the Flower framework to execute the federated learning model, which comprised ten rounds of training. The Federated Averaging (FedAvg) algorithm was employed to aggregate the client updates on the server in the FL global model. To determine the model's performance, we measured it against several metrics, including loss, accuracy, and the F1 score. The loss function serves as a reliable measure of the model's overall capability, with a lower value indicating superior model performance. The initial data processing and setup were performed on a machine powered by an Intel Core i9 processor with 64GB of DDR4 RAM, ensuring the dataset was refined by resolving any missing values labeled as 'nan' or 'null'. The global model was then executed on a Linux-based cloud server, which was configured with 8 VCores and 16GB of operational memory.

B. Result analysis

In the framework of our study on attack scenarios, we carefully designed a setup that includes two distinct 5G core networks, each aimed at replicating a specific type of cyber attack. We then implemented the proposed detection model in each of these 5G cores to identify network-based attacks. Figure 2 displays the clustering outcomes of the final model, obtained after weight aggregation on the test dataset. The presented values represent the performance of the clustering process, indicating that some anomaly records exceed the predefined threshold. The precise setting of the threshold is critical in clustering the records. As illustrated in the figure, while most records fall below the threshold, some instances surpass it, resulting in their classification as anomalies.

The confusion matrix table is another way to assess the model's effectiveness. It demonstrates the actual and predicted values, showcasing the number of correctly and incorrectly clustered records. Therefore, the confusion matrix for the final model is provided in Figure 3, which illustrates robust performance.

Next, we perform a comprehensive analysis of the dataset's features to show their correlations with the final model outcome. Figure 4 demonstrates the top ten most influential features, ranked by their significance. As depicted in Figure 4, it becomes evident that the features "http.request," "tcp.len," and "tcp.window_size" stand out with the strongest correlation rates among all the features within the dataset.

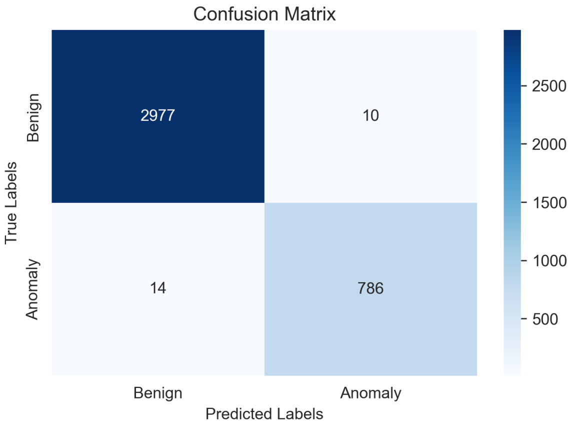

Fig. 3. The confusion matrix.

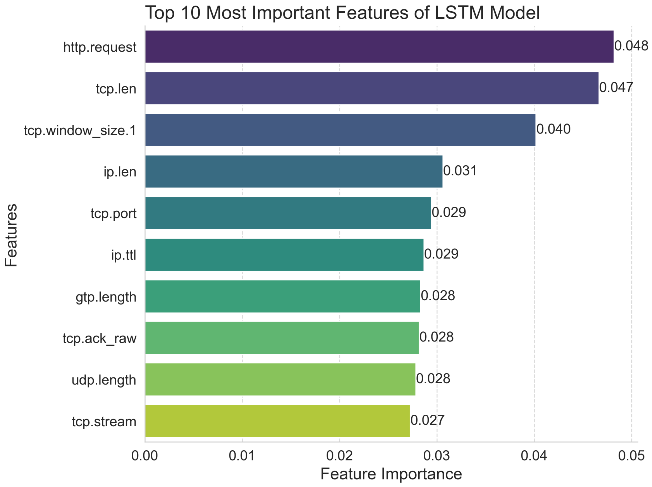

Fig. 4. The top 10 most important features.

In Table III, we present the overall performance evaluation results of our proposed FL-LSTM model for anomaly detection in 5G core networks, alongside comparisons with other established centralized models. The metrics used for evaluation are precision and F-score, which are crucial in assessing the model's ability to distinguish the records while minimizing false positives correctly. The proposed FL-LSTM model outperforms the traditional Autoencoder, K-Means, and SVM models, achieving an impressive precision of 0.9967 and an F-score of 0.9960. These results highlight the superior performance of our FL-LSTM model in effectively detecting anomalies within the 5G core network, demonstrating its potential for enhancing network security and reliability.

VI. Conclusion and Future Work

In this research paper, we present a novel approach for detecting cyber attacks on the 5G core network using un-

TABLE III
PERFORMANCE EVALUATION OF EACH CLIENT

Model	Precision	F-score
Autoencoder	0.4704	0.5451
K-Means	0.9417	0.8545
SVM	0.8460	0.8540
FL-LSTM	0.9967	0.9960

supervised Federated Learning. Our method is based on an LSTM model, which has been demonstrated to be effective in identifying attacks on the 5G network. To evaluate the proposed method, we conducted experiments on a developed publicly-facing 5G testbed architecture. This testbed includes multiple 5G core systems, allowing us to simulate various attack scenarios and generate both malicious and normal traffic. The deployed model was tested on this testbed, utilizing a clustering technique to group records into two clusters, benign traffic, and anomalies, without relying on labeled data. The experimental results showcased the excellent performance of our proposed method, as it achieved a high detection rate while successfully distinguishing between different types of cyber-attacks. Additionally, our work highlights the potential of Federated Learning for security systems in 5G networks, as it facilitates collaborative learning among security systems while preserving user privacy. This study aims to contribute to ongoing efforts and inspire further exploration to address the growing security challenges in 5G networks. To facilitate progress, we recommend developing and evaluating Federated Learning models to combat diverse cybersecurity threats in the 5G context and encourage exploring the integration of our proposed model with other security measures to enhance the overall security of 5G networks.

ACKNOWLEDGMENT

This research has been funded by the European Commission grant IDUNN (101021911) and the Research Council of Finland 6G Flagship Programme (Grant Number: 346208).

REFERENCES

[1] P. Porambage, G. Gür, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6g security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021.

[2] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5g technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles," *IEEE access*, vol. 8, pp. 117 593–117 614, 2020.

[3] M. N. I. Farooqui, J. Arshad, and M. M. Khan, "A bibliometric approach to quantitatively assess current research trends in 5g security," *Library Hi Tech*, vol. 39, no. 4, pp. 1097–1120, 2021.

[4] T. Taleb, C. Benzaïd, M. B. Lopez, K. Mikhaylov, S. Tarkoma, P. Kostakos, N. H. Mahmood, P. Pirinen, M. Matinmikko-Blue, M. Latva-Aho *et al.*, "6g system architecture: A service of services vision," *ITU journal on future and evolving technologies*, vol. 3, no. 3, pp. 710–743, 2022.

[5] M. Banafaa, I. Shayea, J. Din, M. H. Azmi, A. Alashbi, Y. I. Daradkeh, and A. Alhammadi, "6g mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities," *Alexandria Engineering Journal*, 2022.

[6] M. Waqas, S. Tu, Z. Halim, S. U. Rehman, G. Abbas, and Z. H. Abbas, "The role of artificial intelligence and machine learning in wireless networks security: Principle, practice and challenges," *Artificial Intelligence Review*, vol. 55, no. 7, pp. 5215–5261, 2022.

[7] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021.

[8] Y. Liu, X. Yuan, Z. Xiong, J. Kang, X. Wang, and D. Niyato, "Federated learning for 6g communications: Challenges, methods, and future directions," *China Communications*, vol. 17, no. 9, pp. 105–118, 2020.

[9] Y. Kim, Y. Kim, and H. Kim, "A comparison experiment of binary classification for detecting the gtp encapsulated iot ddos traffics in 5g network," *Journal of Internet Technology*, vol. 23, no. 5, pp. 1049–1060, 2022.

[10] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5g core via pfcp dos attacks: the case of blocking uav communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, pp. 1–27, 2022.

[11] S. Park, B. Cho, D. Kim, and I. You, "Machine learning based signaling ddos detection system for 5g stand alone core network," *Applied Sciences*, vol. 12, no. 23, p. 12456, 2022.

[12] Z. Tian, R. Patil, M. Gurusamy, and J. McCloud, "Adseq-5gcn: Anomaly detection from network traffic sequences in 5g core network control plane," in *2023 IEEE 24th International Conference on High Performance Switching and Routing (HPSR)*. IEEE, 2023, pp. 75–82.

[13] S. Sheikhi and P. Kostakos, "Ddos attack detection using unsupervised federated learning for 5g networks and beyond," in *2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2023, pp. 442–447.

[14] L. F. Maimó, Á. L. P. Gómez, F. J. G. Clemente, M. G. Pérez, and G. M. Pérez, "A self-adaptive deep learning-based system for anomaly detection in 5g networks," *Ieee Access*, vol. 6, pp. 7700–7712, 2018.

[15] J.-M. Tilli and R. Kantola, "Data plane protocols and fragmentation for 5g," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2017, pp. 207–213.

[16] S.-L. C. Tsao, "Enhanced gtp: an efficient packet tunneling protocol for general packet radio service," in *ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No. 01CH37240)*, vol. 9. IEEE, 2001, pp. 2819–2823.

[17] T. A. Navarro do Amaral, R. V. Rosa, D. F. C. Moura, and C. Esteve Rothenberg, "Run-time adaptive in-kernel bpf/xdp solution for 5g upf," *Electronics*, vol. 11, no. 7, p. 1022, 2022.

[18] Y. Cao, Y. Chen, and W. Zhou, "Detection of pfcp protocol based on fuzz method," in *2022 2nd International Conference on Computer, Control and Robotics (ICCCR)*. IEEE, 2022, pp. 207–211.

[19] C.-Y. Hsieh, Y.-W. Chang, C. Chen, and J.-C. Chen, "Design and implementation of a generic 5g user plane function development framework," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021, pp. 846–848.

[20] S. Park, S. Kwon, Y. Park, D. Kim, and I. You, "Session management for security systems in 5g standalone network," *IEEE Access*, vol. 10, pp. 73 421–73 436, 2022.

[21] M. Geva, A. Herzberg, and Y. Gev, "Bandwidth distributed denial of service: Attacks and defenses," *IEEE Security & Privacy*, vol. 12, no. 1, pp. 54–61, 2013.

[22] V. Parekh and M. Saravanan, "A hybrid approach to protect server from ip spoofing attack," in *2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES)*. IEEE, 2022, pp. 1–9.

[23] I. H. Abdulqadder, S. Zhou, D. Zou, I. T. Aziz, and S. M. A. Akber, "Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5g networks using ai-based defense mechanisms," *Computer Networks*, vol. 179, p. 107364, 2020.

[24] S. Sheikhi and P. Kostakos, "A novel anomaly-based intrusion detection model using psogwo-optimized bp neural network and ga-based feature selection," *Sensors*, vol. 22, no. 23, p. 9318, 2022.

[25] S. Sheikhi, "An effective fake news detection method using woa-xgbtree algorithm and content-based features," *Applied Soft Computing*, vol. 109, p. 107559, 2021.

[26] S. Sheikhi and P. Kostakos, "Safeguarding cyberspace: Enhancing malicious website detection with pso-optimized xgboost and firefly-based feature selection," *Computers & Security*, p. 103885, 2024.