Blockchain and AI for Collaborative Intrusion Detection in 6G-enabled IoT Networks

Massinissa Chelghoum*, Gueltoum Bendiab†, Mohamed Aymen Labiod‡, Mohamed Benmohammed*, Stavros Shiaeles§ and Abdelhamid Mellouk‡
*LIRE Laboratory, University of Constantine 2- Abdelhamid Mehri, Ali Mendjeli Campus, 25000 Constantine, Algeria,
massinissa.chelghoum@univ-constantine2.dz, mohamed.benmohammed@univ-constantine2.dz
†Department of Electronics, University of Frères Mentouri, LIRE Laboratory, Constantine 25000, Algeria,
bendiab.kelthoum@umc.edu.dz
‡University of Paris-Est Creteil, LISSI, TincNET (CIR), F-94400, Vitry-sur-Seine, France,
mohamed-aymen.labiod@u-pec.fr, mellouk@u-pec.fr
§Centre for Cybercrime and Economic Crime, University of Portsmouth, PO1 2UP, Portsmouth, UK
sshiaeles@ieee.org

***Abstract*—The advent of 6G technology has paved the way for unprecedented advancements in the Internet of Things (IoT), ushering in an era of hyper-connectivity and ubiquitous communication. However, with the proliferation of interconnected devices in 6G-enabled IoT ecosystems, the risk of malicious intrusions and new cyber threats becomes more prominent. Furthermore, the incorporation of AI into 6G networks introduces additional security concerns, such as the risk of adversarial attacks on AI models and the potential misuse of AI for cyber threats. Consequently, securing the extensive and diverse array of connected devices poses a substantial challenge in the 6G environment and needs reconsideration of prior security traditional methods. This paper aims to address these challenges by proposing a novel collaborative intrusion detection system (CIDS) that relies on AI and blockchain technologies. The collaborative nature of the proposed CIDS fosters a collective defense approach, where nodes within the IoT network actively share threat intelligence, enabling rapid response and mitigation. The effectiveness of the proposed system is evaluated through comprehensive simulations and proof-of-concept experiments. The results demonstrate the system's ability to effectively detect and mitigate falsified and zero-day attacks, thereby fortifying the security infrastructure of 6G-enabled IoT environments.**

***Index Terms*—AI, Blockchain, 6G network, Security, Collaborative Intrusion Detection, zero-day attacks, Security**

I. Introduction

6G technology represents the sixth generation in the evolution of wireless communication systems, surpassing its predecessor, 5G, with faster speeds, increased capacity, ultra-low latency, and remarkable bandwidth [1]–[4]. Positioned as the successor to 5G, 6G carries the potential to establish an all-encompassing network environment that seamlessly interconnects humans, devices, and machines [1], [3]. According to a report by Statista, 6G is currently slated to enable a connection density of 107 devices/KM^2, ten times higher than the connection density of 5G, which enables the connection of up to 1 million devices per square kilometer (KM^2) [5]. However, with a more extensive and diverse range of connected devices, 6G networks are expected to offer an expanded attack surface for malicious actors, rendering them more vulnerable to cyber threats and malicious activities [2]–[4]. Furthermore, the integration of artificial intelligence (AI) and machine learning (ML) as a core component of the 6G network [6], may introduce new security challenges mainly related to adversarial attacks on AI models, data integrity, and the security of AI-driven decision-making processes [2]. Network slicing, which is expected to be expanded and improved in 6G, will also introduce new security challenges that will make intrusion detection more difficult for current defense systems [2], [7]. The consequences of sophisticated and zero-day attacks have the potential to evolve into significant threats on the whole 6G network by compromising only one slice [8].

Therefore, innovative techniques for collaborative intrusion detection and threat intelligent sharing in 6G are required to automate forthcoming networks. This paper focuses on solving these issues by proposing a novel Collaborative Network Intrusion Detection System (CNIDS) that relies on Deep Learning (DL) and Blockchain (BC) technologies. DL is employed by the CNIDS to detect and respond to potential attacks by analyzing network abnormalities rather than relying on signature-based methods. In particular, the ability of DL to learn complex patterns and representations from data is crucial for identifying sophisticated patterns associated with different types of zero-day and advanced intrusions. On the other hand, BC serves as a foundation for extensive and reliable sharing and real-time updates of attack instances. This fosters a collective defense mechanism wherein security information is promptly exchanged among participants in the network. Additionally, BC plays an important role in maintaining trust among collaborating entities [9]. The results from the proof-of-concept experiments demonstrate the ability of the proposed system to detect and mitigate falsified and zero-day attacks effectively. More details are provided in the next sections. The rest of the paper is structured as follows: Section 2 provides a summary of relevant publications on the topics of 6G security issues and CNIDSs that rely on blockchain and AI. Next, Section 3 introduces the design and conception of the proposed

system. It also provides a detailed description of the AI-based detection approach. After that, Section 4 presents a prototype that implements and validates the proposed scheme, with a discussion of the obtained results. Finally, Section 5 highlights research gaps and recommendations for future work directions, with proposals and a conclusion.

II. Related work

Recently, various AI-based solutions to detect intrusions, identify malware, and implement mitigation schemes in 6G-enabled IoT networks have been proposed [3], [10]–[12]. In this particular context, researchers in [12] explored the application of diverse learning methods to develop robust intrusion detection systems suitable for deployment in the domain of intelligent and secure vehicular networks, which are one of the industrial verticals in the coming sixth generation (6G) networks. This review study suggested that proactive ML, such as reinforcement learning and imitative learning, is expected to be the new intelligent tool for improving the performance of proactive detection. This expectation holds particular relevance in the context of the exceptionally high network capacity expected in 6G. Within the same context, authors in [10] proposed a hybrid method that relies on Maximum Entropy Inverse Reinforcement Learning (MaxEntIRL) and Multi-agent Reinforcement Learning (MARL) for effective anomaly detection and cyber-attack mitigation in 6G-V2X (Vehicle-to-Everything) Environments. The authors confirmed that their approach achieved an accuracy rate 8.2% higher than that of existing systems.

Ensemble Learning (EL) has been also used by many researchers to develop sophisticated CINDs, threat identification mechanisms, and anomaly detection frameworks for the particular task of securing 6G networks [3], [13]. Specifically, EL can offer a more thorough and efficient safeguard against a broad spectrum of cyber threats and attacks within 6G environments. This can be achieved by leveraging diverse models and combining their outputs [13]. Authors in [3] introduced an anomaly detection system that relies on a hybrid EL technique for securing 6G networks. The proposed method encompasses three key stages: data preprocessing, feature selection, and identification of intrusions. This is achieved through the utilization of a hybrid EL technique, which combines decisions from support vector machines (SVM) and random forests (RF) classifiers, resulting in an enhanced overall performance. The efficacy of this approach has been assessed across various datasets, with distinct sets of features. The most notable performance metrics were observed on the UNSW-NB2015 [14] dataset, where the method achieved an accuracy rate of 99.9% and a false alarm rate of 0.0076%.

Toward the same direction, several Federated Learning (FL)-based solutions have been proposed for more effective intrusion detection in 6G networks, which are expected to be highly distributed and decentralized [3], [15]–[17]. FL aligns well with the characteristics and requirements of 6G networks, offering privacy-preserving, decentralized, and adaptable solutions for intrusion detection while addressing challenges related to latency, security, scalability, and resilience [3], [15]. For instance, in [16], authors proposed a hierarchical FL-based framework for detecting intrusions in 6G. This framework incorporates a lightweight intrusion detection stage to identify abnormal flows as well as a high-level intrusion detection stage that encompasses advanced intrusion detection to gain in-depth insights into malicious flows. Both of these stages are placed at the far edge. In addition, the framework implemented a mitigation mechanism on SDN controllers to determine appropriate countermeasures according to detected attacks. This could be the continuous quarantining of malicious flows, dropping flows, or disabling the flow source to fully minimize its impact. The framework's performance is assessed using the MNIST dataset [11], achieving an accuracy rate of 94.7%.

Blockchain-based IDSs have been proposed for 6G environments to mainly cope with their dynamic nature. These approaches enable the concept of trust-based collaborative distributed intrusion detection (CID) where anomalies can be detected based on the logs and network data shared by different participants in the network. The trustworthiness of participant nodes within the blockchain network is typically determined through the analysis of required information exchanged among CIDS nodes [18]–[22]. For instance, the CIDS proposed in [21] used a permissioned blockchain for saving flow rules produced by SDN controllers when an attack is detected by an IDS in a 6G network. This blockchain consists of SDN firewalls and controllers, with controllers possessing full permissions, including sending, reading, and writing, whereas firewall nodes are limited to receiving and reading. Detection of intrusions is done by a hybrid ML-based detection technique that relies on a Bidirectional Gated Recurrent Neural Network (BiGRNN) in conjunction with the Chaos Game Optimization (CGO) technique. The effectiveness of the proposed CIDS was verified using the Industrial Control System (ICS) Cyber-attack dataset [23], yielding an accuracy rate of 91.50%. Similarly, authors in [22], exploited ML with an IDS that involves three ML algorithms for detecting intrusions in assistance with the Ethereum blockchain for an enhanced trust evaluation. The system is deployed within an Internet of Vehicles (IoV) environment, consisting of network infrastructures, Autonomous Vehicles (AVs), and Road Side Units (RSUs) ts main purpose is to monitor and store intrusion alerts transmitted by AVs to the nearest RSU. Verification of messages from AVs is performed by witness AVs, aimed at minimizing the influence of potentially malicious AVs. The intrusion detection process employs K-Nearest Neighbor (KNN), Naive Bayes (NB), and modified Stochastic Gradient Descent (SGD) as training methods, each producing a locally stored model. Evaluation in the testing phase, using these ML models, yielded a 98% accuracy rate.

In summary, the application of artificial intelligence and blockchain technologies for developing robust CNIDs and mitigation systems, in 6G networks, is currently a prevalent research topic because it offers the best way to detect and respond to potential threats in real-time. However, it remains in its early stages and requires further research.

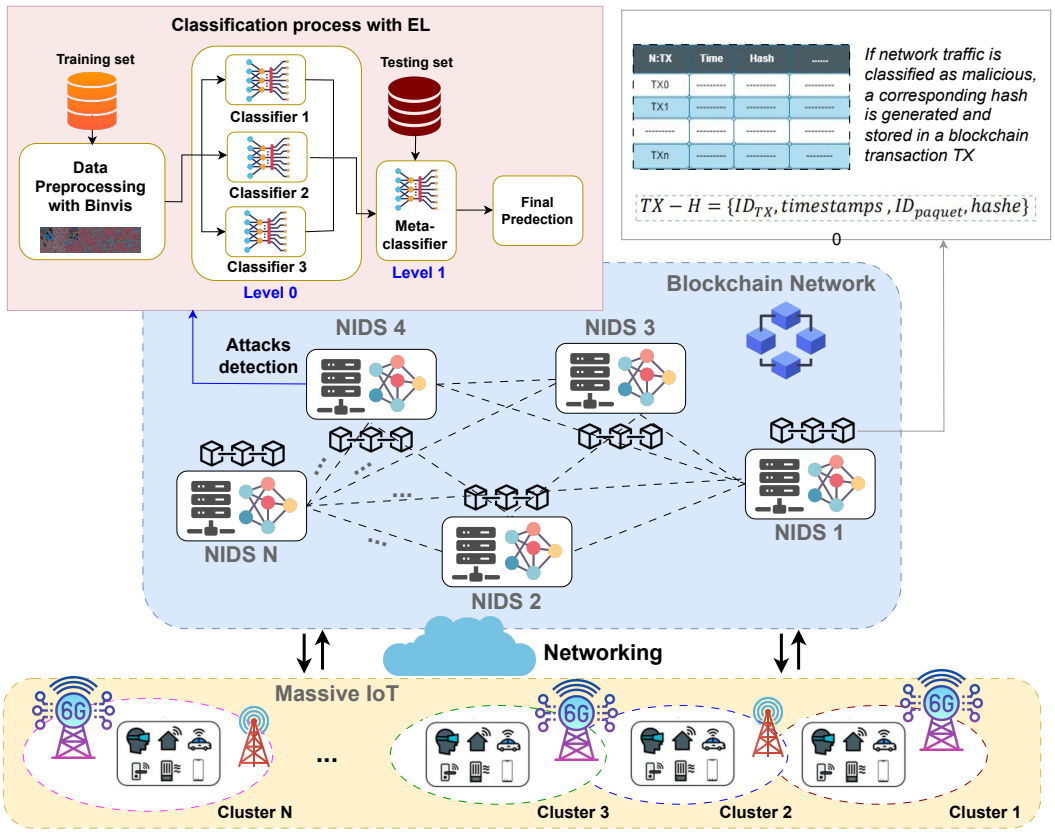


Fig. 1: High-level architecture of the proposed system

III. SYSTEM MODEL

Our collaborative intrusion detection approach is illustrated in Fig. 1, where each Network Intrusion Detection System (NIDS) serves as a node in the blockchain network to monitor real-time incoming traffic in a 6G-enabled IoT environment (e.g., smart hospitals, smart homes, smart supermarkets, etc.). Each NIDS implements an EL-based detection approach that relies on deep learning and visual representation. This approach consists of two main modules: a module for visual representation of network traffic using a visualization tool and a classification module that utilizes deep learning to classify 2D images and identify malicious traffic. As illustrated in Fig. 1, the blockchain is primarily used to store and manage hashes related to attacks identified by the EL-based intrusion detection module in transactions. These will be considered as signatures of these new attacks. These hashes may also be employed in the realm of digital forensics, serving as digital evidence to substantiate claims against malicious entities when requested by a judicial institution. The structure of a transaction in our blockchain (denoted as TX-H) is defined as follows:

$$\text{TX-H} = \{ID_{\text{RT}}, timestamps, ID_{\text{paquet}}, \text{Hash}\} \quad (1)$$

where ID_{RT} is the identifier of the transaction, $timestamps$ is the time of the transaction, whereas ID_{paquet} is the identifier of the network traffic (packet) identified as malicious, while Hash represents the corresponding hash generated through the use of a hashing method (e.g., SHA-256 or SHA-512).

As mentioned before, the classification of network traffic involves two essential steps. Firstly, network traffic streams are converted into 2D images using the visualization tool Binvis. These images are then filtered through a dual-level EL classification module based on deep learning and Convolutional Neural Networks (CNN) models to detect whether the captured network traffic is malicious or not. This approach represents an enhancement of the method in [24]. Specifically, we increased the dataset size to enable the learning model to provide more robust results. Another innovation we introduced is the ensemble learning (EL) method that allows combining the classification decisions from different classifiers to achieve more robust and reliable protection concerning the nature of the captured network traffic. In addition, a blockchain is used as a distributed signature base among the various NIDS nodes in the network. This also ensures collective intelligence, enabling the identification of patterns and suspicious behaviours that might be challenging for an individual NIDS to detect. Actually, the shared information among different NIDSs helps create a more comprehensive view of potential threats.

In our approach, we employed the EL method known as stacked generalization [25], in which a new model learns the optimal way to combine predictions from various existing trained models. As shown in Fig. 1, this method encompasses

two levels; level 0 and level 1. For the level 0 classification, we employed three models, namely Residual Neural Network (ResNet) [26], Dense Convolutional Network (DenseNet) [27], and EfficientNet [28], which are among the most high-performing deep learning models for image classification. We opted for ResNet-50, a 50-layer convolutional neural network consisting of 48 convolutional layers, one MaxPool layer, and one average pool layer. CNN featuring multiple stacked layers often exhibited higher training error percentages compared to models with fewer layers. The introduction of a residual network framework addressed this issue by incorporating shortcut connections and leveraging residual functions. This design enables DNN with stacked layers to mitigate training errors. The direct connections in this architecture facilitate the bypassing of certain layers in the model. For the second model, DenseNet is a CNN featuring dense connections. The fundamental concept is to ensure maximum information transmission between layers in the network, establishing direct connections among all layers. The key characteristic is that each layer in the network is connected not only to the next layer but also directly to every layer in front of it. The input for each layer is derived from the output of all preceding layers. We opted for DenseNet-121 which is a variant of DenseNet with 121 layers. For the last model, EfficientNet, we selected EfficientNet-b1 [28], a variant known for its efficiency in balancing model accuracy and computational resources. EfficientNet introduces a novel compound scaling method that optimizes both the depth, width, and resolution of the network. This approach allows for superior performance while maintaining efficiency in terms of computational costs. At level 1, the data involves using the outputs of the Level 0 sub-models as inputs. Instead of relying on a single model, we employ a Random Forest (RF) Classifier as the meta-learner at Level 1 [29]. The purpose of the meta-learner is to learn the optimal combination of predictions from the Level 0 models, enhancing the overall predictive performance. Thereby, EL combines predictions from multiple models, enhancing flexibility (reducing bias) and reducing sensitivity to specific data (reducing variance). The main methods are bagging, where models are trained in parallel on random subsets, and boosting, where models are trained sequentially, learning from previous mistakes. In our system, we have chosen to use RF, which is an ensemble model using bagging. It employs decision trees as individual models. Each tree is trained on a random subset of the data, contributing to the overall robustness of the model. In essence, RF is a collection of decision trees that work together to improve predictive accuracy and generalization.

IV. Proof-of-concept experiments and results

The simulation experiments were performed on a physical machine running Intel ® Core (TM) i5-10300H CPU @2.5GHz, with 16 GB memory and a Hard disk of 1000 GB SSD. A prototype of the proposed CIDS is implemented. Due to performance constraints, the experiments were carried out in a private Ethereum blockchain environment with two nodes under Linux Ubuntu (ubuntu-22.04.2) by using the packages NodeJS, NPM, Geth (go-Ethereum), and Truffle. Furthermore, a smart contract named "StorageData.sol" was developed and deployed within the private blockchain network utilizing the Truffle framework with Solidity language. The primary objective of this smart contract is to facilitate interaction with intrusion detection systems and record hashes of detected attacks on the blockchain. Interaction with the smart contract is ensured via a front-end web application created using the web3.js API (Application Programming Interface). The intrusion detection system was implemented using Python 3 and the fast.ai library, and a deployed instance of the trained model was deployed on each node within the blockchain.

It is noteworthy to highlight that integrating Ethereum into our solution could potentially introduce performance challenges, particularly in terms of scalability, latency, and privacy considerations. These issues will be tackled in our upcoming research work, where we will delve into alternative consensus mechanisms and federated learning techniques to fine-tune the proposed solution to meet the specific requirements and constraints of 6G networks.

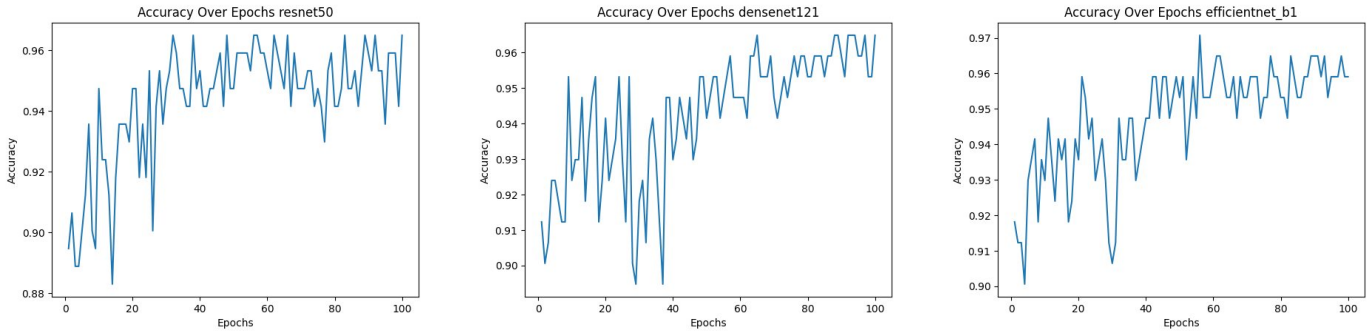
A. Dataset Collection

The dataset, created for training and testing the learning module, comprises 1000 2D images (1024 × 215 pixels) that represent both normal and malicious network traffic. Malicious samples were collected from various public repositories dedicated to malware traffic analysis [30]–[32]. As shown in Fig. 3, the malicious samples represent real-world traffic generated by diverse attack types, including trojans, botnets, IoT-based attacks (DDoS, Keyloggers, OS scans, spyware), backdoors, etc. On the other hand, normal samples represent regular network traffic generated from clean devices within the Cyber-trust testbed [33]. This normal traffic is generated through routine network-intensive activities like copying text and media files across the network, running SSH sessions, streaming media content, and API interactions. The dataset is publicly accessible on the IEEE DataPort website [34].

B. Results and discussion

The implemented CIDS system was tested using the remaining 20% of the datasets after 80% had been used for training the individual learning models in level 0. Notably, these foundational models were trained on a dataset comprising two distinct classes: normal and abnormal network traffic, ensuring a robust foundation for subsequent evaluations." As stated in the previous section, in the level 0 classification process, we have used ResNet50, DenseNet121 and EfficientNet-b1, trained with a batch_size of 8 2D images generated by the binvis tool and with 100 epochs for each of these models.

Graphs in Fig. 2b, Fig.2c and Fig. 2a illustrate the accuracy rates achieved by the three models over 100 epochs, which reached impressive levels: 97.07% for ResNet50, 96.49% for DenseNet121, and a remarkable 97% for EfficientNet-b1. Notably, during this rigorous testing phase, EfficientNet-b1 achieved a superior accuracy rate on the testing dataset, outperforming the other two models.



(a) ResNet50 (b) DenseNet121 (c) EfficientNet-b1

Fig. 2: Accuracy rates over epochs for the three learning models of level 0.

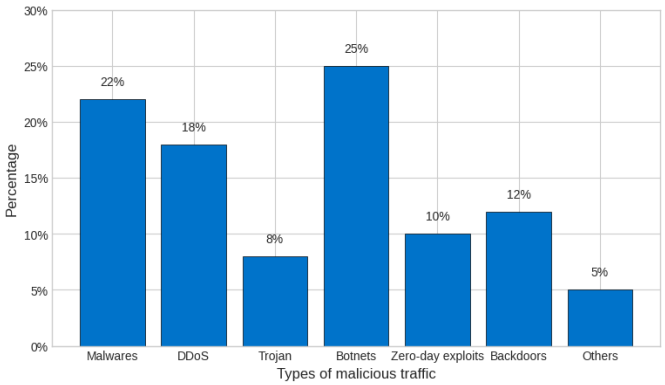


Fig. 3: Distribution of malicious network traffic samples based on malware types

In level 1, we chose the Random Forest classifier to implement the meta-model that takes as input the outputs of the basic models. The implementation of the Random Forest classifier is carried out with the Python sklearn library [35] which is very popular for the implementation of machine learning algorithms as well as the different methods of EL. Following the EL stacking method principle, the predictions from the base models are merged to enable the meta-model to utilize these predictions as input. This facilitates the determination of the best predictions, thereby enhancing predictive performance. After preparing and combining the predictions of basic models, we implemented the Random Forest Classifier with 100 decision trees. After meta-model training, we achieved prediction performance with accuracy rates ranging between 98% and 99%, with a minimum false positive rate equal to 2.3% and reduced error rates during prediction.

Table I provides a summary of the results obtained from the conducted experiments, offering a comparative analysis of various models' performance metrics, including accuracy, precision, recall, F1-score, and false positive rate.

Evaluated models consist of DenseNet121, EfficientNet-b1, ResNet50, and a reference model from a previous study [24], alongside a proposed "Meta-model" for comparison. The Meta-model demonstrates the highest accuracy among all models, closely followed by EfficientNet-b1 and ResNet50, while DenseNet121 achieves slightly lower accuracy. The reference model [24] exhibits the lowest accuracy. This comparison underscores the efficacy of the Meta-model in achieving high accuracy in classification tasks. The stacking method employed enables the Meta-model to leverage predictions from base models, enhancing predictive performance by approximately 2% compared to basic models at level 0. Additionally, the stacking method surpasses the basic methodology presented in [24] by 4-5%, showcasing significant benefits from integrating stacking. The precision of the Meta-model stands notably high at 99.00%, indicating fewer false positive predictions compared to other models, with a false positive rate of 2.3%. This decrease in false alarms enhances confidence in positive predictions and reduces unnecessary alerts. The precision achieved by the meta-model also surpasses that of all other models, standing at an impressive rate of 99.00%, indicating that the meta-model is making fewer false positive predictions compared to other models, with a rate of 2.3%. This results in a decrease in false alarms that can overwhelm security professionals with unnecessary alerts and provide more confidence in the positive predictions it makes.

TABLE I: Comparative analysis of the achieved results

Models	**Accuracy**	**Precision**	**Recall**	**F1-score**	**FP rate**
DenseNet121	96.49%	96.66%	98.48%	96.18%	04.50%
EfficientNet-b1	97.00%	96.96%	98.48%	97.77%	04.00%
ResNet50	97.07%	98.36%	98.59%	97.90%	05.00%
Ref [24]	94.50%	95.78%	94.02%	94.90%	03.00%
Meta-model	99.00%	98.50%	98.80%	98.00%	02.30%

It is also crucial to note that upon identifying network traffic as malicious, the hashes and identifiers of the corresponding pcap files are correctly stored in blockchain transactions. Subsequently, these stored hashes effectively served as attack signatures for all the NIDS within the blockchain.

V. Conclusion

This paper proposes a Collaborative Intrusion Detection System (CIDS) that leverages DL and BC technologies. DL is

employed for its ability to detect and respond to potential attacks by analyzing network abnormalities, while BC facilitates extensive and reliable sharing of real-time updates on attack instances. The integration of these technologies establishes a collective defense mechanism, fostering swift and secure information exchange among network participants. Proof-of-concept experiments showcased the effectiveness of the proposed system in detecting and mitigating falsified and zero-day attacks. The integration of AI-based detection approaches, blockchain for information sharing, and collaborative intrusion detection marks a promising avenue for fortifying the security posture of 6G networks. In the proposed approach, we employed stacked generalization, an ensemble learning method with two levels. At level 0, ResNet-50, DenseNet-121, and EfficientNet-b1 models classify network traffic streams into 2D images. At level 1, an RF-based meta-learner combines predictions from these models, enhancing overall classification accuracy. As future work, we plan to integrate Federated Learning (FL) into our system. FL holds the potential for solving privacy concerns and enhancing model accuracy, particularly in dynamic and distributed network environments characteristic of 6G. Additionally, research efforts will be directed toward developing efficient communication strategies among participating nodes to reduce latency, enhance real-time collaboration, and guarantee the scalability of the proposed CIDS for large-scale networks.

REFERENCES

[1] I. Tomkos, D. Klonidis, E. Pikasis, and S. Theodoridis, "Toward the 6g network era: Opportunities and challenges," *IT Professional*, vol. 22, no. 1, pp. 34–38, 2020.

[2] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[3] M. M. Saeed, R. A. Saeed, M. Abdelhaq, R. Alsaqour, M. K. Hasan, and R. A. Mokhtar, "Anomaly detection in 6g networks using machine learning methods," *Electronics*, vol. 12, no. 15, p. 3300, 2023.

[4] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[5] P. Taylor, "Connection density of 4g, 5g, and 6g mobile broadband technologies." [Online]. Available: http://surl.li/qwynx

[6] F. Tariq, M. R. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6g," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 118–125, 2020.

[7] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, "Ai and 6g security: Opportunities and challenges," in *2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*. IEEE, 2021, pp. 616–621.

[8] T. Seals, "An emerging threat: Attacking 5g via network slices." [Online]. Available: https://www.darkreading.com/threat-intelligence/an-emerging-threat-attacking-5g-via-network-slices

[9] G. Bendiab, A. Hameurlaine, G. Germanos, N. Kolokotronis, and S. Shiaeles, "Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence," *IEEE Transactions on Intelligent Transportation Systems*, 2023.

[10] S. B. Prathiba, G. Raja, S. Anbalagan, K. Arikumar, S. Gurumoorthy, and K. Dev, "A hybrid deep sensor anomaly detection for autonomous vehicles in 6g-v2x environment," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 3, pp. 1246–1255, 2022.

[11] H. Xiao, K. Rasul, and R. Vollgraf, "Fashion-mnist: a novel image dataset for benchmarking machine learning algorithms," *arXiv preprint arXiv:1708.07747*, 2017.

[12] F. Tang, Y. Kawamoto, N. Kato, and J. Liu, "Future intelligent and secure vehicular network toward 6g: Machine-learning approaches," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 292–307, 2019.

[13] M. M. Saeed, R. A. Saeed, A. S. Gaid, R. A. Mokhtar, O. O. Khalifa, and Z. E. Ahmed, "Attacks detection in 6g wireless networks using machine learning," in *2023 9th International Conference on Computer and Communication Engineering (ICCCE)*. IEEE, 2023, pp. 6–11.

[14] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 military communications and information systems conference (MilCIS)*. IEEE, 2015, pp. 1–6.

[15] D. Sirohi, N. Kumar, P. S. Rana, S. Tanwar, R. Iqbal, and M. Hijjii, "Federated learning for 6g-enabled secure communication systems: a comprehensive survey," *Artificial Intelligence Review*, pp. 1–93, 2023.

[16] A. Alotaibi and A. Barnawi, "Idsoft: A federated and softwarized intrusion detection framework for massive internet of things in 6g network," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 6, p. 101575, 2023.

[17] L. J. Vinita and V. Vetriselvi, "Federated learning-based misbehaviour detection on an emergency message dissemination scenario for the 6g-enabled internet of vehicles," *Ad Hoc Networks*, vol. 144, p. 103153, 2023.

[18] L. Alevizos, V. T. Ta, and M. H. Eiza, "A novel efficient dynamic throttling strategy for blockchain-based intrusion detection systems in 6g-enabled vsns," *Sensors*, vol. 23, no. 18, p. 8006, 2023.

[19] A. Razaque, J. Yoo, G. Bektemyssova, M. Alshammari, T. T. Chinibayeva, S. Amanzholova, A. Alotaibi, and D. Umutkulov, "Efficient internet-of-things cyberattack depletion using blockchain-enabled software-defined networking and 6g network technology," *Sensors*, vol. 23, no. 24, p. 9690, 2023.

[20] W. Li and W. Meng, "Bctrustframe: enhancing trust management via blockchain and ipfs in 6g era," *IEEE Network*, vol. 36, no. 4, pp. 120–125, 2022.

[21] S. Sakraoui, M. Derdour, and A. Ahmim, "6g-secureids: Blockchain-enhanced secure knowledge transfer for distributed intrusion detection systems in advanced networks," in *2023 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2023, pp. 1–6.

[22] S. Anbalagan, G. Raja, S. Gurumoorthy, K. Ayyakannu *et al.*, "Blockchain assisted hybrid intrusion detection system in autonomous vehicles for industry 5.0," *IEEE Transactions on Consumer Electronics*, 2023.

[23] T. Morris, "Industrial control system (ics) cyber attack datasets." [Online]. Available: https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets.

[24] G. Bendiab, S. Shiaeles, A. Alruban, and N. Kolokotronis, "Iot malware network traffic classification using visual representation and deep learning," in *2020 6th IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2020, pp. 444–449.

[25] M. Sewell, "Ensemble learning," *RN*, vol. 11, no. 02, pp. 1–34, 2008.

[26] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 770–778.

[27] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 4700–4708.

[28] M. Tan and Q. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *International conference on machine learning*. PMLR, 2019, pp. 6105–6114.

[29] C. Zhang and Y. Ma, *Ensemble machine learning: methods and applications*. Springer, 2012.

[30] "tatsu-i/malware-traffic-analysis.net." [Online]. Available: https://github.com/tatsu-i/malware-traffic-analysis.net

[31] "Publicly available pcap files." [Online]. Available: https://www.netresec.com/?page=PcapFiles

[32] "Malware capture facility project." [Online]. Available: https://www.stratosphereips.org/datasets-malware

[33] "cyber-threat intelligence gathering, detection, and mitigation platform." [Online]. Available: https://cyber-trust.eu/

[34] "913 malicious network traffic pcaps and binary visualisation images dataset." [Online]. Available: http://surl.li/phlcz

[35] "scikit-learn machine learning in python." [Online]. Available: https://scikit-learn.org/stable/