


# Leveraging Deep Learning for Intrusion Detection in IoT Through Visualized Network Data

Amine Hattak<sup>1,3</sup>, Fabio Martinelli<sup>1</sup>, Francesco Mercaldo<sup>2,1</sup> <sup>a</sup> and Antonella Santone<sup>1</sup>

<sup>1</sup>*Institute for Informatics and Telematics, National Research Council of Italy (CNR), Pisa, Italy*

<sup>2</sup>*University of Molise, Campobasso, Italy*

<sup>3</sup>*La Sapienza, University of Rome, Rome, Italy*

**Keywords:** Internet of Things, Network Traffic Classification, Deep Learning, Network Intrusion Detection, Security.

**Abstract:** In an era marked by increasing reliance on digital technology, the security of interconnected devices and networks has become a paramount concern in the realm of information technology. Recognizing the pivotal role of network analysis in identifying and thwarting cyber threats, this paper delves into network security, specifically targeting the classification of network traffic using deep learning techniques within the Internet of Things (IoT) ecosystem. This paper introduces a deep learning-based approach tailored for traffic classification, beginning with raw traffic data in PCAP format. This data undergoes a transformation into visualized images, which serve as input for deep learning models designed to differentiate between benign and malicious activities. We evaluate the efficacy of our proposed method using the TON\_IoT dataset (Dr Nickolaos Koroniotis, 2021), comprising 10 network traces across two categories: nine related to diverse vulnerability scenarios and one associated with a trusted application. Our results showcase an impressive accuracy of 99.1%, underscoring the potential of our approach in bolstering network security within IoT environments.


## 1 INTRODUCTION AND RELATED WORK

The Internet of Things (IoT) has emerged as a transformative force, revolutionizing how we interact with technology and the world around us. With billions of interconnected devices spanning various domains such as smart homes, healthcare systems, industrial facilities, and transportation networks, IoT has unleashed unprecedented levels of connectivity, efficiency, and convenience. However, this interconnected ecosystem also presents a fertile ground for cyber threats, with the potential to disrupt and undermine the very fabric of IoT infrastructure.

Cyber-attacks targeting IoT devices have become increasingly prevalent and sophisticated. These attacks pose significant risks to both individual privacy and broader societal security, by exploiting vulnerabilities in IoT devices, ranging from weak authentication mechanisms and insecure communication protocols to inadequate software patching and configuration errors. Such vulnerabilities not only compro-

mise the confidentiality, integrity, and availability of data transmitted by IoT devices but also enable malicious actors to orchestrate large-scale disruptions and attacks. From distributed denial-of-service (DDoS) (Sonar and Upadhyay, 2014) assaults leveraging compromised IoT botnets (Kolias et al., 2017) to ransomware (Yaqoob et al., 2017) campaigns targeting vulnerable smart devices, the threat landscape facing the IoT domain is diverse and evolving, for example we can find also some cyber-attacks such as MITM (Li et al., 2017). Moreover, the consequences of successful cyber-attacks on IoT infrastructure can be far-reaching, potentially leading to physical harm, financial losses, and reputational damage for individuals, organizations, and entire industries. As IoT continues to proliferate and integrate into every aspect of modern life, safeguarding this interconnected ecosystem against cyber-threats has become an imperative. Effective cybersecurity strategies must encompass robust measures for device authentication, data encryption, intrusion detection, and incident response to mitigate the ever-present risks posed by malicious actors (Vishwakarma and Jain, 2020).

In a research work (Hattak et al., 2023) presents a

<sup>a</sup>  <https://orcid.org/0000-0002-9425-1657>

novel approach to network traffic classification using Deep Learning (Mercaldo et al., 2022; Huang et al., 2023) techniques. This work introduces an innovative approach that combines Deep Learning with image-based representations (Huang et al., 2024a; Huang et al., 2024b) to achieve robust and explainable network traffic classification. The authors of the following work (Moustafa, 2021) introduce a distributed architecture for assessing AI-based security systems at the edge using the TON\_IoT datasets. It focuses on enhancing security measures in IoT networks through innovative architectural approaches. The study (Booij et al., 2021) emphasizes the importance of standardizing features and attack types in IoT network intrusion datasets like ToN\_IoT. It highlights the role of heterogeneity in enhancing the effectiveness of intrusion detection systems within IoT environments. In another work (Martinelli et al., 2022) the authors proposed an intrusion detection method for the smart grid. Starting from network traffic packet files, they have computed a feature vector composed by 26 different features. By exploiting supervised machine learning, they built seven different models, obtaining with five of seven models and they achieved high scores in terms of precision and recall.

In this paper, we present deep-learning based approach to address these security concerns by detecting intrusions in The IoT ecosystem. By harnessing visualization techniques, we convert raw captured network traffic files from PCAP format into images, enabling enhanced analysis and detection capabilities.

## 2 THE METHOD

In this study, we introduce a method for image-based network traffic classification leveraging deep learning models focusing on the IoT domain. Our proposed method aims to substantiate the accuracy and resilience of intrusion detection systems through the integration of image analysis techniques for the IoT ecosystem. To elucidate our proposed methodology, we delineate it into distinct steps, illustrated in Figure 1. This graphical representation expounds our envisioned approach for evaluating network intrusion detection and prediction using deep learning models. The initial step undertake the collection of samples or a dataset for captured network traffic in an IoT ecosystem, comprising both "normal" and "malware" traces. It is imperative to meticulously label each sample and categorize them into distinct families to ensure the robustness of subsequent model training and evaluation. This curated dataset serves as the foundation for training and testing the deep learning models. We will do

that in two approaches to compare which one is the best for such tasks.

The primary strategy revolves around binary classification, which entails distinguishing between two classes: "Normal" and "Attack." Here, the focus is on segregating network traffic into either of these categories, where normal traffic signifies typical, benign communication, while the "Attack" class encapsulates any anomalous or malicious activities detected within the network. Expanding upon this foundational approach, the research endeavors to delve deeper into network traffic analysis by adopting a more nuanced 10-class classification scheme. This expanded framework involves the classification of network traffic into a diverse families, each representing distinct types of activities or communication patterns. By adopting a multi-class classification approach, the research aims to enhance the granularity of network traffic analysis, enabling more detailed insights into the diverse nature of network activities. This comprehensive classification scheme not only facilitates the identification of malicious behavior but also provides valuable contextual information about the nature and origins of various network activities, thereby augmenting the overall effectiveness of intrusion detection and network security measures.

The raw network traffic data will be pre-processed to remove any irrelevant information or noise that can affect the classification task. Moreover we will transform both the packet header and the packets payloads to ensure the robustness and the flexibility of our approach for network intrusion detection in IoT. This approach is helpful in two scenarios encrypted and non-encrypted network traffic. If the traffic is encrypted, then the bytes that comprise the packet payload would be random and indistinguishable from noise. In this case, it's not feasible to create meaningful images directly from the encrypted payload bytes. However, to generate images from encrypted traffic for visualization purposes, we need to take a different approach. One possible approach is to focus on the packet headers or metadata rather than the payload. Packet headers contain crucial information for network communication and analysis, such information can be summarized in the source and destination addresses, protocols, ports, total length, fragment offset, time to live (TTL), options. Subsequently, we advocate for the transformation of network data, presented in PCAP format, into visualized images, marking the second step of our proposed method. This transformation renders the data suitable for consumption by deep learning models, enabling seamless integration into training and testing workflows. Notably, image generation can be conducted in either grayscale or

color (RGB) modes to accommodate specific requirements. Following this, the subsequent step entails resizing the input images to ensure uniformity in dimensions, a prerequisite to mitigate the potential loss of information that could undermine the accuracy of deep learning models. These models are then meticulously trained and evaluated on the curated dataset, with performance metrics gauged against the classification task.

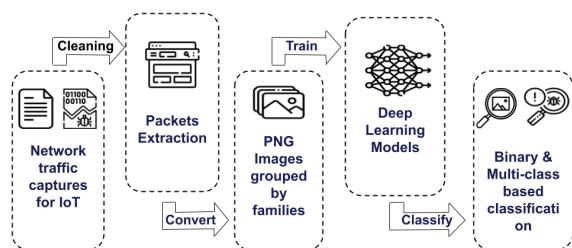


Figure 1: Overall schema of the method.

In this work we introduce a novel methodology for image-based network traffic classification, focusing on the IoT domain and leveraging deep learning models. The proposed method aims to enhance the accuracy and resilience of intrusion detection systems by integrating image analysis techniques tailored to the IoT ecosystem. The methodology involves several key steps, beginning with the collection and labeling of a dataset comprising both "normal" and "malware" traces of network traffic. Two approaches are explored: binary classification, distinguishing between "Normal" and "Attack" classes, and a more nuanced 10-class classification scheme, offering detailed insights into diverse network activities. Pre-processing of raw network traffic data involves removing noise and transforming packet headers and payloads to ensure robustness and flexibility, applicable to both encrypted and non-encrypted traffic. Visualized images are generated from PCAP-formatted network data, followed by resizing for uniformity. Finally, deep learning models are trained and evaluated on the curated dataset to gauge performance against the classification task, thus validating the effectiveness of the proposed methodology.

### 3 EXPERIMENTAL ANALYSIS

This section, we outline the experiment undertaken to validate the efficacy of the proposed methodology. Initially, we delineate the (real-world) datasets selected for analysis, followed by a presentation of the experimental results.

#### 3.1 Experimental Setup

The experiments were conducted on a workstation equipped with an Intel Core i7 11th generation processor (2.3 GHz), 16GB of RAM, and an NVIDIA GeForce RTX 3070 GPU. The operating system used was Ubuntu 22.04.2 LTS (GNU/Linux 5.15.133.1-microsoft-standard-WSL2 x86\_64). Python 3.8 along with TensorFlow 2.4 and PyTorch 1.7 libraries were utilized for model training and evaluation. All experiments were run using a freely use tool for malware analysis represented as images (Iadarola et al., 2021).

#### 3.2 Dataset

The TON\_IoT dataset has been used in research works related to cybersecurity and intrusion detection systems. One such research work is "Analysis of ToN\_IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT" published in the journal Applied Sciences in 2022 (Tareq et al., 2022). The study conducted a complete investigation of the ToN\_IoT database to train models for cybersecurity. The TON\_IoT Telemetry Dataset has also been mentioned as a new generation dataset for data-driven intrusion detection systems (Alsaedi et al., 2020). Additionally, the TON\_IoT dataset is available for academic research purposes and has been used in the development of realistic botnet datasets for network forensic analytics (Dr Nickolaos Koroniotis, 2021).

The TON\_IoT dataset represents a cutting-edge collection of datasets tailored for evaluating the efficacy and fidelity of various cybersecurity applications based on Artificial Intelligence (AI) within the realms of Industry 4.0/Internet of Things (IoT) and Industrial IoT (IIoT) systems. Referred to as 'ToN\_IoT', these datasets encompass a diverse range of data sources gathered from Telemetry datasets of IoT and IIoT sensors, Operating systems datasets of Windows 7 and 10, Ubuntu 14 and 18 TLS, as well as Network traffic datasets. The datasets were meticulously curated from a realistic and large-scale network environment established at the IoT Lab of UNSW Canberra Cyber, School of Engineering and Information Technology (SEIT), UNSW Canberra @ the Australian Defence Force Academy (ADFA) (UNS, 2024). The TON\_IoT datasets are designed to facilitate the validation and testing of a multitude of cybersecurity applications such as intrusion detection, threat intelligence, malware detection, fraud detection, privacy preservation, digital forensics, adversarial machine learning, and threat hunting. These datasets are freely available for academic research purposes, perpetually granting access to scholarly exploration. For com-

mercial use, permission from the author, Dr. Nour Moustafa, is required. The dataset directories encompass raw datasets including IoT/IIoT data logged in log and CSV files from various sensors like weather and Modbus sensors, network datasets in PCAP formats from ZEEK (Bro) tool (Author(s), 2020) (Author(s), 2023), and Linux datasets captured through tracing tools on Ubuntu systems. The TON\_IoT dataset serves as a valuable resource for training Machine Learning and Deep Learning algorithms to enhance cybersecurity measures within IoT ecosystems. Overall, the TON\_IoT dataset stands as a pivotal resource for researchers delving into cybersecurity applications within IoT environments, offering a rich source of heterogeneous data to drive advancements in intrusion detection systems and other AI-based security solutions. Tables 1 describes in detail the stats network dataset of Ton.IoT.

Table 1: Statistics of Network Records for Ton.IoT network dataset.

Type	No of rows
Backdoor	508116
DDoS	6165008
DOS	375328
Injection	452659
MITM	1052
Password	1718568
Ransomware	72805
Scanning	7140161
XSS	2108944
Normal	796380

In this work we have used the networked datasets in PCAP format which was captured using Zeek tool. After the pre-processing and transformation into image we split the samples are divided into three sets: training, validation, and test, with a split ratio of 80:10:10 respectively. For both datasets (the binary and multi-class datasets) there are 2,764 samples in the test set, while the training set consists of 24,806 samples, which are further split into 22,053 specifically for training and the remaining 2,753 for validation. The samples from each family are evenly distributed among the sets to ensure a balanced distribution.

### 3.3 Image Generation

The process of converting captured network data in PCAP format to an image is a method of visualizing network traffic data in a more intuitive and human-readable format, while also providing valuable input for training deep learning models. This approach allows for the analysis and interpretation of network

traffic patterns more efficiently and effectively by identifying trends and anomalies in network traffic that may not be immediately apparent in the raw data. The process typically involves first reading the binary data of the PCAP file extracting the packets header which contains information such as source and destination IP addresses, port numbers, protocol types, packet sizes, etc. After that calculating the size of the image, reshaping the data to create a 2D array, and finally, converting the data to an image using an image processing library. Depending on the requirement, the image can be in grayscale or RGB mode. The grayscale image is created by using the same data for all three channels (red, green, and blue) and reshaping it according to the image size. The RGB image is created by creating three separate arrays for red, green, and blue channels, and then stacking them together to create the final data array. This later will be used to generate the RGB images. The generated images through this process will be used as input for training various deep-learning models. The ability of deep learning models to automatically extract features and patterns from images makes them well-suited for analyzing IoT network traffic data. Furthermore, the ability to create a large dataset of network traffic images will be used to train and evaluate different deep learning architectures, such as models that are known in the literature (MobileNet, VGG16, etc).

The main function "process\_pcap(pcap\_path)" is defined to handle packet processing. It initializes an empty list "current.bytes" to accumulate bytes from packets, then iterates through each packet in the PCAP file using "rdpcap(pcap\_path)". then for each packet it extracts the raw bytes from the packet and appends them to current.bytes if the accumulated bytes exceed the maximum size allowed for an image: it creates an image from the accumulated bytes using create\_image() function, it constructs a filename based on the packet summary and the number of accumulated bytes. Saves the image to the specified output directory, it resets current.bytes to an empty list to start accumulating bytes for the next image, after processing all packets: If there are remaining bytes in current.bytes, it creates an image and saves it using the same procedure as above.

Finally, images are generated from the accumulated bytes of packets, ensuring that no information is lost during the process. Each image filename reflects the packet summary and the size of accumulated bytes, providing context about the data used to generate the image. The figure 2 represents the final output from PCAP to image. It is obviously that different network traffic are generating different images with distinguishable features for each family.

**Data:** PCAP

**Result:** Generating PNG images initialization;

```

while Packets are not finished do
    Extract raw bytes from the packet and
    append them to current_bytes;
    if accumulated bytes exceed maximum
    size allowed for an image then
        Create an image from accumulated
        bytes using create_image()
        function Construct a filename based
        on packet summary and the number
        of accumulated bytes;
        Save the image to the specified output
        directory;
        Reset current_bytes to an empty list
        to start;
        accumulating bytes for the next
        image;
    else
        there are remaining bytes in
        current_bytes Create an image and
        save it using the same procedure as
        above;
    end
end
    
```

Algorithm 1: From PCAP to PNG Image.

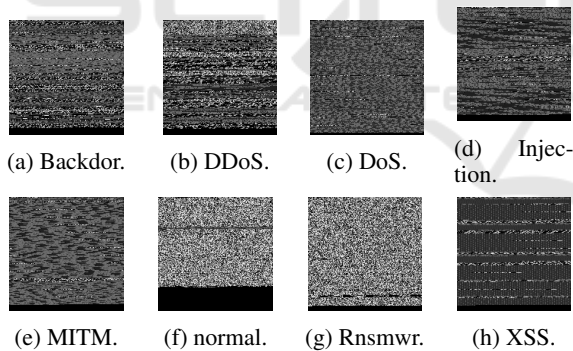


Figure 2: A visualization analysis of some network traffic classes of Ton\_IoT dataset.

Our proposed methodology integrates deep learning techniques with visualization of recorded network traffic in PCAP format to detect intrusions in the IoT ecosystem. Initially, raw PCAP files containing network traffic data are preprocessed and transformed into visual representations using image conversion techniques. These visualized datasets are then fed into a deep-learning model for training and evaluation. We employ deep learning models for their ability to extract spatial features from images and detect patterns indicative of intrusions.

### 3.4 Deep Learning Models for IoT Network Analysis

Deep learning models play a crucial role in analyzing IoT network data, offering powerful capabilities for traffic classification and anomaly detection. Three prominent models, CNN (Convolutional Neural Networks), MobileNet, ResNet50, and VGG16, each bring unique advantages to IoT network analysis. The following are some advantages of using such models in IoT network traffic analysis image-based:

#### Convolutional Neural Networks (CNN)

- CNNs excel in feature extraction from complex data, making them ideal for IoT traffic classification
- They can handle both low-dimensional and high-dimensional features simultaneously, enhancing robustness in classification tasks
- CNN models efficiently recognize patterns in datasets and are effective in detecting anomalies in sequential data

#### MobileNet

- MobileNet is specifically designed for mobile and edge devices, offering efficient on-device processing capabilities for IoT applications
- Its architecture enables lightweight and fast inference suitable for resource-constrained environments like IoT networks

#### ResNet50

- ResNet50 is known for its deep architecture with residual connections that facilitate training of very deep networks effectively
- The residual connections help mitigate issues like gradient vanishing and network degradation, common in overly complex models

#### VGG16

- VGG16 is recognized for its simplicity and effectiveness in image classification tasks, making it a strong candidate for IoT traffic analysis
- Its architecture with 16 layers strikes a balance between depth and complexity, offering a good compromise for efficient feature extraction

In conclusion, leveraging CNNs like MobileNet, ResNet50, and VGG16 in IoT network analysis provides a diverse set of tools with distinct advantages. These models enable efficient traffic classification, anomaly detection, and feature extraction critical for optimizing IoT network performance and security.

### 3.5 Results and Discussion

Table 2 presents the hyperparameters utilized for various deep learning (DL) models in the context of the research work. These parameters are critical as they directly influence the performance and efficiency of the models in processing and analyzing network traffic data.

The models encompassed in this study include CNN (Convolutional Neural Network), MobileNet, ResNet50, and VGG16, each distinguished by unique architectures and capabilities suited for various tasks within network traffic analysis and intrusion detection. Standardized input dimensions of 224x224 pixels with three RGB color channels are maintained across all models to ensure consistency and comparability in the experimental setup. The pivotal parameters of epochs and batch size, crucial for the training process of DL models, involve a configuration of 40 epochs and a batch size of 32 across all models, striking a balance between computational efficiency and model convergence. Additionally, the depth of DL models, denoted by the number of layers, significantly impacts their ability to extract intricate patterns and features from input data. Specifically, the table specifies the layer count for each model: CNN (13 layers), MobileNet (29 layers), ResNet50 (50 layers), and VGG16 (16 layers), reflecting the diversity in architectural complexity employed during the experimentation phase.

The table (Table 3) provides a comparison between the performance results of different machine learning models on test sets for binary (2 classes) and multi-class (10 classes) classification tasks. The models evaluated include Convolutional Neural Network (CNN), MobileNet, ResNet50, and VGG16.

For the binary classification task (2 classes), the performance metrics reported include accuracy (Acc), precision (Prec), recall (Rec), F1-score (F1), and area under the receiver operating characteristic curve (AUC). Similarly, for the multi-class classification task (10 classes), the same performance metrics are provided.

The results indicate that across all models, the performance is generally higher for the binary classification task compared to the multi-class classification task. This discrepancy is expected as binary classification tasks are inherently simpler compared to multi-class classification tasks.

Among the models evaluated, CNN consistently achieves the highest performance across both binary and multi-class classification tasks, with accuracy, precision, recall, F1-score, and AUC values exceeding 0.9 for both tasks. This suggests that CNN is ef-

fective in capturing the underlying patterns in the data and making accurate predictions.

MobileNet, ResNet50, and VGG16 also demonstrate strong performance across both classification tasks, with accuracy values ranging from approximately 0.9 to 0.95 for the binary classification task and from approximately 0.9 to 0.95 for the multi-class classification task. These results indicate that these models are capable of achieving high levels of accuracy and reliability in classifying images across different categories.

Overall, the performance results presented in the table highlight the effectiveness of deep learning models, particularly CNN, in image classification tasks. These findings can inform the selection of appropriate machine learning models for similar classification tasks in practical applications.

## 4 CONCLUSIONS

In this paper, we proposed a visualized technique for network analysis focusing on IoT ecosystem aimed to automatically discriminate between legitimate and malicious network traces. In detail, we propose to extract the packet headers that contain information about the source and destination addresses, protocols, ports, and other relevant metadata in case of encrypted traffic, to represent these network traces in terms of images which will play a role as input for several deep-learning models to detect the application that generated the specific network trace. We have achieved a score of 99.1% in terms of Accuracy of the binary classification task.

As future work, we plan to consider more recent deep-learning algorithms such as Vision Transformers (ViT), in order to evaluate the approach's robustness, and we also plan to evaluate the resilience of the proposed approach in real scenarios.

## ACKNOWLEDGEMENTS

This work has been partially supported by EU DUCA, EU CyberSecPro, EU E-CORRIDOR projects, PNRR SERICS\_SPOKE1\_DISE, RdS 2022-2024 cybersecurity, FORESEEN: FORMal mEthodS for attack dEtEction in autonomous drivINg systems (CUP H53D23008210001), MUR - REASONING: foRmal mEthods for computAtional analySis for diagnOsis and progNosis in imagING - PRIN, e-DAI (Digital ecosystem for integrated analysis of heterogeneous health data related to high-impact diseases: innovative model of care and research), Health Opera-

Table 2: The hyperparameters of different DL models.

Model	CNN	MobileNet	ResNet50	VGG16
Input image/vector size	224x224x3			
Epochs and Batch size	40 - 32			
Number of layers	13	29	50	16

Table 3: Comparison between the results of different models on the test sets (binary and 10 classes classification).

Mode	2 classes					10 classes					
	Model	Acc	Prec	Rec	F1	Auc	Acc	Prec	Rec	F1	Auc
CNN	0.991	0.991	0.991	0.991	0.991	0.993	0.899	0.904	0.896	0.9	0.981
MobileNet	0.916	0.917	0.913	0.915	0.915	0.975	0.916	0.919	0.915	0.917	0.977
ResNet50	0.952	0.954	0.951	0.952	0.952	0.99	0.948	0.949	0.947	0.948	0.989
VGG16	0.945	0.95	0.944	0.947	0.947	0.991	0.948	0.95	0.946	0.948	0.994

tional Plan, FSC 2014-2020, PRIN-MUR-Ministry of Health and the National Plan for NRRP Complementary Investments D<sup>3</sup> 4 Health: Digital Driven Diagnostics, prognostics and therapeutics for sustainable Health care and Progetto MolisCTe, Ministero delle Imprese e del Made in Italy, Italy, CUP: D33B2200060001 projects.

This work has been carried out within the Italian National Doctorate on Artificial Intelligence run by the Sapienza University of Rome in collaboration with the Institute of Informatics and Telematics (IIT), National Research Council of Italy (CNR).

## REFERENCES

(2024). School of engineering and technology. <https://www.unsw.edu.au/canberra/about-us/our-schools/engineering-technology>.

Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., and Anwar, A. (2020). Ton\_iot telemetry dataset: A new generation dataset of iot and iiot for data-driven intrusion detection systems. *Ieee Access*, 8:165130–165150.

Author(s) (2020). zeek-osquery: Host-network correlation for ... *arXiv preprint arXiv:2002.04547*.

Author(s) (2023). Introducing uwf-zeekdata22: A comprehensive network traffic ... *Journal Name*, 8(1):18.

Booij, T. M., Chiscop, I., Meeuwissen, E., Moustafa, N., and Den Hartog, F. T. (2021). Ton\_iot: The role of heterogeneity and the need for standardization of features and attack types in iot network intrusion data sets. *IEEE Internet of Things Journal*, 9(1):485–496.

Dr Nickolaos Koroniotis, D. N. M. (2021). The bot-iot dataset. <https://research.unsw.edu.au/projects/bot-iot-dataset>.

Hattak, A., Iadarola, G., Martinelli, F., Mercaldo, F., Santone, A., et al. (2023). A method for robust and explainable image-based network traffic classification with deep learning. In *Proceedings of the 20th International Conference on Security and Cryptography*, pages 385–393.

Huang, P., Li, C., He, P., Xiao, H., Ping, Y., Feng, P., Tian, S., Chen, H., Mercaldo, F., Santone, A., et al. (2024a). Mamlformer: Priori-experience guiding transformer network via manifold adversarial multi-modal learning for laryngeal histopathological grading. *Information Fusion*, page 102333.

Huang, P., Xiao, H., He, P., Li, C., Guo, X., Tian, S., Feng, P., Chen, H., Sun, Y., Mercaldo, F., et al. (2024b). La-vit: A network with transformers constrained by learned-parameter-free attention for interpretable grading in a new laryngeal histopathology image dataset. *IEEE Journal of Biomedical and Health Informatics*.

Huang, P., Zhou, X., He, P., Feng, P., Tian, S., Sun, Y., Mercaldo, F., Santone, A., Qin, J., and Xiao, H. (2023). Interpretable laryngeal tumor grading of histopathological images via depth domain adaptive network with integration gradient cam and priori experience-guided attention. *Computers in Biology and Medicine*, 154:106447.

Iadarola, G., Casolare, R., Martinelli, F., Mercaldo, F., Peluso, C., and Santone, A. (2021). A semi-automated explainability-driven approach for malware analysis through deep learning. In *2021 International Joint Conference on Neural Networks (IJCNN)*, pages 1–8. IEEE.

Kolias, C., Kambourakis, G., Stavrou, A., and Voas, J. (2017). Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84.

Li, C., Qin, Z., Novak, E., and Li, Q. (2017). Securing sdn infrastructure of iot-fog networks from mitm attacks. *IEEE Internet of Things Journal*, 4(5):1156–1164.

Martinelli, F., Mercaldo, F., and Santone, A. (2022). A method for intrusion detection in smart grid. *Procedia Computer Science*, 207:327–334.

Mercaldo, F., Zhou, X., Huang, P., Martinelli, F., and Santone, A. (2022). Machine learning for uterine cervix screening. In *2022 IEEE 22nd International Conference on Bioinformatics and Bioengineering (BIBE)*, pages 71–74. IEEE.

Moustafa, N. (2021). A new distributed architecture for evaluating ai-based security systems at the edge: Network ton\_iot datasets. *Sustainable Cities and Society*, 72:102994.

- Sonar, K. and Upadhyay, H. (2014). A survey: Ddos attack on internet of things. *International Journal of Engineering Research and Development*, 10(11):58–63.
- Tareq, I., Elbagoury, B. M., El-Regaily, S., and El-Horbaty, E.-S. M. (2022). Analysis of ton-iot, unw-nb15, and edge-iiot datasets using dl in cybersecurity for iot. *Applied Sciences*, 12(19).
- Vishwakarma, R. and Jain, A. K. (2020). A survey of ddos attacking techniques and defence mechanisms in the iot network. *Telecommunication systems*, 73(1):3–25.
- Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., and Guizani, M. (2017). The rise of ransomware and emerging security challenges in the internet of things. *Computer Networks*, 129:444–458.

