A_Comparative_Study__on_IoT__Device_Identification_an...

Turnitin

Document Details

Submission ID

trn:oid:::30744:104078353

Submission Date

Jul 10, 2025, 9:24 PM GMT+5

Download Date

Jul 10, 2025, 9:25 PM GMT+5

File Name

A_Comparative_Study__on_IoT__Device_Identification_and_Anomaly_Detection.pdf

File Size

335.4 KB

5 Pages

2,981 Words

17,473 Characters

30% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

53 Not Cited or Quoted 26%
Matches with neither in-text citation nor quotation marks

14 Missing Quotations 4%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

20%	Internet sources
22%	Publications
25%	Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **53** Not Cited or Quoted 26%
  Matches with neither in-text citation nor quotation marks
- **14** Missing Quotations 4%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

20%	Internet sources
22%	Publications
25%	Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	link.springer.com	3%
2	Internet	ouci.dntb.gov.ua	2%
3	Internet	www.mdpi.com	1%
4	Internet	jurnal.itscience.org	1%
5	Submitted works	Polytechnic Institute Australia on 2025-05-23	1%
6	Submitted works	De Montfort University on 2025-05-30	1%
7	Submitted works	National College of Ireland on 2025-02-20	1%
8	Internet	napier-repository.worktribe.com	1%
9	Internet	journals.plos.org	<1%
10	Internet	dokumen.pub	<1%

11	Submitted works	University of Portsmouth on 2024-09-11	<1%
12	Submitted works	Coventry University on 2025-06-20	<1%
13	Submitted works	Asia Pacific Instutute of Information Technology on 2025-06-16	<1%
14	Publication	Mohammed Tawfik. "Optimized intrusion detection in IoT and fog computing usi...	<1%
15	Submitted works	AUT University on 2025-06-15	<1%
16	Publication	Diogo Gaspar, Paulo Silva, Catarina Silva. "Explainable AI for Intrusion Detection ...	<1%
17	Submitted works	Kennesaw State University on 2024-11-19	<1%
18	Internet	fastercapital.com	<1%
19	Publication	Poonam Nandal, Mamta Dahiya, Meeta Singh, Arvind Dagur, Brijesh Kumar. "Pro...	<1%
20	Internet	hiof.brage.unit.no	<1%
21	Internet	peerj.com	<1%
22	Submitted works	Whitecliffe College of Art & Design on 2024-12-08	<1%
23	Submitted works	Middlesex University on 2022-12-06	<1%
24	Submitted works	Georgia State University on 2021-12-09	<1%

25	Submitted works	Southern Arkansas University (Blackboard LTI 1.3) on 2024-12-03	<1%
26	Internet	mesopotamian.press	<1%
27	Internet	res.mdpi.com	<1%
28	Submitted works	Victoria University on 2023-07-01	<1%
29	Internet	www.nature.com	<1%
30	Internet	web.cs.dal.ca	<1%
31	Submitted works	Kaplan College on 2024-08-12	<1%
32	Publication	Tasnimul Hasan, Samia Tasnim. "Real-time explainable IoT security with machine ...	<1%
33	Submitted works	University of Glasgow on 2023-03-24	<1%
34	Submitted works	University of Gloucestershire on 2024-04-18	<1%
35	Submitted works	VIT University on 2025-04-23	<1%
36	Internet	shura.shu.ac.uk	<1%
37	Publication	"ICT Systems Security and Privacy Protection", Springer Science and Business Me...	<1%
38	Submitted works	Asia Pacific Instutute of Information Technology on 2025-05-11	<1%

39	Publication	Khalied M. Albarrak. "Securing the Future of Web-Enabled IoT: A Critical Analysis ...	<1%
40	Submitted works	Middlesex University on 2025-04-11	<1%
41	Submitted works	University of Hertfordshire on 2023-12-04	<1%
42	Submitted works	University of Stirling on 2024-09-13	<1%
43	Publication	Yuehua Huo, Junhan Chen, Yunhao Guo, Wei Liang, Jiyan Sun. "LG-BiTCN: A Light...	<1%
44	Internet	www.frontiersin.org	<1%
45	Submitted works	Buckinghamshire Chilterns University College on 2025-06-02	<1%
46	Submitted works	University of Hertfordshire on 2024-09-01	<1%
47	Submitted works	University of Hertfordshire on 2023-12-04	<1%

A Comparative Study on IoT Device Identification and Anomaly Detection

Nazihah Islam Nawreen
Dept. of CSE
BRAC University
Dhaka, Bangladesh
nazihah.islam.nawreen@g.bracu.ac.bd

Azwad Aziz
Dept. of CSE
BRAC University
Dhaka, Bangladesh
azwad.aziz@g.bracu.ac.bd

***Abstract*—The immense growth of the Internet of Things (IoT) has introduced extreme security challenges, particularly in device identification and anomaly detection within heterogeneous and dynamic environments. In this study we present a comparative analysis of multiple machine learning algorithms—including K-Nearest Neighbors, Naive Bayes, CatBoost, XGBoost, and AdaBoost—applied to a subset of the IoT DIAD 2024 dataset containing benign, DNS spoofing, and ARP spoofing traffic from approximately 58 distinct devices. Rigorous pre-processing steps, including feature selection, label encoding, and dimensionality reduction via Principal Component Analysis (PCA), were employed to enhance models' effectiveness and performance. To address the critical need for model transparency in security applications, Local Interpretable Model-Agnostic Explanations (LIME) was used for interpretability. Experimental results demonstrate that the traditional method Random Forest outperformed, CatBoost and XGBoost in both device identification and anomaly detection tasks, while LIME provided valuable insights into model decision processes. These findings highlight the potential of advanced machine learning and explainable AI techniques for assisting IoT security and move towards future research directions in this domain.**

***Index Terms*—IoT, Machine Learning, XAI, Anomaly Detection, Device Identification, XAI, LIME**

I. Introduction

The rapid expansion of the Internet of Things (IoT) has led to an unprecedented growth of interconnected devices across diverse domains, including smart homes, healthcare, and industrial automation [12]. While this connectivity brings significant benefits, it also introduces complex security challenges, specially in device identification and anomaly detection [13]. Accurately distinguishing between legitimate devices and identifying malicious activities is important for the safety of IoT ecosystems against evolving cyber-threats.

Device identification in IoT networks is complicated by the heterogeneity and large volume of devices, each with distinct communication patterns and hardware characteristics. Concurrently, the detection of anomalies—such as spoofing attacks—demands robust analytical techniques capable of distinguishing between subtle deviations from normal behavior. Among the most prevalent threats are DNS Spoofing and ARP Spoofing, both of which can compromise network integrity and data confidentiality.

To address these challenges, this study conducts a comparative analysis of various machine learning models for IoT device identification and anomaly detection. Leveraging a subset of the IoT Diad 2024 dataset, we selected traffic data from approximately 50 distinct devices and includes labeled instances of Benign, DNS Spoofing, and ARP Spoofing activities, we systematically evaluate the performance of several algorithms: K-Nearest Neighbors (KNN), Naive Bayes, CatBoost, XGBoost, and AdaBoost. To enhance computational efficiency and mitigate the curse of dimensionality, Principal Component Analysis (PCA) is applied to reduce the feature space to five principal components.

Beyond predictive performance, interpretability remains a critical issue for deploying machine learning models in security-sensitive environments. As a result, we incorporate Explainable Artificial Intelligence (XAI) techniques, specifically Local Interpretable Model-agnostic Explanations (LIME), to better interpret the model decisions. Overall the contributions of this paper can be summarized as:

- Utilize a subset of the IoT DIAD 2024 dataset for device identification and anomaly detection
- Compare state of the art machine learning models and evaluate their performance in both of these tasks
- Use LIME to add explainability of the decision making process of the model to understand which features are being focused for making a decision.

II. Literature Review

We carried out a thorough analysis of the previous works in the domain to highlight the main research gap and address them accordingly in our research.

Recently, Hussein et al. [1] proposed an accuracy boosting model (ABM) for IoT device identification using an ensemble of Random Forest and XGBoost algorithms. Their approach achieved 91% accuracy, 93% precision, and 93% recall on an IoT device identification dataset. The study demonstrated that ensemble methods combining multiple base learners can significantly improve device classification performance compared to individual algorithms. However, the research was limited to specific device types and required manual feature engineering. On the other hand, Vajrobol et al. [2] focused specifically on DNS and ARP spoofing detection in IoT environments using a comprehensive machine learning framework. Their study used

Paper	Focus Area	Best Model	Performance	Key Limitation
Hussein et al. (2024)	Device Identification	Random Forest	91% accuracy	Limited device types
Vajrobol et al. (2024)	Spoofing Detection	Random Forest	95.1% accuracy	Limited attack diversity
Usmani et al. (2022)	ARP Spoofing	Decision Tree	100% accuracy	Small dataset
Kalutharage et al. (2024)	XAI Anomaly Detection	Deep Autoencoder	84-100% accuracy	Requires labeled data
Tawfik (2024)	Ensemble IDS	CatBoost Ensemble	99% accuracy	High complexity
Saha et al. (2024)	XAI Framework	ML with XAI	96.2% F1-score	Scalability concerns

TABLE I: Summary of Recent Studies on Detection Techniques

46 features to simultaneously detect both DNS and ARP spoofing attacks, achieving 95.1% accuracy with Random Forest as the best algorithm. However, Usmani et al. [3] investigated ARP spoofing prediction using Long Short-Term Memory (LSTM) networks and decision trees. Their approach achieved 100% accuracy with decision trees and 99% accuracy with LSTM networks, demonstrating the effectiveness of both traditional and deep learning approaches for ARP attack detection. Furthermore, Kalutharage et al. [4] used deep autoencoder models with explainable AI for IoT network attack certainty verification. Their approach achieved 84% accuracy for benign traffic and 100% for attack detection while providing SHAP-based explanations for model decisions. Their research highlighted the importance of XAI in security-critical IoT applications. In another research Tawfik [5] proposed an optimized IDS integrating stacked autoencoders, CatBoost, and transformer-CNN-LSTM ensembles. The approach achieved over 99% accuracy on NSL-KDD, UNSW-NB15, and AWID datasets by combining unsupervised feature extraction with supervised learning. The research demonstrated the utility of hybrid architectures in handling the resource constraints of IoT environments. Similarly, Saha et al [6] presented an adaptive end-to-end IoT security framework integrating machine learning with explainable AI techniques including SHAP and LIME. Their framework achieved a 96.2% F1-score while providing interpretable explanations for security decisions. On the other hand, Douiba et al [7] presented an improved IDS using CatBoost and decision trees for IoT security. Their CatBoost-based approach demonstrated superior performance in accuracy, recall, and precision when evaluated on NSL-KDD, IoT-23, and Bot-IoT datasets. The study highlighted the effectiveness of gradient boosting algorithms in handling the complex and heterogeneous nature of IoT network traffic. In another research, Siganos et al [8] introduced an AI-powered IDSDS with XAI functions for IoT networks. Their approach utilized both LIME and SHAP techniques to provide model interpretability while maintaining high detection accuracy. The study emphasized the trade-off between model performance and interpretability in IoT security applications. Moreover, Tseng et al. [9] applied seven deep learning models including Transformer for IoT network intrusion detection using the CIC-IoT-2023 dataset. The Transformer model achieved 99.40% accuracy in multi-class classification, outperforming previous studies by 3.8%, 0.65%, and 0.29% respectively. In a different research, Meidan et al. [10] applied machine learning algorithms on network traffic data for IoT device identification using a multi-stage meta classifier approach. Thy collected data from nine distinct IoT devices, PCs, and smartphones, achieving 99.281% overall IoT classification accuracy. Table I provides a summary of the literature that has been reviewed.

A. Research Gap

Based on the comprehensive literature review, several important research gaps are highlighted that our proposed study aims to address:

- Most existing studies focus on either device identification or anomaly detection separately, with few works providing integrated solutions for both tasks simultaneously.
- Although PCA has been used in IoT contexts, there is a lacking on research of its specific impact on IoT security model performance, particularly when combined with explainable AI techniques.
- Few studies provide comprehensive comparisons of both traditional machine learning algorithms (KNN, Naive Bayes) and modern ensemble methods (CatBoost, XGBoost, AdaBoost).

III. Dataset

The CIC IoT-DIAD 2024 [11] dataset is an IoT attack dataset specifically designed for dual applications in both IoT device identification and anomaly detection. It is developed by the Canadian Institute for Cybersecurity at the University of New Brunswick. The dataset encompasses 33 distinct attack scenarios systematically categorized into 7 major attack classes and 105 IoT devices.

A. Pre-processing

We created a subset by selecting the classes: Benign , DNS spoofing and ARP spoofing. Unimportant columns like destination_mac was dropped from the dataset. Furthermore, some of the device names were unavilable and only the MAC address was provided which we labeled as ”Unknown”. Additionally, any sort of duplicates were removed and missing values were imputed using median. Moreover, label encoding was applied on the categorical features. Lastly, PCA was applied for dimensionality reduction which only resulted into 5 features. The dataset was splitted into train and test in the ratio of 0.8:0.2 and the summary of the dataset is listed in Table II

Class	Total Samples	Train (80%)	Test (20%)
ARP Spoofing	158,788	127,031	31,757
DNS Spoofing	143,031	114425	28606
Benign	130,736	104,589	26,147
Total	**883,525**	**706,819**	**176,706**

TABLE II: Distribution of Samples Across Classes

IV. Methodology

We begin with a subset of the IoT DIAD 2024 dataset which is focused on three primary classes: Benign, DNS Spoofing, and ARP Spoofing. The dataset includes network traffic records from approximately 58 distinct IoT devices, providing a realistic and diverse representation of both normal and malicious activities. The final dataset comprised 176,706 samples. The dataset was preprocessed with imputation of null values, encoding categorical features, removing duplicated, standard scaling and PCA. After applying the PCA number of features were reduced to 23 from 155. Train-test split ratio was selected to be 80% : 20%. Using the preprocessed dataset, a number of machine learning models were trained separately for anomaly classification and device classification. Then these trained models were used to evaluate the performance on the test set in terms various metrics such as: accuracy, recall, precision, f1-score and confusion metric. All these details were used to analyze the performance achieved by the different models. To gain further insights we also integrated explainable AI , (LIME) to analyze that which features are getting more focus when a particular decision is made by the model. This enhances the reliability of the prediction process. The overall workflow of our research is shown in Figure 1

V. Result Analysis

For the anomaly detection we performed several metrics to evaluate the best performing model, that is, Random Forest model. The accuracy for anomaly detection is 0.99 with F1 score, precision and recall all being 0.99 as well. The accuracy for device identification is 0.93, with 0.83 precision and 0.81 recall and f1 score. Figure 2 shows the bar graph of the different evaluation matrices for the random forest model for anomaly detection. Figure 3 shows the confusion matrix of Random Forest model on attack detection. In the confusion matrix, the rows are the actual labels and the columns are the predicted ones. The diagonal cells are the correct prediction, which shows that most samples were correctly predicted as their true class. The stronger the diagonal, the better the performance of the model.

Furthermore, Table III shows the accuracies for both device and anomaly detection by the models that we have implemented. Among all the models, Random forest shows the highest accuracy and knn shows the second highest. This could be because Random Forest is an ensemble method that combines multiple decision trees each trained on a random subset of the data and features.This helps reduce the overfitting problem, that is when the model learns the training data too well and cannot generalise well on the test data. The averaging of predictions across trees leads to more robust and accurate

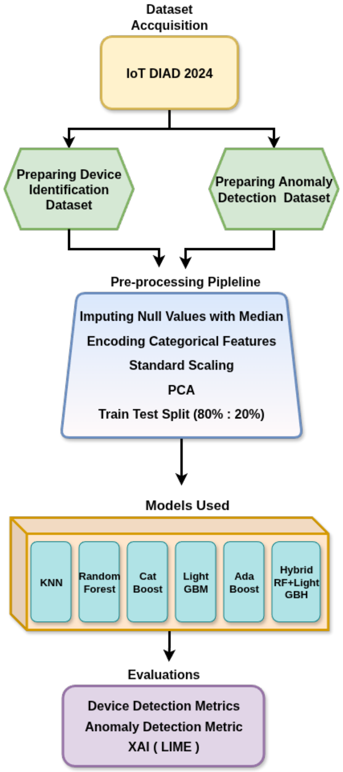

Fig. 1: Overall Workflow

outcomes, especially on complex datasets. The dataset also has significant class imbalance for the device detection, which is handled using class_weight = ’balanced’ while initialising the random forest model.

On the other hand, AdaBoost focuses on misclassified instances by increasing their weights, which can lead to overfitting on noisy or outlier-heavy data. Unlike Random Forest’s parallel tree construction, AdaBoost builds trees sequentially, which can be slower and less effective without extensive tuning, especially on large datasets. LightGBM’s leaf-wise tree growth strategy, while efficient, can overfit, especially on a dataset with complex feature interactions. KNN having the second best performance deviates a little while predicting devices which can be due to the curse of dimensionality, where distance metrics become less meaningful. Lastly, CatBoost excels with categorical data, but the dataset contains numerical features and the labels have been label encoded as well, hence Catboost shows lower performace.

Model	Device Accuracy	Anomaly Accuracy
Random Forest	0.93	0.99
AdaBoost	0.47	0.88
LightGBM	0.39	0.98
KNN	0.91	0.99
CatBoost	0.47	0.97

TABLE III: Performance Achieved by different Models

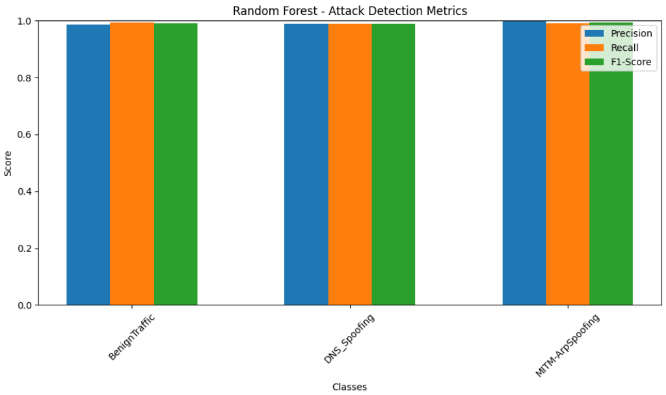

Fig. 2: Precision, Recall and F1-score

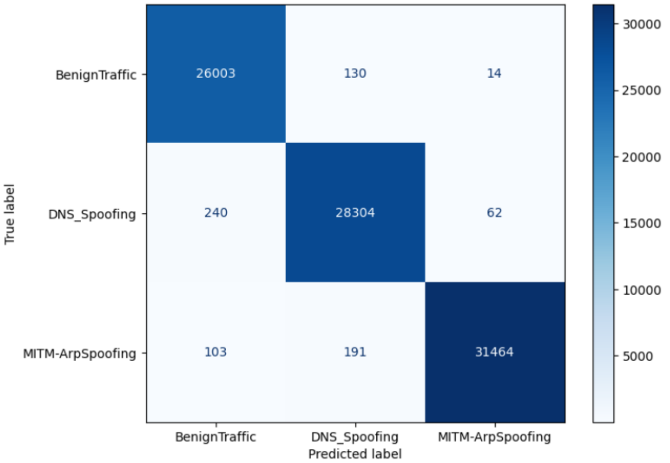

Fig. 3: Confusion Matrix of Random Forest on Anomaly Detection

VI. XAI

In addition to evaluating the model's performance using several performance metrics, it also crucial to learn why a model behaves the way it behaves and which features are utilizing it. Hence, we have implemented explainable AI (XAI) using LIME (Local Interpretable Model-Agnostic Explanations). Figure 4 shows the LIME output of Random Forest model. Each feature is represented as a Principal Component (PC), indicating its threshold and direction of influence. Red bar indicates a decrease and green bar indicates an increase in the likelihood. For example, PC2 greater than -0.38 has a strong positive impact on classifying an instance as DNS_Spoofing, whereas PC1 greater than 7.34 contributes negatively. PC1 refers to the different channel means features which had a strong impact to classify that the sample was not DNS Spoofing. Furthermore, 19 and 23 are flow-based and timing related features which helped to prove that the sample was not DNS Spoofing. Even though, PC2 had a strong positive impact but the overall result was negative and hence it was not a DNS Spoofing sample as predicted by the model.

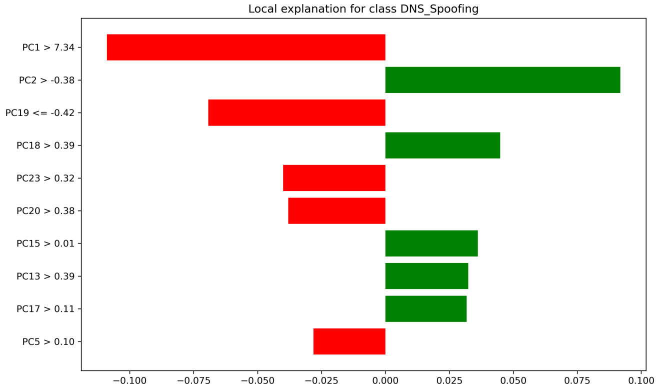

Fig. 4: LIME Explanation

VII. Conclusion and Future Work

In this study we systematically evaluated the effectiveness of various machine learning models for IoT device identification and anomaly detection using the IoT DIAD 2024 dataset. The results show that the traditional Random Forest outperforms the boosting techniques such as CatBoost and XGBoost consistently in both accuracy and robustness, especially after dimensionality reduction with PCA. The integration of LIME for model interpretability further enhances the practical applicability of these solutions by providing transparent and actionable explanations for the decisions.

Despite these promising outcomes, several areas need further exploration. Future work will can focus on expanding the range of attack types and device classes to assess model scalability and generalizability. Additionally, integrating deep learning architectures and could further improve detection capabilities and operational efficiency. Finally, exploring advanced explainability techniques and user-centric evaluation will be crucial for building trust and adoption of AI-driven security solutions in IoT environments.

References

[1] Hussain, S., Aslam, W., Mehmood, A., Choi, G. S., & Ashraf, I. (2024). A machine learning based framework for IoT devices identification using web traffic. *PeerJ Computer Science*, **10**, e1834. https://doi.org/10.7717/peerj-cs.1834

[2] Vajrobol, V., Saxena, G. J., Pundir, A., Singh, S., Gupta, B. B., Gaurav, A., & Rahaman, M. (2025). Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms. *Journal of High Speed Networks*, **31**(1), 61–70. SAGE Publications, London, UK.

[3] Usmani, M., Anwar, M., Farooq, K., Ahmed, G., & Siddiqui, S. (2022). Predicting ARP spoofing with Machine Learning. In *Proceedings of the 2022 International Conference on Emerging Trends in Smart Technologies (ICETST)* (pp. 1–6). Retrieved from https://api.semanticscholar.org/CorpusID:253047076

[4] Kalutharage, C. S., Liu, X., & Chrysoulas, C. (2022). Explainable AI and deep autoencoders based security framework for IoT network attack certainty. In *International Workshop on Attacks and Defenses for Internet-of-Things* (pp. 41–50). Springer.

[5] Tawfik, M. (2024). Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection. *PLOS ONE*, **19**(8), e0304082. https://doi.org/10.1371/journal.pone.0304082

[6] Baral, S., Saha, S., & Haque, A. (2024). An adaptive end-to-end IoT security framework using explainable AI and LLMs. In *Proceedings of the 2024 IEEE 10th World Forum on Internet of Things (WF-IoT)* (pp. 469–474). IEEE.

[7] Douiba, M., Benkirane, S., Guezzaz, A., & Azrour, M. (2022). An improved anomaly detection model for IoT security using decision tree and gradient boosting. *The Journal of Supercomputing*, **79**, 3392–3411. Retrieved from https://api.semanticscholar.org/CorpusID:252075512

[8] Siganos, M., Radoglou-Grammatikis, P., Kotsiuba, I., Markakis, E., Moscholios, I., Goudos, S., & Sarigiannidis, P. (2023). Explainable AI-based intrusion detection in the Internet of Things. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23)* (Article 53, 10 pages). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3600160.3605162

[9] Tseng, S.-M., Wang, Y.-Q., & Wang, Y.-C. (2024). Multi-class intrusion detection based on transformer for IoT networks using CIC-IoT-2023 dataset. *Future Internet*, **16**(8), 284. MDPI.

[10] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J. D., Ochoa, M., Tippenhauer, N. O., & Elovici, Y. (2017). ProfilIoT: A machine learning approach for IoT device identification based on network traffic analysis. In *Proceedings of the Symposium on Applied Computing* (pp. 506–509).

[11] Rabbani, M., Gui, J., Nejati, F., Zhou, Z., Kaniyamattam, A., Mirani, M., Piya, G., Opushnyev, I., Lu, R., & Ghorbani, A. A. (2024). Device identification and anomaly detection in IoT environments. *IEEE Internet of Things Journal*, December 2024.

[12] Statista. (n.d.). *Internet of Things – Worldwide*. Statista Market Forecast. Retrieved July 9, 2025, from https://www.statista.com/outlook/tmo/internet-of-things/worldwide

[13] Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions techniques for Internet of Things (IoT): From vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, **7**, 1397480. Frontiers Media SA.