DTXG-RF-based Intrusion Detection System for Artificial IoT Cyber Attacks

Shayma Wail Nourildean
University of Technology- Iraq
shayma.w.nourildean@uotechnology.edu.iq (corresponding author)

Wafa Mefteh
National Engineering School of Tunis, Tunisia
wafa.mefteh@enit.utm.tn

Ali Mouhsin Frihida
National Engineering School of Tunis, Tunisia
ali.frihida@enit.utm.tn

Received: 31 October 2024 | Revised: 22 November 2024 | Accepted: 27 November 2024

 DOI: https://doi.org/10.48084/etasr.9464

ABSTRACT

The swift advancement of networking technology and the rising incidence of cyber-attacks have made effective cybersecurity a critical priority. The primary concern with IoT networks is their susceptibility to vulnerabilities. IoT security necessitates the substantial involvement of artificial intelligence as a security technology to mitigate these challenges. Cyberattacks are evolving in sophistication, consequently posing greater obstacles in the precise detection of intrusions. An Intrusion Detection System (IDS) is a device or software application that monitors the activities of network systems for malicious actions or policy breaches and produces reports. The primary objective of an IDS is to efficiently identify attacks. Moreover, it is imperative to identify attacks at an early stage to mitigate their effects. Machine learning models have become increasingly popular in IDSs due to their capacity to process substantial data volumes and identify patterns in real time. Machine learning involves building an algorithm to identify consistent patterns within a dataset. This study aimed to build an IDS using an ensemble machine learning (DTXG-RF) model and compare it with DT, XGBoost, KNN, RF, NB, and CatBoost on the CIC-IoT-2023 and a Ransomware dataset. The results showed that the proposed DTXG-RF outperformed other machine learning models with accuracy reaching 95.06%.

Keywords-machine learning; dataset; IDS; IoT; AI; reliability

I. INTRODUCTION

The IoT is essentially a human-machine connection where humans give commands and devices carry them out. To perform this role, a huge amount of data must be generated and transmitted. As the current world's requirements cannot be satisfied by conventional data processing techniques, Artificial Intelligence (AI) is used [1, 2]. The integration of AI and IoT yields the concept of Artificial Intelligence of Things (AIoT). The IoT functions as a digital nervous system, while AI serves as its brain [3]. Cyberattacks are evolving in sophistication, consequently posing greater obstacles in the precise detection of intrusions. The data integrity, confidentiality, and availability are affected by the failure to prevent attacks [4, 5]. Intrusion Detection Systems (IDSs) are employed in cybersecurity platform that detect and identify intrusion attackers [6]. Early attacks detection is necessary to minimize their impact, therefore, the primary goal of an IDS is to detect attacks effectively [7]. Machine learning models have become increasingly important in IDS, as they can deploy significant amounts of data, recognize real time patterns and exhibit unique characteristics, such as network configuration, types of attack, and user behavior [8]. This study aimed to develop an IDS using an ensemble model (DTXG-RF) and compare its accuracy and reliability performance with different machine learning methods, including XGBoost, Naïve Bayes (NB), k-Nearest Neighbor (KNN), CatBoost and Decision Tree (DT).

II. LITERATURE REVIEW

To improve the performance of IDSs, the researchers used neural networks, deep learning, and machine learning. IDS development included implementation methods, data types, authentication methods and some common methods. In [9], IoT IDSs specific classification is presented, as well as different approaches and IoT attacks targeting the IoT network. In [10] a comprehensive survey of current IDSs for IoT contexts is introduced.

III. IOT BASED AI

The next stage is to combine AI and the IoT to create what is referred to as the "Intelligence of Things". IoT devices that incorporate AI can evaluate data, make decisions, and take action based on them without the need for human interaction. Companies may benefit from the advantages of the full integration of the IoT with AI, or AIoT [3]. AI, machine learning, and deep learning are three prevalent terms currently used interchangeably to denote intelligent systems or software [17-19].

A. Cyber Attacks

A cyber security guideline is essential to protect information technology and computer systems, encouraging various organizations and corporations to defend their systems and data against cyber attacks [20, 21]. Although there are different types of cyber attacks, the most common types in IoT are:

- Physical Attacks
- Encryption Attacks
- DoS (Denial of Service)
- Firmware Hijacking
- Botnets
- Man-in-the-Middle
- Ransomware
- Eavesdropping
- Privilege Escalation
- Brute Force Password Attack

B. Intrusion Detection System (IDS)

An IDS plays a significant role to monitor network traffic and identify potential security breaches [6]. An IDS detects network intrusion attempts by monitoring network activities [22]. Data mining, machine learning, and deep learning are different techniques used in IDSs [23].

IV. RESEARCH METHOD

This study aimed to build an IDS for IoT systems to protect against cyber attacks defined in the CIC-IoT2023 dataset, including Ransomware, DoS, DDoS, Mirai, Benign, MiTM, Recon-OSScan, DNS_Spoofing, Recon, Brute-Force, utilizing the proposed DTXG-RF ensemble model. This model was compared to several machine learning models, including DT [23], XGBoost [24], Logistic Regression (LR) [25], kNN [26], Naïve Bayes (NB) [27], and CatBoost [28].

The selection of machine learning algorithms is crucial in the design of IDSs [6]. The implementation of a machine learning model consists of the following primary steps [6]:

- Data Acquisition: The preliminary phase comprises the collection of training data, which is defined in the datasets used.
- Data Preprocessing: This phase encompasses cleaning, feature selection, normalization, data splitting, and altering the training data to make it appropriate for processing by the machine learning model [29].
- Model Selection and Training: Identify the appropriate machine learning model and train it on the training data to discern inherent patterns and correlations.
- Model Evaluation: After training, the model undergoes assessment utilizing distinct test data that was excluded from the training process. This enables the assessment of the model's efficacy in generalizing patterns to novel data. In this study, the evaluation of the machine learning models was performed in terms of Precision, Accuracy, Recall, and F1-score.

The steps in this study were as follows:

1. The preprocessing pipeline involved the following steps to ensure consistency. Replaced invalid values (np.inf, -np.inf) with NaN. Removed incomplete rows to avoid errors. Finally, verification ensured the structure and completeness of the data.
2. Split the dataset into training and testing subsets with data allocation of 20:80 resulting in 20% of the data to the test set, leaving 80% for training.
3. VotingClassifier: Combine multiple models to make a single prediction based on voting.
4. DecisionTreeClassifier (DT): A tree-based model that splits data based on feature values.
5. RandomForestClassifier (RF): An ensemble model that builds multiple DTs and averages their results.
6. XGBClassifier (XGBoost): It is a gradient boosting algorithm, effective for structured data.
7. The VotingClassifier combines the predictions from these multiple models in the model's list
8. Set up a checkpoint to save the best model (based on validation accuracy) during training.
9. Load the best-saved model for evaluation.
10. Predicts the class probabilities for the test set.
11. Calculate metrics to evaluate the model.
12. Compare the results of the ensemble model against single XGBoost, kNN, DT, LR, and NB.

Figure 1 summarizes the steps of this study.

A. Dataset

This study used the CIC IoT 2023 dataset [29], which is particularly helpful for improving cyberattack detection algorithms for IoT devices. This dataset comprises multiple devices, a variety of usage profiles, and both IP and non-IP device data, and provides valuable insights for developing effective detection strategies. The considered attacks are: DoS, DDoS, brute force, spoofing, Web-based, Mirai, and Recon. The proposed cluster model also included ransomware attacks,

using the dataset in [30]. The IoT architecture implemented for the CICIoT2023 consists of 105 IoT, Z-Wave, and Zigbee devices, which were directly affected with the attacks. The proposed DTXG-RF ensemble model outperformed the others with Accuracy and Recall reaching 95.0647%, 95.0265% Precision, and Fl-Score of 95.0297%. The ROC curve is a plot of the True Positive Rate (TPR) versus the False Positive Rate (FPR) at various threshold settings. The Area Under the ROC Curve (AUC) is used to measure a model's ability to distinguish between positive and negative classes. The ROC curve and AUC of DTXG-RF were determined and compared with those of the other single machine-learning models, as shown in Figure 2. The proposed DTXG-RF ensemble model had the greatest AUC of 0.96103, indicating better performance.

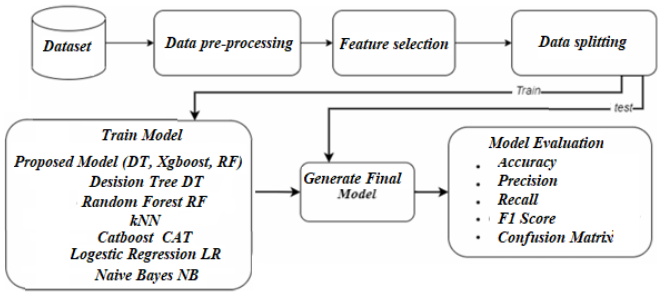

Fig. 1. The overall framework of this study.

B. Evaluation Metrics

Accuracy is the primary criterion for evaluating algorithm performance in classification tasks [31]. It measures the proportion of correct estimates, expressed as:

$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions}$$

Precision measures the proportion of accurately predicted positive outcomes relative to the total predicted positives [31]. It merely indicates the quantity of relevant selected data elements [32].

$$Precision = \frac{TP}{TP+FP}$$

Recall calculates the proportion of accurately anticipated positive instances to the total instances within a designated class [32]. It indicates the number of pertinent data items picked [31].

$$Recall = \frac{TP}{TP+FN}$$

F1 score, also referred to as f-score or f-measure, incorporates both precision and recall to evaluate the performance of an algorithm [32]:

$$F1 - score = \frac{2\times Precision\times Recall}{Recall+Precision}$$

The proposed DTXG-RF ensemble model was trained and tested with different machine learning models for the two datasets, CIC-IoT-2023 [29] and Ransomware [30], using the following specifications: Core i7 CPU, RAM 16.0 GB, Windows 11, Python 3.12.4, and Jupyter 1.0.0

V. RESULTS AND DISCUSSION

Table I shows the evaluation metrics for the proposed DTXG-RF model, along with the respective metrics for the single machine learning models.

TABLE I. EVALUATION RESULTS

ML Model	Accuracy	Precision	Recall	FI-Score
Ensemble DTXG-RF	95.0647%	95.0265%	95.0647%	95.0297%
XGBoost	93.6878%	93.5681%	93.6878%	93.5758%
KNN	89.8039%	90.1108%	89.8039%	89.5440%
DT	94.8139%	94.8267%	94.8139%	94.8161%
LR	69.7545%	69.7647%	69.7545%	64.5945%
NB	57.5973%	66.9938%	57.5973%	55.0630%
CatBoost	93.0366%	93.0503%	93.0366%	92.8612%

The proposed DTXG-RF ensemble model outperformed the others with Accuracy and Recall reaching 95.0647%, Precision of 95.0265%, and Fl-Score of 95.0297%.

The ROC curve is a plot of the True Positive Rate (TPR) versus the False Positive Rate (FPR) at various threshold settings. The Area Under the ROC Curve (AUC) is used to measure a model's ability to distinguish between positive and negative classes. The ROC curve and AUC of DTXG-RF were determined and compared with those of the other single machine-learning models, as shown in Figure 2. The proposed DTXG-RF ensemble model had the greatest AUC of 0.96103, indicating better performance.

VI. CONCLUSION

The integration of IoT and AI can be a powerful solution that can solve many IoT issues related to big data generated by IoT devices IoT devices incorporating AI can measure, make decisions, and act on data without the need for human interaction. IDS are essential for monitoring network traffic to identify potential security breaches, enable attacks to be detected at the earliest stages of attack, and provide opportunities for mitigation Furthermore, IDSs had facilitated the detection of IoT attacks, such as Denial of Service (DoS), Ransomware. Machine learning can be used in IDS to detect known and new attacks, if the model is sufficiently trained for predictive or automated tasks. Deep learning and machine learning models are important detection techniques. In this study, the proposed DTXG-RF ensemble model was used to develop an IDS against the most common types of IoT attacks and the CIC-IoT 2023 and Ransomware dataset, which contains the most common types of attacks in IoT was considered. The proposed DTXG-RF ensemble model outperformed the single machine learning models, achieving improved accuracy of 95.06% in multiclass classification. Future work should involve the use of the proposed model in an ensemble with other deep-learning models utilizing a voting rule classifier.

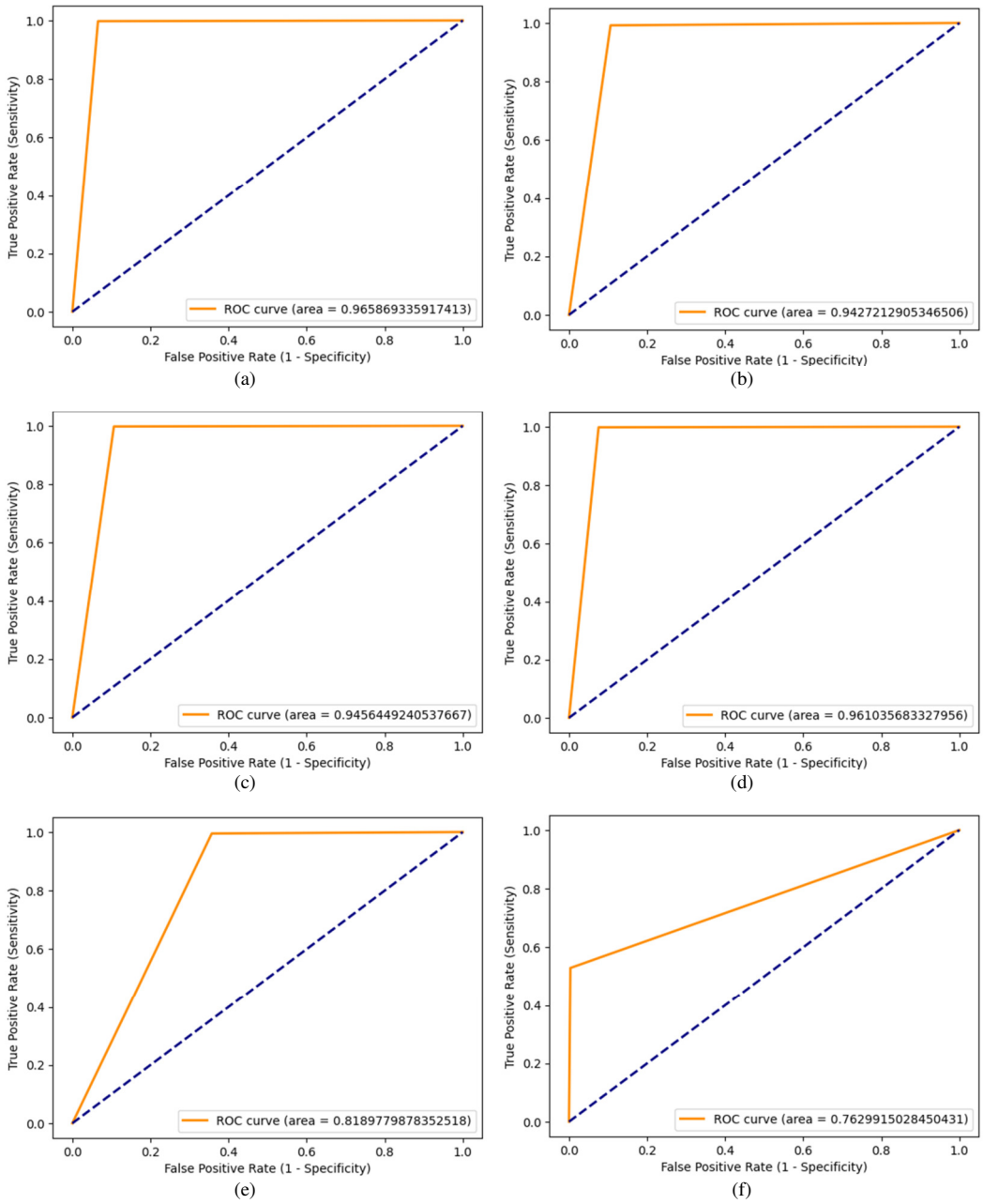

Fig. 2. ROC curves for all machine and ensemble learning models: (a) XGBoost, (b) KNN, (c) DT, (d) Ensemble DTXG-RF, (e) LR, (f) NB.

REFERENCES

[1] A. Karn, "Applications of Artificial Intelligence in IoT and Sensor Networks: A Survey," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 7, no. 3, pp. 2297–3000.

[2] N. A. S. Al-Jamali, I. R. K. Al-Saedi, A. R. Zarzoor, and H. Li, "A New Imputation Technique Based a Multi-Spike Neural Network to Handle Missing Data in the Internet of Things Network (IoT)," *IEEE Access*, vol. 11, pp. 112841–112850, 2023, https://doi.org/10.1109/ACCESS.2023.3323435.

[3] H. Nozari, A. Szmelter-Jarosz, and J. Ghahremani-Nahr, "Analysis of the Challenges of Artificial Intelligence of Things (AIoT) for the Smart Supply Chain (Case Study: FMCG Industries)," *Sensors*, vol. 22, no. 8, Jan. 2022, Art. no. 2931, https://doi.org/10.3390/s22082931.

[4] J. Dumoulin *et al.*, "UNICITY: A depth maps database for people detection in security airlocks," in *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Auckland, New Zealand, Nov. 2018, pp. 1–6, https://doi.org/10.1109/AVSS.2018.8639152.

[5] S. W. Nourildean and Y. A. Mohammed, "IoT based Wireless Sensor Network Improvement Against Jammers Using Ad-Hoc Routing Protocols," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 07, pp. 133–147, Apr. 2023, https://doi.org/10.3991/ijim.v17i07.38587.

[6] P. Dini, A. Elhanashi, A. Begni, S. Saponara, Q. Zheng, and K. Gasmi, "Overview on Intrusion Detection Systems Design Exploiting Machine Learning for Networking Cybersecurity," *Applied Sciences*, vol. 13, no. 13, Jan. 2023, Art. no. 7507, https://doi.org/10.3390/app13137507.

[7] J. Jabez and B. Muthukumar, "Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach," *Procedia Computer Science*, vol. 48, pp. 338–346, Jan. 2015, https://doi.org/10.1016/j.procs.2015.04.191.

[8] S. H. Abd, I. A. Hashim, and A. S. A. Jalal, "Automatic deception detection system based on hybrid feature extraction techniques," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 1, Apr. 2022, https://doi.org/10.11591/ijeecs.v26.i1.pp381-393.

[9] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges," *Cybersecurity*, vol. 4, no. 1, Mar. 2021, Art. no. 18, https://doi.org/10.1186/s42400-021-00077-7.

[10] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A Comprehensive Analyses of Intrusion Detection System for IoT Environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975–990, 2020, https://doi.org/10.3745/JIPS.03.0144.

[11] B. Xu, L. Sun, X. Mao, R. Ding, and C. Liu, "IoT Intrusion Detection System Based on Machine Learning," *Electronics*, vol. 12, no. 20, Jan. 2023, Art. no. 4289, https://doi.org/10.3390/electronics12204289.

[12] R. Alsulami, B. Alqarni, R. Alshomrani, F. Mashat, and T. Gazdar, "IoT Protocol-Enabled IDS based on Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12373–12380, Dec. 2023, https://doi.org/10.48084/etasr.6421.

[13] M. Baich, T. Hamim, N. Sael, and Y. Chemlal, "Machine Learning for IoT based networks intrusion detection: a comparative study," *Procedia Computer Science*, vol. 215, pp. 742–751, Jan. 2022, https://doi.org/10.1016/j.procs.2022.12.076.

[14] P. Sanju, "Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural networks," *Journal of Engineering Research*, vol. 11, no. 4, pp. 356–361, Dec. 2023, https://doi.org/10.1016/j.jer.2023.100122.

[15] A. Kaushik and H. Al-Raweshidy, "A novel intrusion detection system for internet of things devices and data," *Wireless Networks*, vol. 30, no. 1, pp. 285–294, Jan. 2024, https://doi.org/10.1007/s11276-023-03435-0.

[16] X. Yang, G. Peng, D. Zhang, and Y. Lv, "An Enhanced Intrusion Detection System for IoT Networks Based on Deep Learning and Knowledge Graph," *Security and Communication Networks*, vol. 2022, no. 1, 2022, Art. no. 4748528, https://doi.org/10.1155/2022/4748528.

[17] A. S. Dawood, "Machine learning and artificial neural network for data mining classification and prediction of brain diseases," *International Journal of Reasoning-based Intelligent Systems*, vol. 15, no. 3/4, pp. 313–322, 2023, https://doi.org/10.1504/IJRIS.2023.136366.

[18] I. H. Sarker, "AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems," *SN Computer Science*, vol. 3, no. 2, Feb. 2022, Art. no. 158, https://doi.org/10.1007/s42979-022-01043-x.

[19] P. D. Babu, C. Pavani, and C. E. Naidu, "Cyber Security with IOT," in *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, Mar. 2019, pp. 109–113, https://doi.org/10.1109/ICONSTEM.2019.8918782.

[20] S. W. Nourildean, S. I. Jasim, M. T. Abdulhadi, and M. M. Jaber, "Point coordination mechanism based mobile ad hoc network investigation against jammers," *Eastern-European Journal of Enterprise Technologies*, vol. 5, no. 9(119), pp. 45–53, Oct. 2022, https://doi.org/10.15587/1729-4061.2022.265779.

[21] M. Aljanabi, M. A. Ismail, R. A. Hasan, and J. Sulaiman, "Intrusion Detection: A Review," *Mesopotamian Journal of Cyber Security*, Jan. 2021, https://doi.org/10.58496/MJCS/2021/001.

[22] C. T. Dhumal and D. S. V. Pingale, "Analysis of Intrusion Detection Systems: Techniques, Datasets and Research Opportunity." Social Science Research Network, Mar. 06, 2024, https://doi.org/10.2139/ssrn.4749820.

[23] G. Sarailidis, T. Wagener, and F. Pianosi, "Integrating scientific knowledge into machine learning using interactive decision trees," *Computers & Geosciences*, vol. 170, Jan. 2023, Art. no. 105248, https://doi.org/10.1016/j.cageo.2022.105248.

[24] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, CA, USA, Aug. 2016, pp. 785–794, https://doi.org/10.1145/2939672.2939785.

[25] S. Sperandei, "Understanding logistic regression analysis," *Biochemia Medica*, pp. 12–18, 2014, https://doi.org/10.11613/BM.2014.003.

[26] J. Sun, W. Du, and N. Shi, "A Survey of kNN Algorithm," *Information Engineering and Applied Computing*, vol. 1, no. 1, May 2018, https://doi.org/10.18063/ieac.v1i1.770.

[27] I. Wickramasinghe and H. Kalutarage, "Naive Bayes: applications, variations and vulnerabilities: a review of literature with code snippets for implementation," *Soft Computing*, vol. 25, no. 3, pp. 2277–2293, Feb. 2021, https://doi.org/10.1007/s00500-020-05297-6.

[28] L. Prokhorenkova, G. Gusev, A. Vorobev, A. V. Dorogush, and A. Gulin, "CatBoost: unbiased boosting with categorical features," in *Advances in Neural Information Processing Systems*, 2018, vol. 31.

[29] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, Jan. 2023, Art. no. 5941, https://doi.org/10.3390/s23135941.

[30] A. Bensalah, "Ransomware detection data set." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/amdj3dax/ransomware-detection-data-set.

[31] E. Elmahfoud, S. Elhajla, Y. Maleh, and S. Mounir, "Machine Learning Algorithms for Intrusion Detection in IoT Prediction and Performance Analysis," *Procedia Computer Science*, vol. 236, pp. 460–467, Jan. 2024, https://doi.org/10.1016/j.procs.2024.05.054.

[32] M. Vakili, M. Ghamsari, and M. Rezaei, "Performance Analysis and Comparison of Machine and Deep Learning Algorithms for IoT Data Classification." arXiv, Jan. 27, 2020, https://doi.org/10.48550/arXiv.2001.09636.