IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 5, March 2024

Performance Analysis of Tree-Based and Deep Learning Algorithms for Developing Distributed Secure Systems in IoT: A Comparative Study

Aziz Ullah Karimy[1*] and Dr. P ChandraSekhar Reddy[2]

[1,2] Department of Electronics and Communication Engineering,
University College of Engineering , Science & Technology, Hyderabad
Jawaharlal Nehru Technological University, Hyderabad, Telangana, India.
Corresponding author:*azizullah.karimy91@gmail.com, drpcsreddy@jntuh.ac.in

Abstract: *Notably, IoT device utilization has experienced a substantial wave recently, and ensuring these devices' privacy and security has become a critical concern. ML-based security approaches are promising for IoT network protection against security concerns. This study provides a proximate analysis of tree-based and deep-learning algorithms for securing IoT domains. Specifically, we evaluate Decision Tree, RandomForest, XGBoost, Catboost, Extreme Tree, Light GMB, Adaptive Boosting, CNN, LSTM, MLP, GRU, and Autoencoder on four publicly available datasets - IoT23, CICID2017, EdgeIIoT, BotnetIoT and Contiki OS and Cooja simulation were used to generate a dataset featuring various RPL attacks. To assess the performance of a model, we measure its accuracy, precision, recall, and F1-score metrics. Our discoveries indicate that tree-based algorithms outperform deep learning algorithms regarding training time, memory usage, and interpretability while gaining comparable or even better detection accurateness. Conversely, deep-learning algorithms exhibit higher detection rates for rare or previously unseen attacks; their proficiency in detecting complex patterns and relationships within a given dataset has demonstrated remarkable efficacy in data analysis and classification tasks. We conclude that both tree-based and deep learning algorithms have their strengths and weaknesses, and in the IoT environment, one should base the choice of the algorithm on requirements and constraints. Our research shows hybrid approaches combining algorithm strengths can establish secure, distributed IoT systems.*

Keywords: Internet of things; machine learning; distributed secure system; deep learning; hybrid approaches

REFERENCES

[1]. Aziz UllahKarimy1, ,Dr. P Chandrasekhar Reddy2. Securing the Internet of Things: A Study on Machine LearningBased Solutions for IoT Security and Privacy Challenges. ZKG International [Internet]. 2023;8(2). Available from: https://zkginternational.com/archive/volume8/Securing-the-Internet-of-Things-A-Study-on-Machine-Learning-Based-Solutions-for-IoT-Security-and-Privacy-Challenges.pdf

[2]. Lokesh Babu C VM. Why do tree-based models still outperform deep learning on tabular data? 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT). 2022;417–22.

[3]. C LB, M V. Review on Various Machine Learning Algorithms Implemented in IoT Security. In: 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT) [Internet]. Kannur, India: IEEE; 2022 [cited 2023 Nov 8]. p. 417–22. Available from: https://ieeexplore.ieee.org/document/9917738/

[4]. Jamalipour A, Murali S. A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey. IEEE Internet Things J. 2022 Jun 15;9(12):9444–66.

[5]. Tasnim A, Hossain N, Parvin N, Tabassum S, Rahman R, Iqbal Hossain M. Experimental Analysis of Classification for Different Internet of Things (IoT) Network Attacks Using Machine Learning and Deep learning. In:

DOI: 10.48175/IJARSCT-16656

2022 International Conference on Decision Aid Sciences and Applications (DASA) [Internet]. Chiangrai, Thailand: IEEE; 2022 [cited 2023 Nov 8]. p. 406–10. Available from: https://ieeexplore.ieee.org/document/9765108/

[6]. Bekkouche R, Omar M, Langar R, Hamdaoui B. Ultra-Lightweight and Secure Intrusion Detection System for Massive-IoT Networks. In: ICC 2022 - IEEE International Conference on Communications [Internet]. Seoul, Korea, Republic of: IEEE; 2022 [cited 2023 Nov 8]. p. 5719–24. Available from: https://ieeexplore.ieee.org/document/9838257/

[7]. Garcia S, Parmisano A, Erquiaga MJ. IoT-23: A labeled dataset with malicious and benign IoT network traffic [Internet]. Zenodo; 2020 [cited 2023 Nov 8]. Available from: https://zenodo.org/record/4743746

[8]. Kayode Saheed Y, Idris Abiodun A, Misra S, Kristiansen Holone M, Colomo-Palacios R. A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal. 2022 Dec;61(12):9395–409.

[9]. Choudhary S, Kesswani N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT. Procedia Computer Science. 2020;167:1561–73.

[10]. Moustafa N, Slay J. 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) [Internet]. Canberra, Australia: IEEE; 2015 [cited 2023 Nov 8]. p. 1–6. Available from: http://ieeexplore.ieee.org/document/7348942/

[11]. Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications [Internet]. Ottawa, ON, Canada: IEEE; 2009 [cited 2023 Nov 8]. p. 1–6. Available from: http://ieeexplore.ieee.org/document/5356528/

[12]. Thavamani S, Sinthuja U. LSTM based Deep Learning Technique to Forecast Internet of Things Attacks in MQTT Protocol. In: 2022 IEEE Fourth International Conference on Advances in Electronics, Computers and Communications (ICAECC) [Internet]. Bengaluru, India: IEEE; 2022 [cited 2023 Nov 8]. p. 1–4. Available from: https://ieeexplore.ieee.org/document/9716585/

[13]. Selvapandian D, Santhosh R. Deep learning approach for intrusion detection in IoT-multi cloud environment. Autom Softw Eng. 2021 Nov;28(2):19.

[14]. Mitchell, Tom M. Machine learning. Vol. 1. McGraw-hill New York; 1997.

[15]. Chen T, Guestrin C. XGBoost: A Scalable Tree Boosting System. 2016 [cited 2023 Nov 8]; Available from: https://arxiv.org/abs/1603.02754

[16]. Sharafaldin I, Habibi Lashkari A, Ghorbani AA. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization: In: Proceedings of the 4th International Conference on Information Systems Security and Privacy [Internet]. Funchal, Madeira, Portugal: SCITEPRESS - Science and Technology Publications; 2018 [cited 2023 Nov 8]. p. 108–16. Available from: http://www.scitepress.org/DigitalLibrary/Link.aspx?doi=10.5220/0006639801080116

[17]. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning. IEEE Access. 2022;10:40281–306.

[18]. Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, et al. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. IEEE Pervasive Comput. 2018 Jul;17(3):12–22.

DOI: 10.48175/IJARSCT-16656