Available *online* at : http://jnte.ft.unand.ac.id/

Jurnal Nasional Teknik Elektro

| ISSN (Print) 2302-2949 | ISSN (Online) 2407-7267 |

REFERENCES

[1] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset." 2018.

[2] K. Albulayhi, Q. Abu Al-Haija, S. A. Alsuhibany, A. A. Jillepalli, M. Ashrafuzzaman, and F. T. Sheldon, "IoT Intrusion Detection Using Machine Learning with a Novel High Performing Feature Selection Method," *Applied Sciences*, vol. 12, no. 10, 2022, doi: 10.3390/app12105015.

[3] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network forensic mechanism for Botnet Activities in the IoT based on Machine Learning Techniques," Jun. 2017.

[4] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in Internet of Things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, Nov. 2019, doi: 10.1016/J.FUTURE.2019.04.038.

[5] T. Saba, T. Sadad, A. Rehman, Z. Mehmood, and Q. Javaid, "Intrusion Detection System Through Advance Machine Learning for the Internet of Things Networks," *IT Prof*, vol. 23, no. 2, pp. 58–64, 2021, doi: 10.1109/MITP.2020.2992710.

[6] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks," *Electronics (Switzerland)*, vol. 8, no. 11, 2019, doi: 10.3390/electronics8111210.

[7] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," *IEEE Access*, vol. 8, pp. 209802–209834, 2020, doi: 10.1109/ACCESS.2020.3036728.

[8] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020, doi: https://doi.org/10.1016/j.future.2020.03.042.

[9] N. Koroniotis and N. Moustafa, "Enhancing network forensics with particle swarm and deep learning: The particle deep framework," *CoRR*, vol. abs/2005.00722, 2020, [Online]. Available: https://arxiv.org/abs/2005.00722

[10] A. R. Zarzoor, N. A. S. Al-Jamali, and D. A. Abdul Qader, "Intrusion detection method for internet of things based on the spiking neural network and decision tree method," *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 2278–2288, 2023, doi: 10.11591/ijece.v13i2.pp2278-2288.

[11] D. Rani, N. S. Gill, P. Gulia, and J. M. Chatterjee, "An Ensemble-Based Multiclass Classifier for Intrusion Detection Using Internet of Things," *Comput Intell Neurosci*, vol. 2022, 2022, doi: 10.1155/2022/1668676.

[12] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A New Ensemble-Based Intrusion Detection System for Internet of Things," *Arab J Sci Eng*, vol. 47, no. 2, pp. 1805–1819, 2022, doi: 10.1007/s13369-021-06086-5.

[13] S. Alshathri, A. El-Sayed, W. El-Shafai, and E. El-Din Hemdan, "An Efficient Intrusion Detection Framework for Industrial Internet of Things Security," *Computer Systems Science and Engineering*, vol. 46, no. 1, pp. 819–834, 2023, doi: 10.32604/csse.2023.034095.

[14] A. Aljuhani, "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236–42264, 2021, doi: 10.1109/ACCESS.2021.3062909.

[15] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019, doi: 10.1109/ACCESS.2019.2948912.

[16] R. Abu Bakar, X. Huang, M. S. Javed, S. Hussain, and M. F. Majeed, "An Intelligent Agent-Based Detection System for DDoS Attacks Using Automatic Feature Extraction and Selection," *Sensors*, vol. 23, no. 6, 2023, doi: 10.3390/s23063333.

[17] R. Alanazi and A. Aljuhani, "Anomaly Detection for Industrial Internet of Things Cyberattacks," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2361–2378, 2023, doi: 10.32604/csse.2023.026712.

[18] Q. A. Al-Haija and M. Al-Dala'ien, "ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, 2022, doi: 10.3390/jsan11010018.

[19] N. Koroniotis, "Designing an effective network forensic framework for the investigation of botnets in the Internet of Things," 2020.

[20] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 6, 2023, doi: 10.3390/fi15060210.

[21] N. Naz *et al.*, "Ensemble learning-based IDS for sensors telemetry data in IoT networks," *Mathematical Biosciences and Engineering*, vol. 19, no. 10, pp. 10550 – 10580, 2022, doi: 10.3934/mbe.2022493.

[22] Y. Alotaibi and M. Ilyas, "Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things’ Devices Security," *Sensors*, vol. 23, no. 12, 2023, doi: 10.3390/s23125568.

[23] J. B. Awotunde, F. E. Ayo, R. Panigrahi, A. Garg, A. K. Bhoi, and P. Barsocchi, "A Multi-level Random Forest Model-Based Intrusion Detection Using Fuzzy Inference System for Internet of Things Networks," *International Journal of Computational Intelligence Systems*, vol. 16, no. 1, 2023, doi: 10.1007/s44196-023-00205-w.

[24] N. Thockchom, M. M. Singh, and U. Nandi, "A novel ensemble learning-based model for network intrusion detection," *Complex and Intelligent Systems*, 2023, doi: 10.1007/s40747-023-01013-7.

[25] M. and O. S. and A. F. Alshamy Reem and Ghurab, "Intrusion Detection Model for Imbalanced Dataset Using SMOTE and Random Forest Algorithm," in *Advances in Cyber Security*, S. and A. M. Abdullah Nibras and Manickam, Ed., Singapore: Springer Singapore, 2021, pp. 361–378.

[26] E. Alshahrani, D. Alghazzawi, R. Alotaibi, and O. Rabie, "Adversarial attacks against supervised machine learning based network intrusion detection systems," *PLoS One*, vol. 17, no. 10 October, 2022, doi: 10.1371/journal.pone.0275971.

[27] M. Bhati Nitesh Singh and Khari, "An Ensemble Model for Network Intrusion Detection Using AdaBoost, Random Forest and Logistic Regression," in *Applications of Artificial Intelligence and Machine Learning*, H. M. and R. G. Unhelker Bhuvan and Pandey, Ed., Singapore: Springer Nature Singapore, 2022, pp. 777–789.

[28] A. Churcher *et al.*, "An experimental analysis of attack classification using machine learning in IoT networks," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–32, 2021, doi: 10.3390/s21020446.

[29] P. Ghosh and R. Mitra, "Proposed GA-BFSS and logistic regression based intrusion detection system," Jun. 2015, pp. 1–6. doi: 10.1109/C3IT.2015.7060117.

[30] A. Koirala, R. Bista, and J. C. Ferreira, "Enhancing IoT Device Security through Network Attack Data Analysis Using Machine Learning Algorithms," *Future Internet*, vol. 15, no. 6, 2023, doi: 10.3390/fi15060210.

[31] A. Al-Saleh, "A balanced communication-avoiding support vector machine decision tree method for smart intrusion detection systems," *Sci Rep*, vol. 13, no. 1, 2023, doi: 10.1038/s41598-023-36304-z.

[32] Y. Saheed, O. Abdulganiyu, and T. Ait Tchakoucht, "A Novel Hybrid Ensemble Learning for Anomaly Detection in Industrial Sensor Networks and SCADA Systems for Smart City Infrastructures," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, Jun. 2023, doi: 10.1016/j.jksuci.2023.03.010.

[33] B. I. Hairab, M. Said Elsayed, A. D. Jurcut, and M. A. Azer, "Anomaly Detection Based on CNN and Regularization Techniques Against Zero-Day Attacks in IoT Networks," *IEEE Access*, vol. 10, pp. 98427–98440, 2022, doi: 10.1109/ACCESS.2022.3206367.

[34] O. D. and A. A. O. and M. J. O. Mebawondu Olamatanmi J. and Alowolodu, "Optimizing the Classification of Network Intrusion Detection Using Ensembles of Decision Trees Algorithm," in *Information and Communication Technology and Applications*, B. Misra Sanjay and Muhammad-Bello, Ed., Cham: Springer International Publishing, 2021, pp. 286–300.

[35] N. Abdullah, S. Manickam, and M. Anbar, *Advances in Cyber Security Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers: Third International Conference, ACeS 2021, Penang, Malaysia, August 24–25, 2021, Revised Selected Papers*. 2021. doi: 10.1007/978-981-16-8059-5.

[36] D. Rani, N. S. Gill, P. Gulia, F. Arena, and G. Pau, "Design of an Intrusion Detection Model for IoT-Enabled Smart Home," *IEEE Access*, vol. 11, pp. 52509–52526, 2023, doi: 10.1109/ACCESS.2023.3276863.

[37] S. Rachmadi, S. Mandala, and D. Oktaria, "Detection of DoS Attack using AdaBoost Algorithm on IoT System," in *2021 International Conference on Data Science and Its Applications (ICoDSA)*, 2021, pp. 28–33. doi: 10.1109/ICoDSA53588.2021.9617545.

[38] N. Meemongkolkiat and V. Suttichaya, "Analysis on Network Traffic Features for Designing Machine Learning based IDS," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1993/1/012029.

[39] B. Kerim, "Securing IoT Network against DDoS Attacks using Multi-agent IDS," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1898/1/012033.

[40] T. Ghrib, M. Benmohammed, and P. S. Pandey, "Automated diagnosis of attacks in internet of things using machine learning and frequency distribution techniques," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 950–961, 2021, doi: 10.11591/eei.v10i2.2766.

[41] S. Seth, K. K. Chahal, and G. Singh, "A Novel Ensemble Framework for an Intelligent Intrusion Detection System," *IEEE Access*, vol. 9, pp. 138451–138467, 2021, doi: 10.1109/ACCESS.2021.3116219.

[42] A. Mahfouz, A. Abuhussein, D. Venugopal, and S. Shiva, "Ensemble classifiers for network intrusion detection using a novel network attack dataset," *Future Internet*, vol. 12, no. 11, pp. 1–19, 2020, doi: 10.3390/fi12110180.

[43] W. Lian, G. Nie, B. Jia, D. Shi, Q. Fan, and Y. Liang, "An intrusion detection method based on decision tree-recursive feature elimination in ensemble learning," *Math Probl Eng*, vol. 2020, 2020, doi: 10.1155/2020/2835023.

https://doi.org/10.25077/xxxxx