International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 3 (2026)

ijerst.editor@gmail.com

editor@ijerst.com

ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

A Deep Learning-Based Framework for Cyber Attack Detection in IoT Networks

KADADHARAPU ANUPRIYA[1], Dr.S.SWATHI RAO[2]
[1]Student, Department of Computer Science and Engineering, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Assistant Professor, Department of AI & ML, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Email: swathirao1511@gmail.com

***Abstract*— The rapid growth of the Internet of Things (IoT) has connected billions of smart devices, making daily life more convenient while also increasing the risk of cyber threats. Traditional security methods often struggle to identify complex and evolving attacks in large-scale IoT environments. This project presents an intelligent cyberattack detection system that applies machine learning and deep learning techniques to classify network traffic as either normal or malicious. The collected IoT dataset is first pre-processed by handling missing values, converting categorical features into numerical form, and normalizing the data. Principal Component Analysis (PCA) is then used to reduce the number of features while preserving the most important information. Two classification models, namely a Multi-Layer Perceptron (MLP) neural network and a Random Forest classifier, are trained and evaluated using the processed dataset. Their performance is compared based on prediction accuracy and classification results. Experimental findings show that the neural network achieves superior accuracy and effectively detects various attack categories with minimal false predictions. The developed system offers a reliable, scalable, and efficient solution for securing IoT networks against cyber-attacks. This approach demonstrates the potential of machine learning-based intrusion detection systems in improving network security and supporting the protection of modern smart environments.**

***Keywords*— Internet of Things (IoT), Cyber Attack Detection, Intrusion Detection System (IDS), Machine Learning, Deep Learning, Multi-Layer Perceptron (MLP), Random Forest, Principal Component Analysis (PCA), Network Security, IoT Network Traffic.**

I. INTRODUCTION

The Internet of Things (IoT) has transformed the way people interact with technology by connecting everyday devices such as smart home appliances, healthcare systems, industrial sensors, and transportation networks through the internet. These interconnected devices continuously exchange data to improve automation, efficiency, and user experience. However, the rapid expansion of IoT has also increased the number of potential security vulnerabilities. Since many IoT devices have limited processing power and memory, they often lack strong security mechanisms, making them attractive targets for cyber attackers **[9], [17]**.

Cyber-attacks on IoT networks can result in unauthorized access, data theft, denial-of-service attacks, malware infections, and privacy breaches. Traditional intrusion detection systems, which rely mainly on predefined signatures or manually created rules, are often unable to identify new or sophisticated attack patterns. As cyber threats continue to evolve, intelligent detection techniques that can learn from large volumes of network traffic have become increasingly important **[26], [20]**.

Machine learning and deep learning have emerged as effective solutions for network intrusion detection because they can automatically recognize hidden patterns in network traffic and classify malicious activities with high accuracy. Algorithms such as Random Forest and Multi-Layer Perceptron (MLP) neural networks have shown promising performance in detecting different categories of cyber-attacks while reducing false alarms **[32], [13]**.

In addition, feature selection techniques such as Principal Component Analysis (PCA) improve classification efficiency by reducing redundant

information without significantly affecting prediction performance **[33]**. This project develops an IoT cyber-attack detection system that combines data preprocessing, PCA-based feature selection, and machine learning models to identify malicious network traffic. By comparing the performance of Random Forest and MLP classifiers, the proposed system aims to provide an accurate, scalable, and efficient approach for strengthening IoT network security and supporting real-time intrusion detection in modern connected environments.

II. RELATED WORK

1. da Costa et al. (2019) presented a comprehensive survey of machine learning techniques used for intrusion detection in Internet of Things (IoT) environments. The authors discussed how the rapid growth of IoT devices has introduced significant security challenges due to limited computational resources and diverse communication protocols. The survey compared supervised, unsupervised, and hybrid machine learning approaches for detecting network intrusions. It highlighted the strengths and limitations of commonly used algorithms such as Decision Trees, Support Vector Machines, Random Forest, and Artificial Neural Networks. The study concluded that machine learning methods are more effective than traditional rule-based detection systems because they can identify previously unseen attacks by learning traffic patterns. However, the authors also emphasized the importance of selecting appropriate datasets and features to improve detection performance. Their work serves as a valuable foundation for designing intelligent IoT intrusion detection systems that provide higher accuracy and better adaptability against evolving cyber threats.

2. Ferrag et al. (2020) conducted an extensive review of deep learning techniques for cyber intrusion detection. The study examined different neural network architectures, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Autoencoders, and Long Short-Term Memory (LSTM) networks, for detecting malicious network traffic. The authors compared these models using publicly available benchmark datasets and evaluated their effectiveness in terms of accuracy, detection rate, and false alarm reduction. Their findings showed that deep learning models outperform many conventional machine learning algorithms, especially when processing large-scale and complex network traffic. The paper also discussed challenges such as computational cost, dataset imbalance, and the need for real-time processing.

3. Liu and Lang (2019) reviewed various machine learning and deep learning approaches used in intrusion detection systems. The authors categorized intrusion detection techniques based on learning methods and analysed their advantages, disadvantages, and practical applications. The study highlighted that traditional signature-based detection methods are unable to recognize zero-day attacks, whereas machine learning algorithms can identify unknown threats by learning patterns from network traffic. The review compared algorithms such as Random Forest, Support Vector Machine, Decision Tree, Artificial Neural Network, and Deep Neural Network. The authors observed that deep learning models generally achieve higher detection accuracy but require larger datasets and greater computational resources. They emphasized that proper feature engineering, preprocessing, and dataset quality significantly influence model performance. This survey provides useful guidance for selecting suitable algorithms in developing efficient and reliable intrusion detection systems.

[4] Roy et al. (2017) proposed an intrusion detection framework based on Artificial Neural Networks for improving cybersecurity. The study focused on applying deep learning techniques to classify network traffic into normal and malicious categories. The proposed model was trained using benchmark intrusion datasets and evaluated using multiple performance metrics, including accuracy, precision, and recall. Experimental results demonstrated that neural networks could successfully capture complex attack patterns that are difficult for traditional machine learning methods to identify. The authors reported improved detection accuracy while maintaining a low false positive rate. They also emphasized the importance of preprocessing and feature selection in enhancing classification performance. The research concluded that deep learning-based intrusion detection systems are capable of providing robust protection against modern cyber-attacks and can be integrated into real-world network security applications.

[5] Dutta et al. (2020a) developed a deep learning ensemble model for detecting network anomalies and cyber-attacks. Their approach combined multiple deep learning classifiers to improve prediction accuracy and reduce false alarms. The authors evaluated the proposed ensemble using standard cybersecurity datasets and compared its performance with several traditional machine learning algorithms. The results demonstrated that the ensemble model consistently achieved higher accuracy, precision, recall, and F1-score across different attack categories. The study also showed that combining multiple learning models improves generalization and enhances the detection of previously unseen attacks. The authors concluded

that ensemble deep learning techniques provide a more reliable and scalable solution for intrusion detection in modern communication networks. Their findings support the adoption of advanced machine learning methods for securing IoT environments against increasingly sophisticated cyber threats.

III. DATASET DETAILS

The dataset used in this project contains IoT network traffic records collected from smart devices operating in a connected environment. It includes both normal network activities and multiple categories of cyber-attacks, making it suitable for training and evaluating machine learning models for intrusion detection. Each record represents a network communication instance and contains several features that describe packet characteristics, communication protocols, device behaviour, and traffic statistics. The final column of the dataset represents the target class, indicating whether the traffic is normal or belongs to a specific attack category. Before training the models, the dataset undergoes several preprocessing steps to improve data quality. Missing values are handled using suitable imputation techniques, while categorical attributes are converted into numerical values using label encoding. Feature scaling is applied to normalize the data and ensure consistent model performance. Principal Component Analysis is then used to reduce the number of features by selecting the most informative components, which helps improve computational efficiency and minimizes redundancy. The dataset contains approximately 357,952 network traffic records. It is divided into 80% training data and 20% testing data to evaluate the performance of the classification models. The dataset includes various attack categories such as Denial-of-Service , data probing, malicious control, malicious operation, scanning, spying, wrong setup, and normal traffic. This diverse dataset enables the proposed system to learn different attack patterns and accurately classify unknown network traffic.

IV. PROPOSED METHODOLOGY

The proposed system is designed to detect cyber-attacks in Internet of Things (IoT) network traffic using machine learning and deep learning techniques. The complete workflow consists of data collection, preprocessing, feature selection, model training, classification, and attack prediction. The objective is to accurately distinguish between normal network traffic and malicious activities while reducing false detections.

Initially, the IoT network traffic dataset is uploaded into the system. Since the dataset contains both numerical and categorical attributes, preprocessing is performed to improve data quality. Missing values are replaced using appropriate imputation methods, and categorical features are transformed into numerical values through label encoding. The dataset is then normalized using feature scaling to ensure that all features contribute equally during model training. To reduce data complexity and eliminate redundant information, Principal Component Analysis (PCA) is applied. PCA selects the most significant features while preserving the essential characteristics of the original dataset. This step decreases computational time and improves the overall efficiency of the classification models.

After feature selection, the processed dataset is divided into training and testing sets using an 80:20 ratio. Two classification algorithms are employed: a Multi-Layer Perceptron (MLP) neural network and a Random Forest classifier. The MLP model learns complex nonlinear relationships within the network traffic, while the Random Forest algorithm provides robust classification by combining predictions from multiple decision trees. The performance of both models is evaluated using prediction accuracy and confusion matrix analysis.

Finally, the trained model is used to classify new IoT network traffic as either normal or one of several cyber-attack categories, including Denial-of-Service (DoS), scanning, spying, malicious control, malicious operation, data probing, and wrong setup attacks. Experimental results demonstrate that the MLP classifier achieves higher prediction accuracy than the Random Forest model. The proposed approach provides an efficient, scalable, and reliable solution for detecting cyber-attacks in IoT environments and supports timely identification of security threats to protect connected devices and network infrastructure.

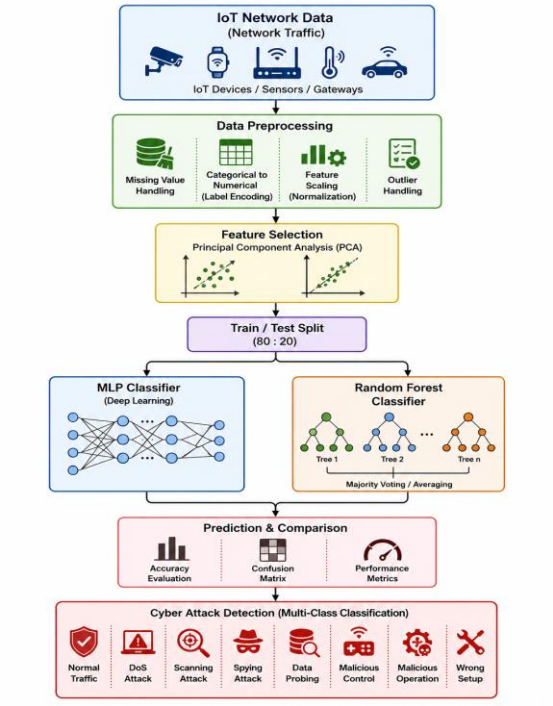

Figure 1: SYSTEM ARCHITECTURE

Figure [1] The proposed system architecture illustrates the workflow for detecting cyber-attack traces in IoT network data using machine learning techniques. Initially, IoT network traffic is collected and pre-processed by handling missing values, encoding categorical features, and normalizing the data. Principal Component Analysis (PCA) is then applied to reduce feature dimensionality while preserving important information. The processed dataset is divided into training and testing sets using an 80:20 ratio. Two classification models, Multi-Layer Perceptron (MLP) and Random Forest, are trained and evaluated. Their predictions are compared using performance metrics, enabling accurate classification of normal traffic and multiple cyber-attack categories in IoT networks.

V.RESULT AND DISCUSSION

The proposed IoT cyber-attack detection system was successfully implemented and evaluated using a real-world IoT network traffic dataset. After preprocessing the data and applying Principal Component Analysis (PCA), both the Multi-Layer Perceptron (MLP) neural network and Random Forest classifier were trained and tested. Experimental results showed that the MLP model achieved approximately **99% prediction accuracy**, outperforming the Random Forest classifier. The confusion matrix indicated that most normal and malicious traffic instances were correctly classified with very few misclassifications. The system effectively detected multiple attack types, including DoS, scanning, spying, malicious control, and data probing, demonstrating its reliability and suitability for securing IoT networks against cyber threats.

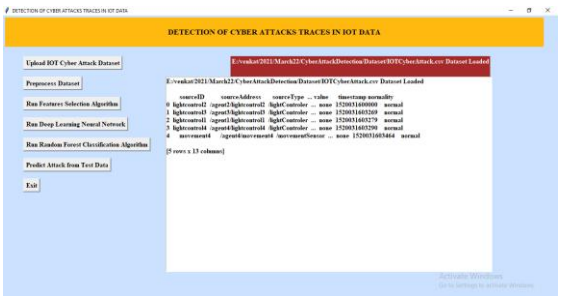

Figure 2: Upload Dataset

Figure [2] illustrates dataset loaded and we can see dataset contains some non-numeric data so we need to Preprocess Dataset to convert non-numeric data to numeric.

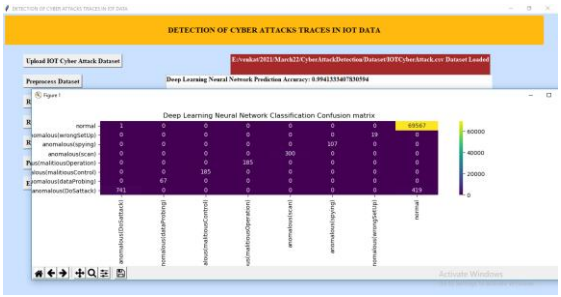

Figure 3: Neural Network

Figure [3] The image shows neural network we got 0.99% accuracy and in confusion matrix graph x-axis represents predicted attacks and y-axis represents True dataset class and in diagonal of graph we can see all test data is correctly predicted.

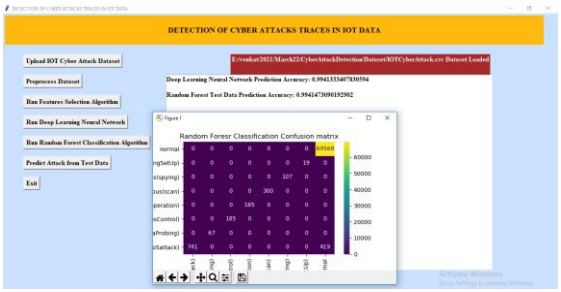

Figure 4: Random Forest

Figure [4] illustrates random forest also we got nearer accuracy but Neural network is higher.

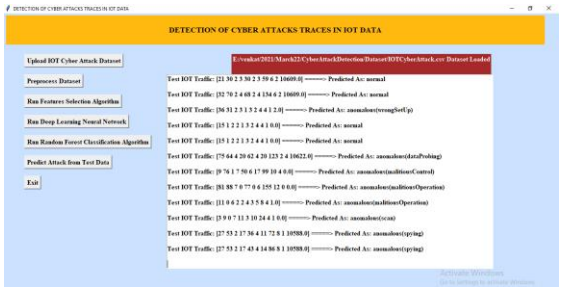

Figure 5: Test Data

Figure [5] The image shows square bracket we can see IOT traces data and after arrow symbol we can see predicted output as NORMAL or attack name. So by using machine learning algorithm we can predict 99% attacks accurately.

DISCUSSION

The experimental results demonstrate that the proposed cyber-attack detection system can effectively identify malicious activities in IoT network traffic. The preprocessing stage, including handling missing values, encoding categorical features, and normalizing the data, improved the quality of the dataset and enabled better model performance. Applying Principal Component Analysis (PCA) reduced the number of input features while preserving important information, which helped decrease computational complexity and improved training efficiency. Among the two classification models evaluated, the Multi-Layer Perceptron (MLP) neural network achieved higher prediction accuracy than the Random Forest classifier. The confusion matrix showed that the majority of normal and attack instances were correctly classified, indicating that the model learned meaningful traffic patterns from the dataset.

The system was able to detect different attack categories, including Denial-of-Service (DoS), scanning, spying, malicious control, malicious operation, data probing, and wrong setup attacks with high reliability. Although the proposed approach produced excellent results, its performance depends on the quality and diversity of the training dataset. Future improvements may include evaluating the model on more recent IoT datasets, incorporating advanced deep learning architectures such as LSTM or Transformer-based models, and implementing real-time intrusion detection. Overall, the proposed system demonstrates that machine learning techniques provide an accurate, scalable, and practical solution for enhancing IoT network security against evolving cyber threats.

VI.CONCLUSION

The increasing use of Internet of Things (IoT) devices has made network security a major concern due to the growing number of cyber-attacks targeting connected systems. This project presented an intelligent cyber-attack detection system that combines machine learning and deep learning techniques to identify malicious network traffic accurately. The proposed approach includes data preprocessing, feature selection using Principal Component Analysis (PCA), and classification using Multi-Layer Perceptron (MLP) and Random Forest algorithms. The experimental results demonstrated that the MLP model achieved higher prediction accuracy than the Random Forest classifier, making it more effective in detecting different categories of IoT cyber-attacks. The preprocessing and feature selection stages also contributed to improving classification performance by reducing redundant information and enhancing data quality. The developed system successfully classified normal and malicious traffic with high accuracy while maintaining efficient processing time. Overall, the proposed system provides a reliable, scalable, and efficient solution for securing IoT networks against evolving cyber threats. It can assist organizations in detecting attacks at an early stage and minimizing potential security risks. In the future, the system can be enhanced by incorporating advanced deep learning models, larger and more diverse datasets, and real-time network monitoring capabilities. These improvements will further strengthen the effectiveness of intrusion detection systems and provide better protection for modern IoT environments.

REFERENCES

1) [Abolhasanzadeh, 2015] Abolhasanzadeh, B. (2015). Nonlinear dimensionality reduction for intrusion detection using auto-encoder bottleneck features. In 2015 7th Conference on Information and Knowledge Technology (IKT), pages 1–5. IEEE.

2) [Agustin et al., 2020] Agustin, P., Sebastian, G., and Maria Jose, E. (2020 (accessed February 3, 2020)). Stratosphere laboratory. a labeled dataset with malicious and benign iot network traffic. https://www.stratosphereips.org/datasets-iot23.

3) [Al-Qatf et al., 2018] Al-Qatf, M., Lasheng, Y., Al-Habib, M., and Al-Sabahi, K.

(2018). Deep learning approach combining sparse autoencoder with svm for network intrusion detection. IEEE Access, 6:52843–52856.

4) [Arel et al., 2009] Arel, I., Rose, D., and Coop, R. (2009). Destin: A scalable deep learning architecture with application to high-dimensional robust pattern recognition. In. 2009 AAAI Fall Symposium Series.

5) [Barut et al., 2020] Barut, O., Luo, Y., Zhang, T., Li, W., and Li, P. (2020). Netml: A challenge for network traffic analytics. arXiv preprint arXiv:2004.13006.

6) [Berman et al., 2019] Berman, D., Buczak, A., Chavis, J., and Corbett, C. (2019). A Survey of Deep Learning Methods for Cyber Security. Information, 10(4):122.

7) [Bieniasz et al., 2019] Bieniasz, J., Stepkowska, M., Janicki, A., and Szczypiorski, K. (2019). Mobile agents for detecting network attacks using timing covert channels. J. UCS, 25(9):1109–1130.

8) [Bobowska et al., 2018] Bobowska, B., Choras, M., and Wozniak, M. (2018). Advanced analysis of data streams for critical infrastructures protection and cybersecurity. J. UCS, 24(5):622–633.

9) [da Costa et al., 2019] da Costa, K. A., Papa, J. P., Lisboa, C. O., Munoz, R., and de Albuquerque, V. H. C. (2019). Internet of things: A survey on machine learningbased intrusion detection approaches. Computer Networks, 151:147–157.

10) [D'Angelo et al., 2020] D'Angelo, G., Ficco, M., and Palmieri, F. (2020). Malware detection in mobile environments based on Autoencoders and API-images. Journal of Parallel and Distributed Computing, 137:26–33.

11) D'Angelo and Palmieri, 2021] D'Angelo, G. and Palmieri, F. (2021). Network traffic classification using deep convolutional recurrent autoencoder neural networks for spatial–temporal features extraction. Journal of Network and Computer Applications, 173:102890.

12) [D'Angelo et al., 2019] D'Angelo, G., Palmieri, F., and Rampone, S. (2019). Detecting unfair recommendations in trust-based pervasive environments. Information Sciences, 486:31–51. [Dhanabal and Shantharajah, 2015] Dhanabal, L. and Shantharajah, S. (2015). A study on nsl-kdd dataset for intrusion detection system based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering, 4(6):446–452.

13) [Dutta et al., 2020a] Dutta, V., Chora´s, M., Pawlicki, M., and Kozik, R. (2020a). A Deep Learning Ensemble for Network Anomaly and Cyber-Attack Detection. Sensors, 20(16):4583.

14) [Dutta et al., 2020b] Dutta, V., Chora´s, M., Pawlicki, M., and Kozik, R. (2020b). Hybrid model for improving the classification effectiveness of network intrusion detection. In Conference on Complex, Intelligent, and Software Intensive Systems. Springer.

15) [Ektefa et al., 2010] Ektefa, M., Memar, S., Sidi, F., and Affendey, L. S. (2010). Intrusion detection using data mining techniques. In 2010 International Conference on Information Retrieval & Knowledge Management (CAMP), pages 200–203. IEEE.

16) [Esp´ındola and Ebecken, 2005] Esp´ındola, R. and Ebecken, N. (2005). On extending f-measure and g-mean metrics to multi-class problems. Sixth international conference on data mining, text mining and their business applications, 35:25–34.

17) [Ferrag et al., 2020] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., and Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50:102419.

18) [Gao et al., 2020] Gao, M., Ma, L., Liu, H., Zhang, Z., Ning, Z., and Xu, J. (2020). Malicious network traffic detection based on deep neural networks and association analysis. Sensors, 20(5):1452.

19) [Goeschel, 2016] Goeschel, K. (2016). Reducing false positives in intrusion detection systems using data-mining techniques utilizing support vector machines, decision trees, and naive bayes for off-line analysis. In SoutheastCon 2016, pages 1–6. IEEE.

20) [Hodo et al., 2017] Hodo, E., Bellekens, X., Hamilton, A., Tachtatzis, C., and Atkinson, R. (2017). Shallow and deep networks intrusion detection system: A taxonomy and survey. arXiv preprint arXiv:1701.02145.

21) [Jin Kim et al., 2017] Jin Kim, Nara Shin, Jo, S. Y., and Sang Hyun Kim (2017). Method of intrusion detection using deep neural network. In 2017 IEEE International Conference on Big Data and Smart Computing (BigComp), pages 313–316. IEEE.

22) [Kim et al., 2016] Kim, J., Kim, J., Thu, H. L. T., and Kim, H. (2016). Long short term memory recurrent neural network classifier for intrusion detection. In 2016 International Conference on

Platform Technology and Service (PlatCon), pages 1–5. IEEE.

23) [Komisarek et al., 2020] Komisarek, M., Choras, M., Kozik, R., and Pawlicki, M. (2020). Real-time stream processing tool for detecting suspicious network patterns using machine learning. ARES conference.

24) [Kozik and Chora´s, 2017] Kozik, R. and Chora´s, M. (2017). Pattern extraction algorithm for netflow-based botnet activities detection. Security and Communication Networks.

25) [Ksieniewicz and Wo´zniak, 2018] Ksieniewicz, P. and Wo´zniak, M. (2018). Imbalanced data classification based on feature selection techniques. In International Conference on Intelligent Data Engineering and Automated Learning, pages 296–303. Springer.

26) [Liu and Lang, 2019] Liu, H. and Lang, B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey. Applied Sciences, 9(20):4396.

27) [Lopez-Martin et al., 2017] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., and Lloret, J. (2017). Network Traffic Classifier With Convolutional and Recurrent Neural Networks for Internet of Things. IEEE Access, 5:18042–18050.

28) [Panda et al., 2012] Panda, M., Abraham, A., and Patra, M. R. (2012). A hybrid intelligent approach for network intrusion detection. Procedia Engineering, 30:1–9.

29) [Pawlicki et al., 2020] Pawlicki, M., Chora´s, M., and Kozik, R. (2020). Defending network intrusion detection systems against adversarial evasion attacks. Future Generation Computer Systems.

30) [Potluri et al., 2018] Potluri, S., Ahmed, S., and Diedrich, C. (2018). Convolutional neural networks for multi-class intrusion detection system. In International Conference on Mining Intelligence and Knowledge Exploration, pages 225–238. Springer.

31) [Rend´on et al., 2020] Rend´on, E., Alejo, R., Castorena, C., Isidro-Ortega, F. J., and Granda-Guti´errez, E. E. (2020). Data sampling methods to deal with the big data multi-class imbalance problem. Applied Sciences, 10(4):1276.

32) [Roy et al., 2017] Roy, S. S., Mallik, A., Gulati, R., Obaidat, M. S., and Krishna, P. V. (2017). A deep learning based artificial neural network approach for intrusion detection. In International Conference on Mathematics and Computing, pages 44–53. Springer.

33) [Topolski, 2020] Topolski, M. (2020). Application of the stochastic gradient method in the construction of the main components of pca in the task diagnosis of multiple sclerosis in children. In Krzhizhanovskaya, V. V., Z´avodszky, G., Lees, M. H., Dongarra, J. J., Sloot, P. M. A., Brissos, S., and Teixeira, J., editors, Computational Science – ICCS 2020, pages 35–44, Cham. Springer International Publishing.

34) [Torres et al., 2016] Torres, P., Catania, C., Garcia, S., and Garino, C. G. (2016). An analysis of recurrent neural networks for botnet detection behavior. In 2016 IEEE biennial congress of Argentina (ARGENCON), pages 1–6. IEEE.

35) [Yan and Han, 2018] Yan, B. and Han, G. (2018). Effective feature extraction via stacked sparse autoencoder to improve intrusion detection system. IEEE Access, 6:41238–41248.

36) [Zhang et al., 2018] Zhang, C., Cheng, X., Liu, J., He, J., and Liu, G. (2018). Deep sparse autoencoder for feature extraction and diagnosis of locomotive adhesion status. Journal of Control Science and Engineering, 2018.

37) [Zhao et al., 2017] Zhao, R., Yan, R., Wang, J., and Mao, K. (2017). Learning to monitor machine health with convolutional bi-directional lstm networks. Sensors, 17(2):273.

38) [Zong et al., 2020] Zong, W., Chow, Y.-W., and Susilo, W. (2020). Interactive threedimensional visualization of network intrusion detection data for machine learning. Future Generation Computer Systems, 102:292–306.