iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.5435

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

A Survey on Machine and Deep Learning Based Intrusion Detection Systems for IoT

Haripriya A P[1], Meenu V[2], Malavika M Hari[3], Risvana K A[4], Sruthi P R[5]
[1]*Associate Professor, Dept. of IT, Government Engineering College, Bartonhill, Thiruvananthapuram, Kerala, India*
[2, 3, 4, 5]*Department of Information Technology, Government Engineering College, Bartonhill, Thiruvananthapuram, Kerala, India*

Abstract: ***In recent times, the Internet of Things (IoT) and its diverse range of applications have emerged as one of the most popular and highly researched areas. The characteristics that make IoT easily applicable to real-life applications also expose it to cyber threats, thereby emphasizing the need for effective security measures. The rapid advancement of IoT is revolutionizing business processes and society as a whole. However, as this technology continues to evolve, it becomes increasingly important to prioritize the detection and awareness of vulnerabilities. Adopting a proactive approach is crucial to prevent unauthorized access to critical resources and business functions, thereby ensuring the continuous availability and operation of the system. Failing to prevent the occurrence of DoS and DDoS attacks can have adverse effects on data confidentiality, integrity, and availability, thereby highlighting the importance of effective intrusion detection and prevention measures. The literature has presented a wide range of intrusion detection methods aimed at addressing computer security threats. These methods can generally be categorized into***
Signature-based Intrusion Detection Systems (SIDS) and Anomaly-based Intrusion Detection Systems (AIDS). In this survey, our aim is to conduct a comprehensive analysis of various anomaly-based intrusion detection systems that utilize machine learning and deep learning approaches.
Keywords: Internet of Things, Intrusion Detection System, Datasets, Machine Learning Algorithms, Deep Learning Algorithms

I. INTRODUCTION

The Internet of Things is an emerging technology that is revolutionizing industries and enhancing daily life through the use of innovative devices. It involves a network of interlinked physical objects, equipped with sensors, software, and network connectivity, which collectively form a system. These devices gather and exchange data, enabling them to interact with each other and their environment. The IoT's specific characteristics, including openness and resource limitations, create particular challenges that make it susceptible to security vulnerabilities and targeted attacks. It is crucial to regularly inspect IoT devices to protect them from a variety of threats.

Analysing the devices and implementing necessary precautions are vital steps in preventing potential attacks and safeguarding against unauthorized access or data breaches. Intrusion Detection is the process of analysing and examining various network traffic and reacting when a mischievous attack happens with the signs of intrusion. An Intrusion Detection System (IDS) helps us identify suspicious activities and potential threats that may go unnoticed by regular firewalls.

Traditional IDS have been replaced by Machine learning and deep learning techniques to enhance their effectiveness in identifying and responding to security threats These techniques analyse large volumes of data generated by IoT devices and detect anomalous or malicious activities more accurately.

Intrusion Detection Systems are designed to automatically identify and analyse abnormal and irregular behaviours within a network or host, with the goal of ensuring security and protection. These systems are capable of detecting various types of attacks across different layers of the network, including the Perception, Transport, and Network layers [1]. Fig 1.1 shows the architecture of Intrusion detection system. IDS can be divided into three main modules such as malicious activities collection, anomaly detection and classification . In the first module, malicious activities are collected from input sources, such as network traffic or system logs. This data serves as the foundation for further analysis. In the second module, the collected data is processed and analysed to identify potential attacks.

This involves comparing the observed behaviour against known attack patterns or using anomaly detection techniques to identify deviations from normal behaviour. Finally, in the third segment, the detected attacks are classified and reported to system administrators or security personnel, who can then take appropriate actions to mitigate the threats and protect the network.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

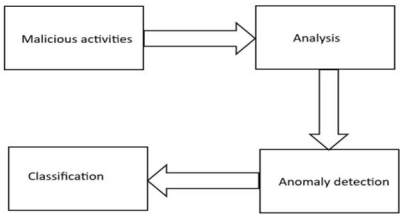


Figure 1.1: Architecture of an intrusion detection system

By efficiently gathering and analysing malicious activities, an Intrusion Detection System (IDS) plays a vital role in strengthening network security. It accomplishes this by promptly identifying and responding to potential threats, thus enhancing the overall security posture.. The reporting mechanism ensures that relevant parties are informed about the detected attacks, enabling them to take appropriate measures to safeguard the network and mitigate the potential impact of the intrusions. The major categories of IDS based on the detection and deployment methods are Detection-based IDS and Data-based IDS [2].

1) Detection-Based IDS

There are two main categories of detection based IDS: signature-based IDS and anomaly-based IDS [3], Signature-based IDS relies on pattern-matching techniques to identify known attacks by comparing network traffic against a database of attack signatures..SIDS may struggle to detect new or unknown attacks until their signatures are added to the database. Maintaining a large signature database and comparing against potential intrusions can be resource-intensive. Anomaly-based IDS is preferred by many researchers due to its ability to detect unknown or previously unseen attacks. AIDS learns the normal behaviour of the system during a training stage using a typical traffic profile and then tests against a new dataset to identify deviations that may indicate intrusions. AIDS can offer better accuracy with a lower false alarm rate, but continuous updating of traffic profiles to account for new attacks can increase system load. AIDS can be further categorized into statistical-based IDS, knowledge-based IDS, and machine learning-based IDS.

2) Data-Based IDS

Data-based IDS, also referred to as location-based IDS, can be classified into three main categories: host-based IDS (HIDS), network-based IDS (NIDS), and hybrid based IDS [4]. Network-based intrusion detection systems monitor network traffic extracted from a network. They can be deployed in various environments and are independent of specific operating systems. NIDS are capable of identifying specific attacks and can be effective in detecting harmful attacks like denial of service (DoS) and brute force. NIDS operate within their own network segment, monitoring the attacks that pass through that segment. SNORT is an example of an open-source NIDS. Host-based intrusion detection systems monitor a wide range of segments within a host device. They can control the behaviour of different objects within the host and are capable of detecting insider attacks that may not involve network traffic. Examples of HIDS include Tripwire and Advanced Intrusion Detection Environment. Both NIDS and HIDS have their advantages and disadvantages. NIDS are easy to set up, operate, and typically have lower costs. However, their effectiveness relies on the availability of security features and signatures. If an NIDS is unaware of certain attacks or lacks necessary signatures, it may fail to identify them. HIDS, on the other hand, function as security managers that maintain and control the host device. By combining the strengths of NIDS and HIDS, a hybrid IDS can provide greater flexibility and effectiveness. Hybrid IDS leverages the best features of both NIDS and HIDS, offering a comprehensive approach to intrusion detection [1].

II. MACHINE LEARNING TECHNIQUES

There are few works present in the literature which suggest methods for machine learning-based intrusion detection systems employ machine learning algorithms to identify and respond to potential intrusions or malicious activities within a network. The authors considered that the systems are trained on labeled datasets containing instances of both normal and malicious network behavior. By learning from these examples, the models can recognize patterns and characteristics associated with various types of attacks. Once trained, they can classify incoming network traffic or events as normal or suspicious based on the patterns they have learned. This enables them to effectively detect and mitigate potential security threats. In this literature review, several papers based on Machine learning based intrusion detection system were reviewed.

In the paper [5], the classification of intrusions using machine learning (ML) algorithms, specifically Linear Discriminant Analysis (LDA), Classification and Regression Trees (CART), and Random Forest (RF) was proposed. The study employed the KDD-CUP dataset, which consists of 42 features and 494,021 instances. The dataset was labeled into five classes: DoS, probes, user-to-remote attack (U2R), remote-to-local, and normal. The research followed a three-step process, including data preprocessing, classification, and evaluation.

During the data preprocessing stage, the features were mapped to functions, and a filter method was used to select relevant features. Through the correlation attribute evaluation and ranker search method, 20 variables were chosen from the initial 42. For classification, LDA, CART, and Random Forest algorithms were utilized. In the evaluation phase, performance metrics such as accuracy and kappa were employed to assess the effectiveness of the models. Based on the experimental findings, the Random Forest algorithm exhibited the highest accuracy rate of 99.65%. It was closely followed by LDA with an accuracy of 98.1%, while CART achieved an accuracy of 98%.The implementation of the work was conducted using R Studio [5].

In the paper [6], A machine learning approach for intrusion detection system on NSL-KDD dataset has been presented in. the study utilized different classification methods including SVM, KNN, LR, NB, MLP, RF, ETC, and DT as an intrusion analysis engine. The NSL-KDD dataset contains a significant number of entries classified as DoS attacks, indicating a strong representation of this attack class. However, the results for the U2L attack class were found to be poor. Overall, the random forest, extra-tree, and decision tree classifiers achieved accuracy levels above 99% across all four feature subsets. These classifiers are effective in handling unevenly distributed data and can mitigate the impact of data imbalance. Random forest, in particular, utilizes the bootstrap process to increase the occurrence of the minority class, thus reducing misclassification. Decision trees demonstrate excellent generalization ability by comprehensively analyzing all possibilities along their branches, leading to exceptional performance. [6].

The effectiveness of six Machine Learning (ML) techniques for detecting MQTT based attacks is highlighted in [7]. The study assesses the performance of different feature abstraction levels, including packet-based, unidirectional flow, and bidirectional flow features. To evaluate the models, a simulated MQTT dataset is generated and used for training and testing. The experimental findings demonstrate the efficacy of the proposed ML models in meeting the requirements of Intrusion Detection Systems (IDS) for MQTT-based networks. The study highlights the significance of employing flow-based features to distinguish MQTT-based attacks from legitimate traffic. On the other hand, packet-based features are deemed adequate for detecting typical network attacks. The dataset used in the study includes normal operation data as well as four attack scenarios. The results provide further evidence of the superiority of flow-based features in effectively distinguishing between benign traffic and MQTT-based attacks due to their shared characteristics.

Regarding performance metrics, the transition from packet-based features to unidirectional flow features significantly improves the weighted average recall from 75.31% to 93.77%, and further to 98.85% with bidirectional flow features. Likewise, the weighted average precision demonstrates a significant improvement, rising from 72.37% when using packet-based features to 97.19% when utilizing unidirectional flow features. Furthermore, the precision further increased to 99.04% when incorporating bidirectional flow features.[7].

The study in [8] focuses on exploring feature extraction techniques for machine learning-based intrusion detection in IoT networks. The study explores different combinations of Feature Reduction (FR) and Machine Learning (ML) techniques to improve classification results using NIDS datasets. The study evaluates six ML models: Deep Feed Forward (DFF), Convolutional Neural Network (CNN), Recurrent Neural Network (RNN), Decision Tree (DT), Logistic Regression (LR), and Naive Bayes (NB). Three Feature Extraction (FE) algorithms are considered: Principal Component Analysis (PCA), Auto-encoder (AE), and Linear Discriminant Analysis (LDA). The evaluation is conducted on three benchmark datasets: UNSW-NB15, ToN-IoT, and CSE-CIC-IDS2018. The results show that LDA achieves higher classification accuracy for the UNSW-NB15 dataset compared to the other two datasets. In fact, the accuracy of LDA for UNSW-NB15 is close to that achieved using the complete set of features. Among the ML models, the Dense Feed Forward (DFF) model performs exceptionally well when applied to the complete dataset, thanks to its ability to assign weights to relevant features.

The experimental evaluation conducted explores various combinations of feature extraction (FE) and machine learning (ML) techniques to identify effective combinations tailored to each dataset. LDA consistently achieves the best results among the ML models with FE algorithms, while Naive Bayes (NB) exhibits relatively poorer performance. Moreover, concerning the UNSW-NB15 dataset, the CNN classifier demonstrates superior performance when applied to the dimensions derived from autoencoder (AE) techniques. [8].

Ensemble methods combine the predictions of multiple individual models to make a final decision or prediction. In the paper [9], an ensemble-based intrusion detection model is proposed, utilizing six different supervised ML classification techniques for intrusion detection. These ML algorithms include Decision Tree (DT), Naive Bayes (NB), Gaussian multinomial, Random Forest (RF), Logistic Regression (LR), Linear SVM, and Stochastic Gradient Descent Classifier (SGD Classifier). The study uses the CICIDS 2017 dataset, which contains 15 class labels. The six ML algorithms were applied for multiclass classification using all the features of the dataset to categorize the 15 different types of labels. Additionally, binary classification algorithms were applied to the same dataset's features.The model is evaluated with four feature selection methods and found that the Linear SVM method showed the best performance in both binary and multiclass classification algorithms. It achieved an average accuracy of 88.19% and 85.56% for binary and multiclass classification, respectively. Consequently, Linear SVM was selected for further classification processes.o improve the overall detection performance, the results of the Decision Tree, Naive Bayes, and Logistic Regression algorithms, which demonstrated optimum performance, were combined using a hard voting module. This ensemble method detected all types of attacks present in the dataset, providing significant accuracy while requiring low computational power and resources, and achieving a low false alarm rate [9].

III. DEEP LEARNING TECHNIQUES

The authors suggest that deep learning-based intrusion detection system excel at automatically learning complex patterns and representations from large volumes of data, making them well suited for intrusion detection tasks. The literature review examined multiple papers that revolve around Deep learning-based intrusion detection systems. Protocol Based Deep Intrusion Detection (PB-DID) has been proposed in [10], in which the features of the two latest benchmark data sets, the UNSW-NB15 and the Bot-IoT are compared. The PB-DID process involves feature comparison, feature selection methods, data preprocessing, and model training using the LSTM deep learning model. The UNSWNB15 dataset contains 49 features, with the 48th feature representing a multi-class label and the 49th feature as a binary label. On the other hand, the Bot-IoT dataset consists of 46 features, with the last three features representing labels. Through the analysis and comparison of features in both datasets, the authors identify that 29 features in the Bot-IoT dataset are similar to those in the UNSW-NB15 dataset. To address issues like data imbalance and overfitting, the authors select an equal number of packets from each category. The PB-DID architecture employs an LSTM model with an input layer, two hidden layers, and an output layer. Two types of output layers are used: one for binary classification and the other for multi-class classification. The DL (Deep Learning) technique is applied to classify DoS (Denial of Service) and DDoS (Distributed Denial of Service) traffic. The model achieves an accuracy of 96.3% [10].

The research paper [11] introduces a novel Intrusion Detection System (IDS) that utilizes Deep Neural Networks (DNN) to address the challenges posed by complex security-related networks and evolving attacks. The proposed IDS employs Deep Convolutional Neural Networks (DCNN) for anomaly detection, classification, and characterization. To handle the issue of new attack variations, the researchers develop a novel technique called Two-Stage Deep Learning (TSDL). This technique incorporates stacked autoencoders and a SoftMax classifier for Network Intrusion Detection System (NIDS). The performance of the IDS is evaluated using two publicly available datasets, namely UNSW-NB15 and KDD99. The experimental analysis showcases enhanced detection capabilities and recognition rates. Specifically, the achieved accuracy rates are reported as 99.996% for the KDD99 dataset and 89.134% for the UNSW-NB15 dataset. [11].

AI-Empowered Framework IDS for IoT has been proposed in [9]. The framework consists of two main phases. The first phase involves utilizing the collected data from IoT devices to construct a deep learning model capable of detecting and predicting intrusions. The model is trained using the data to learn patterns and characteristics of normal and intrusive behavior in IoT networks. In the second phase, explainable AI (XAI) approaches are applied to integrate the deep learning model with the sensed data from IoT networks. This integration enables the interpretation and explanation of the predictions made by the model, providing insights into the reasons behind the classification decisions. The implementation of the proposed framework utilizes PyTorch and XAI libraries, including SHAP. These tools enable the analysis of two well-established public network security datasets: NSL-KDD and UNSW-NB15. By utilizing these datasets, the framework can be evaluated and validated for its effectiveness in detecting and predicting intrusions in IoT networks [12].

The research paper [10] introduces a DNN-based intrusion detection system for MQTT-enabled IoT smart systems The proposed model's performance is assessed by utilizing both the MQTT-IoT-IDS2020 dataset and an additional MQTT dataset for evaluation purposes. To assess the effectiveness of the proposed DNN-based IDS, its performance is compared to conventional machine learning (ML) based IDSs such as KNN, NB, DT, and RF.

The model utilizes a default learning rate and the ADAM optimizer During the evaluation process, binary-class and multi-class attack classification are performed, and various activation functions are tested at the output layers. The results clearly indicate that the proposed deep learning model attains a high level of accuracy in both binary-class and multi-class attack classification tasks. For Bi-flow and Uni-flow featured data, the accuracy reaches 99% and 98% respectively. In the case of Packet-flow featured data, the accuracy for binary-class and multi-class classification is 94% and 90% respectively. Furthermore, the proposed model is tested against various attacks, including DoS and MitM, in an MQTT-based IoT system. The results indicate that the proposed model outperforms other state-of-the-art deep learning models, exhibiting higher accuracy in detecting and classifying attacks [13].

IV. CONCLUSION

Intrusion Detection System technologies continue to evolve and they will more closely simulate and replicate the functionality of their real-world counterparts. Indeed, cybercriminals are becoming increasingly proficient at targeting computer users through a combination of sophisticated techniques and social engineering strategies. They employ various tactics to mask their identities, encrypt their communication, distance themselves from illegal profits, and leverage resilient infrastructures to avoid detection and compromise. As a result, the need for advanced intrusion detection systems capable of detecting modern malware becomes increasingly crucial to safeguard computer systems.

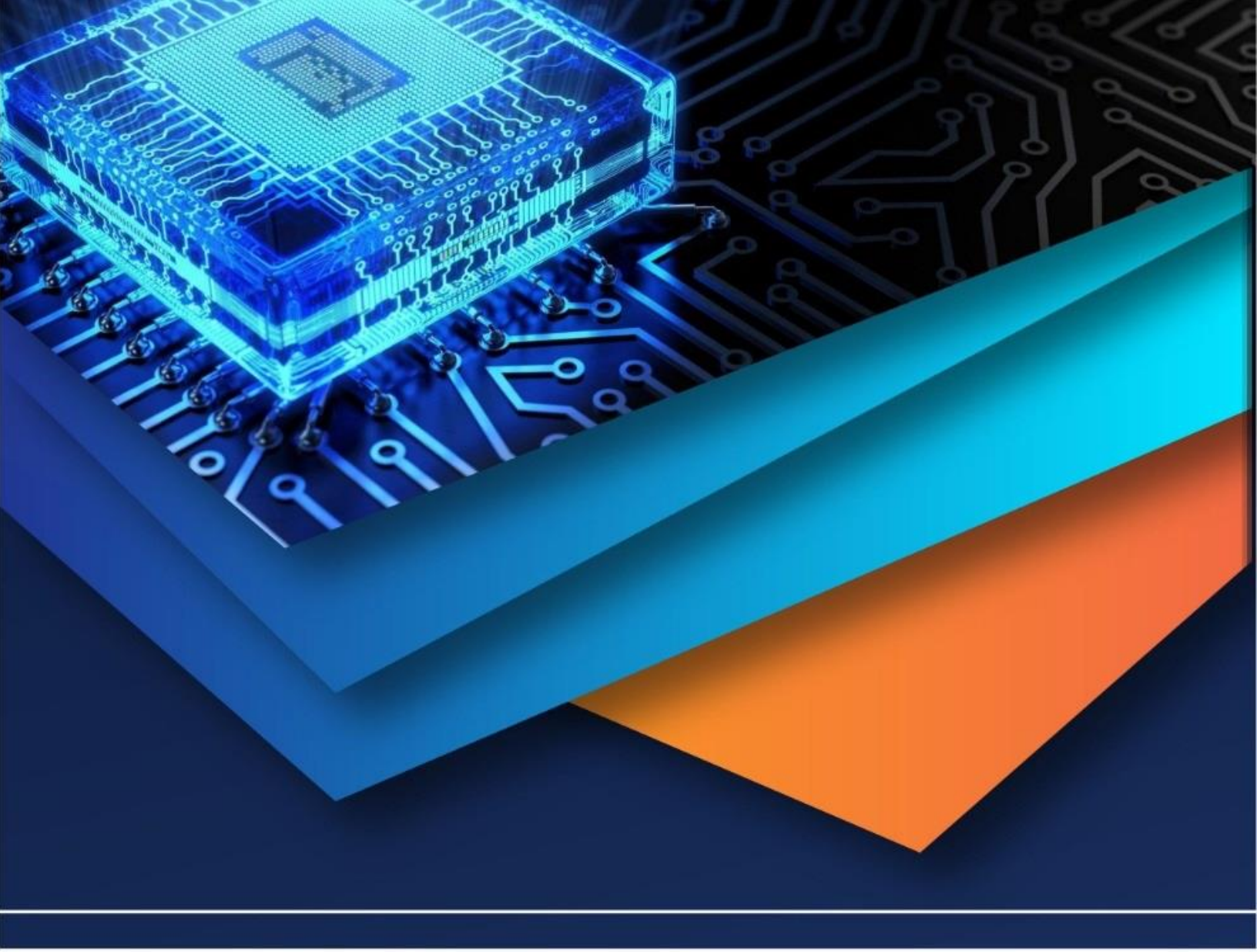
From the survey, it was concluded that despite the availability of numerous intrusion detection systems, there is a demand for more efficient models to address future cybersecurity challenges in the IoT domain. The analysis covered various datasets used for intrusion detection and examined different performance metrics for IDS.

V. ACKNOWLEDGMENT

The authors of this paper declare that they have cited paper references to the corresponding authors and have avoided all forms of plagiarism to the best of their abilities

REFERENCES

[1] Abhishek Verma and Virender Ranga. “Machine learning based intrusion detection systems for IoT applications”. In: Wireless Personal Communications 111 (2020), pp. 2287–2310.
[2] Adeel Abbas et al. “A new ensemble-based intrusion detection system for internet of things”. In: Arabian Journal for Science and Engineering (2021), pp. 1–15
[3] Pedro Garcia-Teodoro et al. “Anomaly-based network intrusion detection: Techniques, systems and challenges”. In: computers & security 28.1-2 (2009), pp. 18–28.
[4] Asmaa Shaker Ashoor and Sharad Gore. “Importance of intrusion detection system (IDS)”. In: International Journal of Scientific and Engineering Research 2.1 (2011), pp. 1–4.
[5] T Saranya et al. “Performance analysis of machine learning algorithms in intrusion detection system: A review”. In: Procedia Computer Science 171 (2020), pp. 1251–1260.
[6] Iram Abrar et al. “A machine learning approach for intrusion detection system on NSL-KDD dataset”. In: 2020 international conference on smart electronics and communication (ICOSEC). IEEE. 2020, pp. 919–924.
[7] Hanan Hindy et al. “Machine learning based IoT intrusion detection system: An MQTT case study (MQTT-IoT-IDS2020 dataset)”. In: Selected Papers from the 12th International Networking Conference: INC 2020. Springer. 2021, pp. 73– 84.
[8] Mohanad Sarhan et al. “Feature extraction for machine learning-based intrusion detection in IoT networks”. In: Digital Communications and Networks (2022).
[9] Adeel Abbas et al. “A new ensemble-based intrusion detection system for internet of things”. In: Arabian Journal for Science and Engineering (2021), pp. 1–15.
[10] Muhammad Zeeshan et al. “Protocol-based deep intrusion detection for dos and ddos attacks using unsw-nb15 and bot-iot data-sets”. In: IEEE Access 10 (2021), pp. 2269–2283.
[11] Amjad Rehman Khan et al. “Deep learning for intrusion detection and security of Internet of things (IoT): current analysis, challenges, and possible solutions”. In: Security and Communication Networks 2022 (2022).
[12] Zakaria Abou El Houda, Bouziane Brik, and Lyes Khoukhi. ““why should i trust your ids?”: An explainable deep learning framework for intrusion detection systems in internet of things networks”. In: IEEE Open Journal of the Communications Society 3 (2022), pp. 1164–1176.
[13] Muhammad Almas Khan et al. “A deep learning-based intrusion detection system for mqtt enabled iot”. In: Sensors 21.21 (2021), p. 7016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY