Comparative Analysis of Intrusion Detection Systems for Internet of Things

Nithya Nedungadi, Akshitha K Subran, Sriram Sankaran
Center for Cybersecurity Systems and Networks
Amrita Vishwa Vidyapeetham, Amritapuri, India

2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) | 979-8-3503-0767-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ANTS59832.2023.10468987

***Abstract*—The expansion of IoT has led to an abundance of interconnected devices that are susceptible to cyber risks, including malware, ransomware, denial-of-service attacks, and data breaches. Conventional security measures are frequently inadequate in handling these notorious threats, giving rise to the importance of Intrusion Detection Systems (IDS) as a vital means of identifying and mitigating them. The comparative analysis of IDS involves evaluating and comparing the performance of different IDS solutions based on a set of criteria, such as detection accuracy, resource consumption, and ease of deployment and management. Several network service providers offer packet analysis services, yet selecting the optimal IDS approach is a challenging and crucial decision due to its substantial impact on performance and energy consumption for resource-constrained IoT devices. IDS techniques have been well examined for this purpose in terms of performance, but the evaluation of energy usage is typically unexplored. In this work, we comparatively analyse the signature-based and anomaly-based Intrusion Detection Systems using the CIC IoT dataset. Our experiments conducted using Raspberry Pi and an external source meter reveal that Anomaly-based IDS uses 12.5% more peak power while utilizing only 8% of CPU resources, as compared to the 10% utilization of a Signature-based IDS which achieves a higher accuracy of 95.52%. The insights from the study can be used to help organisations make informed decisions about selecting and deploying the most appropriate IDS for their IoT environments.**

I. Introduction

An Intrusion Detection System (IDS) is a diligent monitoring system designed to detect any unauthorized access, activity, or alteration of files by computers or networks. It intends to track and analyze network traffic from different resources and detect malicious activities. We categorize IDS approaches in the Internet of Things (IoT) as signature-based [1], hybrid [2], specification-based [3] and anomaly-based [4], depending on the detection mechanism.

Despite the advancements in IoT Intrusion Detection Systems (IDS), certain limitations and gaps persist within the existing solutions. The high false alarm rate is a major issue, leading to excessive false positives. These IDSs may have challenges in detecting emerging attacks [5].

An IDS has the potential to thwart an attack aimed at a specific host unless the host has already been compromised. However, it can't prevent a compromised host from launching malicious activities like DDoS attacks [6]. IDSs typically operate on a single host or router as centralized solutions. They must reduce malicious network traffic, failing to optimize network capacity and needlessly consuming energy for routing discarded packets.

Due to resource constraints, it is difficult to deploy IDS to IoTs, necessitating effective packet analysis for attack detection, which requires more CPU cycles and increases energy usage. Evaluating the energy and performance of such IDS is essential for a successful implementation, depending on the requirements of the application.

In this work, we provide a comparative analysis of Signature-based and Anomaly-based IDS, since they are the most popular and widely acknowledged IDS [7]. Our focus lies in configuring these IDS platforms for IoT environments, utilizing embedded hardware like Raspberry Pi. Furthermore, we perform an assessment of power usage through source meters [8], analyzing the performance and energy consumption of IoT devices, alongside evaluating the resource utilization of IDS systems.

Our analysis reveals that, Anomaly-based IDS on the Raspberry Pi consumes 3.2 watts of peak power compared to the Signature-based IDS's 2.8 watts. The latter performs better, scoring 95.52% accuracy, compared to 93.2% for the anomaly-based version. The CPU resource utilization for the Anomaly-based IDS and the Signature-based IDS are around 8% and 10%, respectively. The insights from our study can be used to assist organizations in making sensible decisions about choosing and installing the most suitable IDS for their IoT environments.

II. Related Work

In this section, we review existing literature along with the different categories of Intrusion Detection Systems.

Green IDS: Mauro Migliardi *et al.* [9], proposed reducing energy consumption in core networks by swiftly discarding malicious packets. Their simulation employed an energy model grounded in existing green networking initiatives, showcasing potential energy reduction. Yet, the success relies on factors such as the proportion of malicious packets, idle equipment energy, and consumption patterns with traffic.

Specification-Based IDS: Behavior-specification-based intrusion detection is a method that uses human-specified legitimate behaviors to measure a node's misbehavior, enabling lightweight intrusion detection in systems with severe resource constraints where user, group, or data profiling is not feasible [3].

979-8-3503-0767-2/23/$31.00 ©2023 IEEE

2023 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS): Women in Engineering (WiE)

Signature-Based IDS: The likelihood of detection improves with targeted signatures for the exploited vulnerability. Ongoing research aims to create signatures by spotting these payloads in network traffic. For instance, Rubin *et al.* [5] proposed a method to counter the utilization of techniques that fragment the payload into multiple TCP packets. Hence, understanding both the content and transmission of the exploit's payload is crucial. In particular, if odd payloads lacking malicious intent are identified, alerts should be triggered for payloads linked to malicious objectives.

Anomaly-Based IDS: The research by Tanzila Saba *et al.* [4] presents a CNN-based technique for anomaly-based IDS, leveraging the Internet of Things' potential to effectively analyze all IoT traffic, demonstrating the model's ability to identify potential breaches and unusual traffic patterns. The preliminary work by Nimmy *et al.* [10] illustrates that supervised classification algorithms and selected features can effectively distinguish normal IoT device behavior from anomalous behavior caused due to a DDoS attack.

Hybrid IDS: In hybrid detection, signature-based methods can rapidly and effectively identify known attacks, while anomaly-based techniques are employed to discover novel or unrecognized attacks that evade signature-based systems [3].

Comparative study:

IoT IDSs based on specification and anomaly consider intrusions when deviations from normal behavior occur, without relying on machine learning techniques and manually creating specifications [2].

Suricata proved to be the most effective open-source Network Intrusion Detection System (NIDS) in a research [11] that compared the performance of Snort IDS's latest release, Snort 3, with Suricata IDS in resource use, packet losses, and warnings lost.

Signature-based solutions, unlike anomaly-based methods, can be outsourced and utilize threat intelligence, simplifying rule creation, modification, and customization [12]. They provide detailed threat insights for easy investigation and decision-making.

Rohit Jaysankar *et al.* [13] evaluated the signature-based approaches in terms of classification accuracy, energy consumption, and execution time of the algorithms on a custom attack dataset generated using Wireshark and on the publicly available NSL-KDD dataset.

In contrast to existing approaches, our study examines the energy and performance impacts of Signature-based and Anomaly-based IDS in IoTs, analyzing energy-performance trade-offs. The model is developed for anomaly-based IDS and signature-based IDS using two classification algorithms.

III. Background

This section gives a quick overview of intrusion detection systems and the various techniques we used to conduct this study.

A. Signature-based Intrusion Detection: Basic Operation

Signature-based Intrusion Detection (SIDS) is a method for identifying proven attacks by identifying their characteristics. SIDS, such as Snort, Suricata, and Bro [7], identify and block attacks based on specific traffic patterns like viruses and malware, using the CIC-IoT dataset's attack patterns. These SIDS trigger alerts if network traffic matches a signature.

SIDS offers practical advantages, such as active communities and vendors providing signature databases for organizations to use [14]. Signature-based systems like Snort and Suricata effectively detect intrusions by identifying system events with known malicious behavior. However, they lack the ability to detect unknown attacks and require specialized knowledge for rule construction and updates.

Suricata is a multi-threaded IDS system built on the Snort codebase, providing scalable protection against diverse threats. It uses multiple CPU cores, supports various protocols, has a robust rule language, and can identify zero-day attacks [15].

B. Anomaly-based Intrusion Detection: Basic Operation

Anomaly-based Intrusion Detection (AIDS) is a cybersecurity system that identifies anomalous activity in a network or system, recognising deviations from expected patterns. It collects data from traffic, system performance, network logs, and user behaviours to provide a baseline of normal behaviour. AIDS looks for variations from this baseline on a regular basis to look for unexpected patterns, serious events, or statistical anomalies that might signal security issues or unusual behaviour.

The system uses machine learning algorithms like Isolation Forest, SVM, and K-Means Clustering to improve IoT security, while deep learning, specifically CNN-based systems, can enhance anomaly-based intrusion detection, thereby enhancing IoT security [16].

IV. Energy and Performance Model

In this section, we provide an overview of the performance and energy costs associated with the IDS to identify threats and raise alarms. When an intrusion detection system discovers and alerts on a real infiltration attempt, it is referred to as True Positives (TP). When an IDS issues an alarm for a behaviour that is not malicious, this is referred to as a false positives (FP). True Negatives (TN) packets are those the IDS recognises a behaviour as acceptable and the action is truly acceptable. When a real intrusion or malicious behaviour is not detected by the IDS, this is referred to as a false negative (FN). Computations are done to evaluate the performance and correctness of the system. According to the confusion matrix by Karl Pearson [17], the performance metrics are given by the equations (1) through (4);

$$Accuracy = \frac{(TP + TN) \times 100}{TP + TN + FP + FN} \tag{1}$$

Precision: Precision is defined as the proportion of attack cases that were correctly predicted relative to the predicted size of the attack class.

$$Precision = \frac{TP \times 100}{TP + FP} \tag{2}$$

Recall: Recall is defined as the proportion of correctly predicted attack cases to the actual size of the attack class.

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

F1 Score: An evaluation of a test's accuracy is done using the F1-score. It measures the balance between precision and recall of a classification model.

$$F1score = \frac{2 \times Recall \times Precision \times 100}{Recall + Precision} \tag{4}$$

Average Power: The power values are noted using the source meter. Average Power is measured as the power consumed per unit time. It is estimated using the equation (5).

$$P_{average} = \frac{P_{total}}{T_{time}} \tag{5}$$

where P_{total} and T_{time} refer to total power consumption and unit time respectively

Energy Consumption: Energy consumption measures power usage for a device's functions or operations over a specific period. It is calculated by using the equation (6).

$$Energy = P_{average} \times T_{time} \tag{6}$$

where $P_{average}$ is the average power and T_{time} is the unit time.

V. Experimental Set-up

In this section, we comparatively analyse SIDS and AIDS in particular with detection accuracy, false positive rates, resource consumption (power, CPU utilisation, and energy), and ease of deployment and management.

A. Dataset – CIC IOT

The CIC IoT dataset [18], from the Canadian Institute for Cybersecurity, focuses on tackling security issues relating to IoT networks and devices. The dataset includes both legitimate and fraudulent IoT network traffic, making it useful for assessing and enhancing cybersecurity and intrusion detection systems specifically designed for IoT contexts. The CIC IoT dataset is used to analyse and develop strong security solutions to safeguard IoT systems from emerging cyber threats.

There are 382931 records in the dataset that include attributes such as flow_duration, Rate, ack_count, syn_count, and others. Distributed Denial of Service (DDoS) attacks like DDoS_ICMP_Flood, DDoS_UDP_Flood, a botnet (malware) Mirai_udpplain, SQL injection, Cross Site Scripting (XSS), etc. are some of the attacks that are included in the dataset. Figure 1 represents how attacks are distributed throughout the dataset.

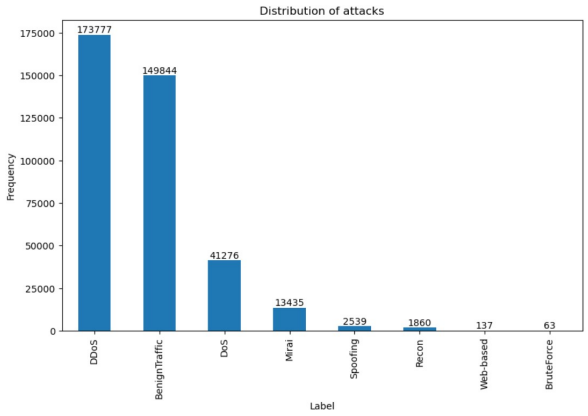

Fig. 1. Distribution of attacks in the dataset

B. Infrastructure

In this section, we discuss the experimental set-up for running the IDS in IoT devices (Raspberry Pi), including the source meter for power measurement. A visual representation of the experimental arrangement is outlined in Figure 2.

The Raspberry Pi 4 is a flexible and powerful single-board computer with enhanced functionality. The platform contains the ARM-based 2-core CPU 1.5GHz, and a 16 GB SD card, running on the Raspbian operating system. We deploy the SIDS by configuring the rules and AIDS modeled using Machine Learning algorithms within the Raspberry Pi device.

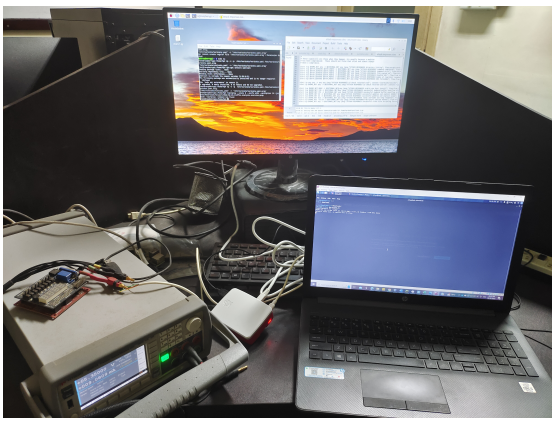

Fig. 2. Experimental Set-up

In the case of AIDS, the ML model is trained with the dataset and the IDS detects alerts for the particular attacks specified based on the test data. Random Forest Classifier and Light Gradient Boosting Machine (LGBM) Classifier are the decision-tree algorithms used to create the model.

Random forest is an ensemble learning technique that uses multiple decision trees to produce more accurate predictions than individual models. It provides information about feature importance, helps identify influential features, and can detect anomalies in unexpected or extreme values [19]. LGBM is a gradient boosting framework designed for efficient training of large datasets. It can learn complex patterns and is useful

for anomaly detection by setting a threshold for instances deviating significantly from expected patterns.

Classifiers were chosen for their ability to handle large datasets and feature sets, reducing overfitting risk through decision tree averaging, and their strong performance in high-dimensional data.

In the case of SIDS, the dataset is employed to configure rules or signatures. We create dependable rules for identifying attack signatures by utilizing features derived from ML algorithms [19]. The IDS analyzes network packets and detects a correlation between signatures and attack patterns, generating an alert accordingly.

Power Measurement:

We utilize a Keithley's series 2461 Source Measure Unit (SMU) [8] to measure the power consumption of the Raspberry Pi boards. Merging the source and measurement circuits into a single device, SMU enables rapid and accurate power consumption measurements. The Raspberry Pi devices are connected to the SMU, which logs the power consumed by the devices at predetermined intervals. Using this utility, we will be able to measure power in real time.

VI. Energy and Performance Analysis

In this section, we provide an analysis of energy consumption, CPU utilization, and performance incurred as a result of IDS running on the IoT platform. Our experiment consists of Raspberry Pi as the IoT device, and the SIDS (Suricata and Snort) and AIDS, using two ML decision tree algorithms (Random Forest and LGBM).

A. Power consumption of IoT

In this subsection, we analyze the power consumed by IoT devices while detecting attacks.

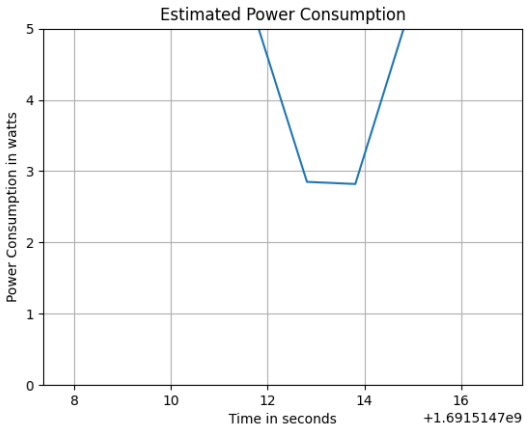

Fig. 3. Power consumption for Signature-Based IDS

Figure 3 shows the power consumed by the SIDS. After conducting network traffic scans for potential attacks, power consumption decreases to a minimal level and remains constant when no new attacks are detected. Notably, the findings demonstrate an elevation in power usage upon the detection of the attacks. This is due to the additional processing demands of the IDS, which are necessary for correlating network traffic with attack signatures.

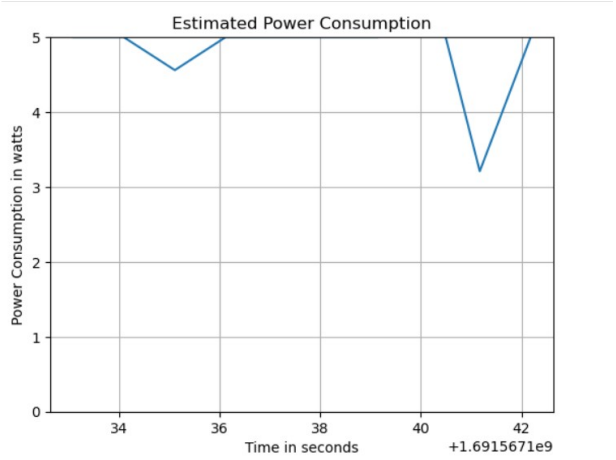

Fig. 4. Power consumption for Anomaly-Based IDS

The power usage of AIDS is depicted in Figure 4. In AIDS, the model is trained over a suitable period of time and is constantly checked for changes in power usage patterns that could indicate security threats or anomalies. The amount of power used will remain constant while training and scanning network packets. The figure visually illustrates the increase in power consumption upon the detection of an attack.

B. CPU consumption of IoT

In the following section, we will analyze the CPU usage of the IoT device during attack detection. Even while the IDS is detecting several attacks, the CPU utilisation for SIDS and AIDS never reaches 100%, demonstrating the IDS's capacity to handle many attacks without being overwhelmed.

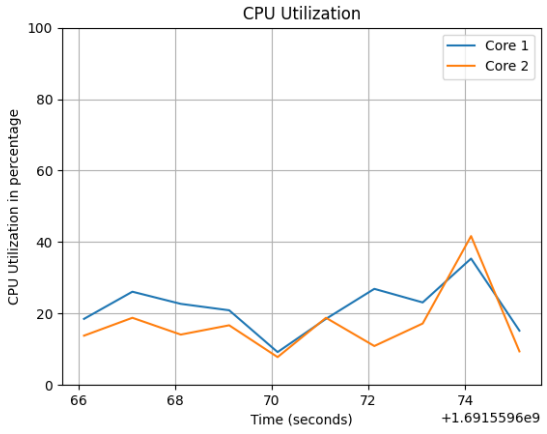

Fig. 5. CPU utilization for Signature-based IDS

The results for the SIDS's CPU use are shown in Figure 5. Results show that the CPU usage of SIDS is relatively high.

ANTS'23 - Women in Engineering (WiE)

With the detection of more attacks, the IDS experiences an increase in CPU usage. This is due to the SIDS's increased processing requirements to compare network traffic against attack signatures. Based on the graph, the average CPU utilization is around 38%, while the average CPU utilization for each core is about 28%. This indicates that around 10% of the entire CPU resources are being used by the SIDS.

Figure 6 shows the CPU usage of AIDS. When an anomaly is found while scanning the network traffic, the IDS launches additional processes to investigate it further. To determine the characteristics and scope of the observed anomaly, the system may examine system logs, network traffic, or other data sources during these computations, which temporarily boost CPU use. The graph shows that the average CPU utilization is around 23%, while the average CPU utilization for each core is about 15%. This indicates that the AIDS utilizes around 8% of the CPU's total resources.

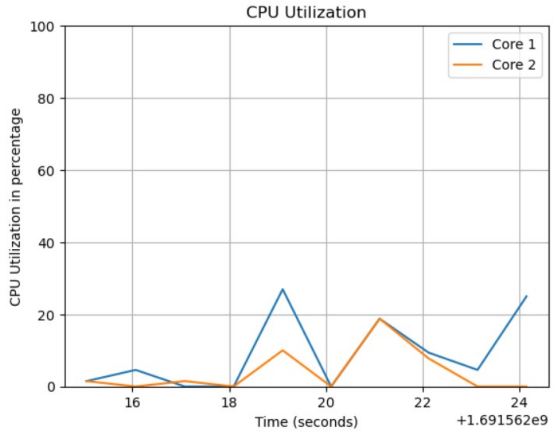

Fig. 6. CPU utilization for Anomaly-based IDS

C. Performance of IoT

In this study, Wireshark is used as an IP traffic monitor application for SIDS to see if IDS does not detect any packets and gather the following statistics. True Positive (TP) = 384525, False Positive (FP) = 35492, True Negative (TN) = 382931, False Negative (FN) = 0.

The SIDS analyzed network traffic packets included in the model and found to have 95.52% better accuracy than 93.2% achieved by AIDS.

D. Comparative Analysis

In this study, we perform a comparative analysis of SIDS and AIDS, using the metrics of power consumption, CPU utilization, and accuracy of detecting the attacks. The analysis is summarized in Table 1.

The study reveals that AIDS uses more power than SIDS due to machine learning algorithms, specifically Random Forest and LGBM, which increase precision and dependability in forecasting. However, these algorithms can be computationally intensive, consuming more power during training and retraining processes. SIDS, on the other hand, is more efficient and potentially consumes less power.

Metrics	Signature-based IDS	Anomaly-based IDS
Power consumption	2.8 watts	3.2 watts
CPU utilization	10%	8%
Accuracy	95.52%	93.2%
Precision	91.55%	90.1 %
Recall	100%	88.7 %
F1 Score	95.59%	85.2 %

TABLE I
COMPARATIVE ANALYSIS

Higher CPU utilization was observed in the case of SIDS, primarily driven by the requirement to manage a substantial repository of attack signatures and to execute supplementary processing for comparing network traffic against these signatures. In contrast, AIDS generally exhibits lower CPU usage, as it doesn't necessitate the maintenance of an extensive attack signature database and can identify network traffic anomalies with reduced computational demands.

Evaluated in terms of performance based on the accuracy, precision, recall, and F1 score, SIDS performs at a higher rate than AIDS. And this may vary based on the algorithms chosen by the organisation to deploy the IDS.

VII. DISCUSSION

In this research, we conducted a concise comparative analysis of two IDS variants. While our emphasis is on a select set of metrics, this investigation lays the foundation for analyzing additional forms of IDS, such as specification-based IDS [3] and Hybrid IDS [2], through the incorporation of additional performance evaluation measures, encompassing detection latency, storage and I/O consumption. The performance of AIDS may vary depending on the algorithm we choose. An organisation may choose which IDS type to use in their IoT settings based on these variables.

While the study primarily centers around conducting a comparative analysis of energy-performance trade-offs, this investigation can serve as an outline for further research to devise an energy-efficient IDS model suitable for implementation within organizations. This, in turn, could enhance the effectiveness of IDS in their IoT devices.

The significant concern is that, IDS on Raspberry Pi (IoT) devices may increase packet drops without inspection due to increased processing power and increased susceptibility to overheating due to the device's large processing power.

VIII. CONCLUSION

In this work, by comparative analysis we profiled the CPU and energy consumption of both SIDS and AIDS. We specifically set up the IDS platforms for the Internet of Things made up of embedded hardware like Raspberry Pi. Analyzing the resource utilization of the IDS, based on the performance, power consumption and CPU utilization of the IoT device was done while running the IDS. Our analysis revealed that

based on power or energy consumption and performance level, SIDS performs better than AIDS. Whereas considering CPU utilization, the anomaly IDS can be leveraged. By deploying a distributed IDS architecture on multiple IoT devices, where the workload is distributed, and devices cooperate to enhance threat detection efficiency, it is possible to markedly decrease power consumption, resulting in a more energy-efficient IDS solution. Our study will help organizations make informed decisions about selecting and deploying the most appropriate IDS for their IoT environments. The results from the study can be used for developing and modeling energy-efficient IDS, thereby develop better-performing IDS in IoT devices.

IX. Acknowledgment

Nithya Nedungadi would like to acknowledge the support from the Ministry of Electronics and Information Technology (MeitY), Government of India, under the Visvesvaraya PhD Scheme for Electronics and IT. We also acknowledge Dr. Swapna MP of our center for her invaluable assistance and support in enhancing our understanding of the content.

References

[1] T. Sommestada, H. Holma, and D. Steinvall, "Influencing the effectiveness of signature-based network intrusion detection systems," *Information security journal: a global perspective*, 2022.

[2] A. Heidari and M. A. J. Jamali, "Internet of things intrusion detection systems: a comprehensive review and future directions," *Cluster Computing*, 2022.

[3] H.-Y. Kwon, T. Kim, and M.-K. Lee, "Advanced intrusion detection combining signature-based and behavior-based detection methods," *Electronics*, 2022.

[4] T. Saba, A. Rehman, T. Sadad, H. Kolivand, and S. A. Bahaj, "Anomaly-based intrusion detection system for iot networks through deep learning model," *Computers and Electrical Engineering*, 2022.

[5] S. Rubin, S. Jha, and B. Miller, "Automatic generation and analysis of nids attacks," in *Proceedings - Annual Computer Security Applications Conference*, 2004.

[6] A. A. Acharya, K. Arpitha, and B. S. Kumar, "An intrusion detection system against udp flood attack and ping of death attack (ddos) in manet," *International Journal of Engineering and Technology (IJET)*, vol. 8, no. 2, 2016.

[7] Q. Hu, S.-Y. Yu, and M. Asghar, "Analysing performance issues of open-source intrusion detection systems in high-speed networks," *Journal of Information Security and Applications*, 2020.

[8] "Keithley 2400 sourcemeter." http://www.tek.com/keithley-sourcemeter-units/keithley-smu-2400-series-sourcemeter.

[9] M. Migliardi and A. Merlo, "Energy consumption simulation of different distributed intrusion detection approaches," in *27th International Conference on Advanced Information Networking and Applications Workshops*, 2013.

[10] K. Nimmy, M. Dilraj, S. Sankaran, and K. Achuthan, "Leveraging power consumption for anomaly detection on iot devices in smart homes," *Journal of Ambient Intelligence and Humanized Computing*, 2022.

[11] A. A. E. Boukebous, M. I. Fettache, G. Bendiab, and S. Shiaeles, "A comparative analysis of snort 3 and suricata," in *2023 IEEE IAS Global Conference on Emerging Technologies*, 2023.

[12] R. Ramachandran, P. Arya, and P. Jayanthy, "A novel method for intrusion detection in relational databases," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017.

[13] J. Rohit, M. V. Sunku, and S. Sriram, "Machine learning–based approach for detecting beacon forgeries in wi-fi networks," in *Artificial Intelligence and Deep Learning for Computer Network*, pp. 13–33, 2023.

[14] O. Abiodun, E. Abiodun, M. Alawida, R. Alkhawaldeh, and H. Arshad, "A review on the security of the internet of things: challenges and solutions," *Wireless Pers. Commun.*, 2021.

[15] D. Fadhilah and M. I. Marzuki, "Performance analysis of ids snort and ids suricata with many-core processor in virtual machines against dos/ddos attacks," in *2nd International Conference on Broadband Communications, Wireless Sensors and Powering (BCWSP)*, 2020.

[16] R. Vinayakumar, K. Soman, and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pp. 1222–1228, IEEE, 2017.

[17] K. Pearson, "On the theory of contingency and its relation to association and normal correlation," 1904.

[18] "Cic iot dataset 2023." https://www.unb.ca/cic/datasets/iotdataset-2023.html.

[19] T. Varunram, M. Shivaprasad, K. Aishwarya, A. Balraj, S. Savish, and S. Ullas, "Analysis of different dimensionality reduction techniques and machine learning algorithms for an intrusion detection system," in *2021 IEEE 6th International Conference on Computing, Communication and Automation (ICCCA)*, pp. 237–242, IEEE, 2021.