

Comparative Analysis of Machine Learning Techniques for DDoS Intrusion Detection in IoT Environments

Godwin Chukwukelu¹^a, Aniekan Essien²^b, Adewale Imram Salami³ and Esther Utuk⁴

¹*IT Services Department, Forctix Ltd, London, U.K.*

²*Operations and Management Science, Healthcare & Innovation Group, University of Bristol, Bristol, U.K.*

³*Department of Computer Science, Leadcity University, Ibadan, Nigeria*

⁴*University of East Anglia, Norwich, U.K.*

Keywords: Intrusion Detection System (IDS), Distributed Denial of Service (DDoS), Internet of Things (IoT), Machine Learning Algorithms.

Abstract: This study addresses the challenge of Distributed Denial of Service (DDoS) attacks in the Internet of Things (IoT) environment by evaluating the effectiveness of Intrusion Detection Systems (IDS) using machine learning techniques. Due to the lightweight computational configuration of IoT systems, there is a need for a classifier that can efficiently distinguish between legitimate and malicious network traffic without demanding substantial computational resources. This research presents a comparative analysis of four machine learning models: (i) k-Nearest Neighbour (k-NN), (ii) Support Vector Machine (SVM), (iii) Random Forest (RF), and (iv) Multilayer Perceptron (MLP), to propose a lightweight DDoS intrusion detection classifier. A novel classification model based on the MLP architecture is proposed, focusing on minimalistic design and feature reduction to achieve accurate and efficient classification. The model is tested using the CICIDS2017 dataset and demonstrates high accuracy and computational efficiency, making it a viable solution for IoT environments where computational resources are limited. The findings show that the proposed μ ML-IDS model achieves an accuracy of 99.8%, F-score of 96.5%, and precision of 99.96%, with minimal computational overhead, highlighting its potential for real-world application in protecting IoT networks against DDoS attacks.


1 INTRODUCTION


The advent of the Internet of Things (IoT) has transformed everyday objects into interconnected smart devices, creating a network of over 20 billion devices globally ((Al-Hadhrami & Hussain, 2021). This rapid proliferation, fuelled by advancements in IP addressing and affordable microcontrollers, has not only enhanced connectivity but also exposed these devices to diverse cyber threats, notably Distributed Denial of Service (DDoS) attacks (Salim et al., 2020). The impact of such attacks can be catastrophic, especially when targeting critical national infrastructures like healthcare systems, where a cyberattack can lead to devastating consequences, including loss of life (Willing et al., 2021). Besides critical infrastructures, common IoT

devices, such as smart bulbs, doors, and TVs are also vulnerable, posing risks of financial loss, privacy breach, and data theft (Verma & Ranga, 2020).

Given these emerging threats, this research is driven by the need to reinforce the security of IoT networks. The study focuses on understanding the role and effectiveness of Intrusion Detection Systems (IDS) in safeguarding IoT-connected devices (MR et al., 2021). It aims to devise solutions for the prevention of DDoS attacks on these networks and contribute to the limited literature regarding IDS's role in IoT security.

The key contributions of this study are centered around the development and comparative analysis of machine learning models to address the challenge of detecting Distributed Denial of Service (DDoS) attacks in Internet of Things (IoT) networks (Sharafaldin et al.,

^a <https://orcid.org/0000-0003-2489-7767>

^b <https://orcid.org/0000-0001-9501-0647>

2019). The primary contribution is the proposition of a novel, lightweight, high-accuracy, and high-precision classifier, termed the $\mu ML-IDS$ model. This model stands out for its minimal computational demands, addressing a significant limitation prevalent in existing data-driven DDoS intrusion detection systems.

In addition, we meticulously perform a comprehensive analysis that navigates the trade-off between model complexity and accuracy, a crucial consideration for IoT networks operating on edge or fog computing infrastructures (Butun et al., 2013; Vinayakumar et al., 2019). The emphasis is placed on developing classifiers that are computationally lightweight yet effective. The $\mu ML-IDS$ model achieves this balance by employing a robust feature selection approach, data normalization, and efficient model training processes. These techniques ensure accurate classification of DDoS attacks while distinguishing them from legitimate network traffic.

A significant aspect of this research is the comprehensive comparative analysis performed across various benchmark models. This analysis demonstrates that the $\mu ML-IDS$ model surpasses others in terms of accuracy and F-score. Additionally, the study encompasses a thorough review of existing and proposed intrusion detection systems for IoT networks. This review highlights the current limitations and opens avenues for future research in this niche field.

The remainder of this study unfolds as follows: The literature review in Section 2 provides a deep-dive into the Internet of Things (IoT), Intrusion Detection Systems (IDSs), and Distributed Denial of Service (DDoS) in IoT, including a discussion on various DDoS detection methods and the role of machine learning. Section 3 outlines the research methodology, detailing the development of $\mu ML-IDS$, a lightweight machine-learning IDS, and covers aspects from dataset pre-processing to evaluation methods. Section 4 presents the core findings, including a comprehensive comparative analysis of several machine learning models for DDoS detection in IoT networks, with a focus on model performance evaluation and experimental results. Finally, the closing chapter discusses implications, limitations and future research.

2 THEORETICAL BACKGROUND

2.1 Internet of Things (IoT)

The Internet of Things (IoT) represents a

transformative evolution in internet technology, characterized by an extensive network of interconnected devices (Roopak et al., 2020). Khujamatov et al. (2021) define IoT as a network of physical objects equipped with technology for communication within themselves and with the external environment, impacting economic and social systems. These interconnected devices, or 'things,' encompass a wide range of applications from home automation to industrial and environmental monitoring (Firouzi et al., 2020; Zarpelão et al., 2017). IoT's expansion also includes the Industrial Internet of Things (IIoT), which integrates traditional industrial control networks with IoT technologies (K. Yu et al., 2021). Figure 1 depicts a graphical representation of the architecture of IoT devices.

The rapid growth of IoT has significant implications for cybersecurity. The diversity of IoT devices, each with unique data, hardware, software configurations, and communication protocols, poses a substantial challenge to information safety and security (Roopak et al., 2020). Kumar & Kumar (2023) highlight the heightened susceptibility of these networks to cyber threats, particularly Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. These attacks not only disrupt essential services but can also lead to significant financial loss, privacy breaches, and in severe cases, loss of life (Verma & Ranga, 2020). The increasing number of cybercrimes, as evidenced by attacks on healthcare systems and other critical infrastructures, underscores the urgent need for robust cybersecurity measures in the IoT domain (Willing et al., 2021).



Figure 1: IoT architecture.

As IoT continues to evolve, enhancing its security becomes paramount. The integration of IoT into daily life and its application across various sectors necessitates a rigorous focus on safeguarding these

systems against cyber threats. This is critical for maintaining the integrity and reliability of IoT networks and for ensuring the safety and privacy of users and businesses reliant on this technology.

2.2 Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) play a crucial role in network security, monitoring and analysing events to detect intrusions that threaten the confidentiality, integrity, or availability of computer systems or networks (Bace & Mell, 2001). These systems, both software and hardware, are categorized into Passive IDS, which monitor and alert administrators of changes, and Active IDS, which also block suspicious traffic (Saranya et al., 2020). The evolution of IDS began with Jim Anderson in 1980, leading to various products developed to meet growing security demands (Ahmad et al., 2021).

IDS deployment can be either Host-based, focusing on individual hosts, or Network-based, protecting entire networks. Detection techniques fall into three categories: Signature-based IDS (SIDS), which compare data patterns against a database of attack signatures; Anomaly-based IDS (AIDS), defining a typical activity profile and flagging deviations as anomalies (Latif et al., 2020); and Hybrid-based IDS, combining the features of SIDS and AIDS.

Incorporating Artificial Intelligence (AI) into IDS design, particularly Machine Learning (ML) and Deep Learning (DL), has become prevalent. ML algorithms in IDS are designed to discover hidden patterns in data, enhancing the accuracy and timeliness of attack detection (Ahmad et al., 2021; Parveen Sultana et al., 2019). This approach is increasingly important due to the large volume and velocity of network data, which standard detection systems struggle to process effectively. The incorporation of AI in IDS represents a significant advancement in network security, addressing the evolving challenges in detecting and preventing cyber threats efficiently.

2.3 Distributed Denial of Service (DDoS) in IoT

DDoS attacks in IoT environments represent a significant escalation from traditional DoS attacks, characterized by the overwhelming of networks or servers through excessive data flooding, rendering them inaccessible to legitimate traffic (Vishwakarma & Jain, 2020). These attacks, often distributed across geographically spread devices, result in substantial

operational disruptions, financial losses, and potentially life-threatening situations (Al-Hadhrami & Hussain, 2021; Snehi & Bhandari, 2021). The sophistication and frequency of DDoS attacks have increased, posing a challenge to even advanced IDSs that employ machine learning techniques (Roopak et al., 2020). The nature of these attacks has evolved from targeting network and transport layers to the more stealthy and damaging application-layer attacks (Salim et al., 2020).

The rise of IoT devices has unfortunately expanded the attack surface for DDoS attacks. Attackers exploit vulnerabilities in software and hardware, using IoT devices to build botnets capable of generating significant DDoS traffic (Cvitić et al., 2021). DDoS attacks have been categorized into traditional and IoT-based attacks, the latter utilizing low-security IoT devices to form botnets (Snehi & Bhandari, 2021; Susilo & Sari, 2020). The significant increase in DDoS attack volumes over recent years highlights the urgent need for effective detection and prevention strategies (Gaur & Kumar, 2022).

2.4 DDoS Detection Methods

DDoS attack detection focuses on distinguishing between legitimate and malicious network traffic. Efficient detection systems are especially crucial for IoT networks, where attacks can severely compromise network security (Schulter et al., 2006). These detection methods are generally categorized into anomaly-based, hybrid, and signature-based systems. Anomaly-based IDS monitor network activity against a defined normal behaviour, alerting administrators of significant deviations (Khraisat et al., 2019; Vinayakumar et al., 2019). Hybrid IDS combine the strengths of anomaly and signature-based systems, offering broad detection capabilities (Fenil & Mohan Kumar, 2020). Signature-based IDS rely on a database of known attack patterns, comparing incoming traffic against these signatures to identify threats. Despite their ease of deployment, they struggle against novel attacks and require continuous database updates to remain effective.

2.5 Machine Learning for DDoS Intrusion Detection in IoT Networks

The design of Intrusion Detection Systems (IDS) for IoT platforms often relies on analysing network patterns, typically evaluated using standard datasets, such as KDDCUP, NSL-KDD, UNSW-NB15, and CSE-CIC-IDS18 (Kiran et al., 2020). However, there

is a gap in research presenting solutions based on data pattern analysis for attack identification, underscoring the necessity of developing a framework for detecting threats in IoT environments using data patterns derived from IoT networks.

Machine Learning (ML) and Deep Learning (DL) are pivotal in enhancing the efficacy of IDS in IoT networks. These techniques utilize both labelled and unlabelled data, employing algorithms including randomised K-Means clustering to enhance classifier diversity and achieve reliable intrusion detection. This approach is essential given the complex nature of DDoS attacks, which can render devices and networks inoperable, resulting in significant financial and data losses, and in severe cases, endangering lives.

The rise in sophisticated DDoS attacks challenges even the most advanced ML-based IDS, highlighting the need for innovative solutions in this domain (Roopak et al., 2020). The integration of ML in IDS must therefore be strategic, considering both the complexity of the IoT environment and the nature of DDoS attacks. This need drives the ongoing research and development in IDS using ML and DL techniques, aiming to create more robust and effective defence mechanisms against DDoS attacks in IoT networks.

3 METHODOLOGY DESIGN

3.1 μ ML-IDS: A Lightweight Machine-Learning IDS for DDoS Detection in IoT Networks

This study introduces μ ML-IDS, a machine-learning-based Intrusion Detection System (IDS) focused on detecting Distributed Denial of Service (DDoS) attacks in IoT networks. The approach employed in this research involves meticulous data wrangling, cleaning, and preprocessing, underscoring the necessity for detailed data analysis in developing effective IDS solutions (Doriguzzi-Corin et al., 2020). Recognizing the shortcomings in current literature, which primarily emphasizes detection rates and model accuracy without adequate consideration for computational requirements, μ ML-IDS is designed as a computationally lightweight model. This design decision not only enhances the model accuracy but also ensures that it is well-suited for environments with limited computing resources, a common scenario in IoT networks.

μ ML-IDS stands out for its ability to process and classify data rapidly, implementing detection in milliseconds, thus aligning with the needs of IoT networks for real-time intrusion detection. The system's architecture is optimized for deployment in computational environments typical of IoT devices, where resource minimization is crucial. Figure 2 presents the graphical representation of the proposed methodology for μ ML-IDS.

3.2 Model Development and Methodology

The development of the IDS classifier in this study entailed a meticulous process of data preparation and model training. Initially, the dataset underwent cleaning to remove null and infinite values, reducing the dataset to 225,711 records. Subsequently, a manual feature reduction was conducted to eliminate redundant features, ensuring that only the most relevant variables were used for model training, leaving 77 features in the final dataset.

The dataset was then normalized to a range of 0 to 1 to mitigate the impact of scale variations on the machine learning models. Following normalization, the dataset was split into training and testing sets using a 70:30 train-test ratio, a standard practice in data analytics. Each of the four machine learning models was trained on the same training dataset and evaluated on the testing dataset to maintain consistency and fairness in the evaluation process. This approach ensured that the models were developed and assessed under comparable conditions.

3.3 Experimental Setup

The experimental setup for this study was conducted on a Windows computer equipped with an Intel Core i7 processor (3.6GHz Quad-core), 1TB of hard disk storage, and 32GB of RAM, running Windows 11. The experiments utilized Python v3.6 and scikit-learn v1.0.2, ensuring a robust computational environment for machine learning analysis. This setup was essential for handling extensive datasets like the NSL-KDD, which features over 22,000 data entries and 43 independent features, and the CICIDS2017 labelled dataset, deemed most suitable for this study. The CICIDS2017 dataset, designed by the University of New Brunswick Institute for Cybersecurity, includes up-to-date data closely resembling real-world network attack scenarios. This comprehensive dataset includes a wide range of network attack types, providing a realistic and challenging environment for

testing and evaluating the machine learning models developed in this research.

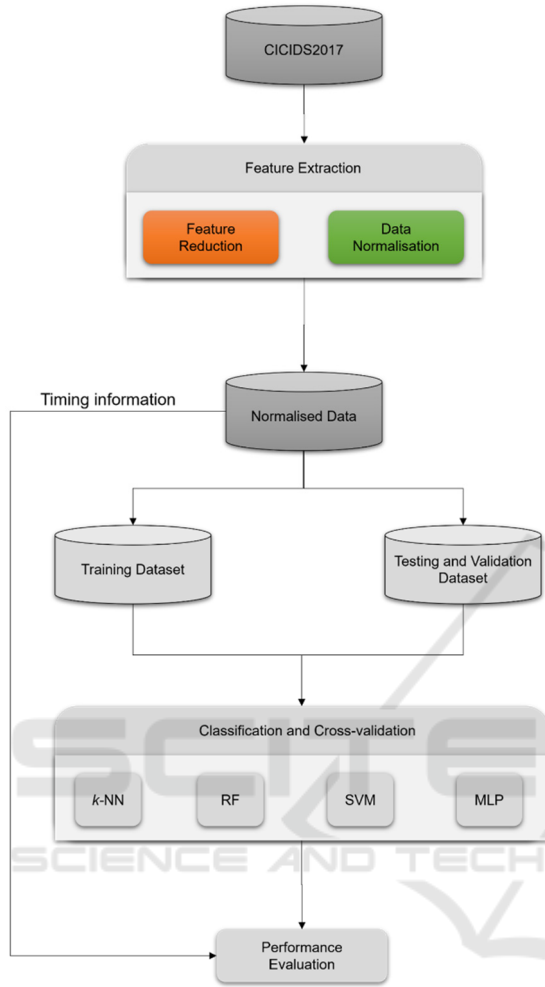


Figure 2: Methodology for the proposed IDS.

3.4 Evaluation Methods and Measures

The performance of machine learning models in intrusion detection is a binary classification task that can be assessed using various metrics. A confusion matrix is typically employed for visual discriminative evaluation, plotting predicted classes against actual classes and distinguishing true positives, true negatives, false positives, and false negatives (Figure 3). The evaluation metrics used include:

1. **Accuracy:** the ratio of true classifications to total predictions, defined by Equation (1) below:

$$\frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

2. **Recall:** otherwise referred to as the true positive rate, and the ratio of correct classifications made

to the sum of correct classifications and wrongly classified negatives. Equation (2) below is used to compute recall:

$$\frac{TP}{TP + FN} \quad (2)$$

3. **Precision:** the ratio of correct classifications to positive classifications, calculated by the following equation (3):

$$\frac{TP}{TP + FP} \quad (3)$$

4. **F-Measure:** harmonic mean of recall and precision, calculated using Equation (4).

$$2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (4)$$

These metrics provide a comprehensive view of model performance, addressing limitations such as the inability of accuracy to penalize false negatives, crucial in intrusion detection systems (IDS). The study aligns with literature advocating for balanced metrics like the F-measure and geometric mean, more suited for discriminating false classifications.

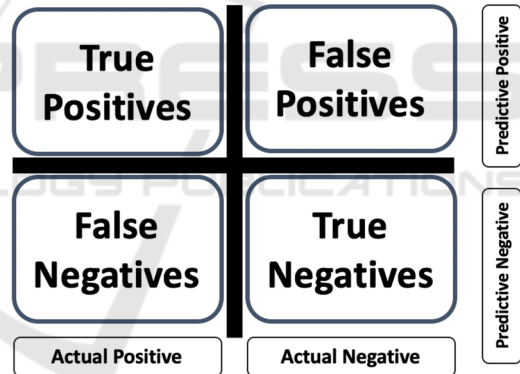


Figure 3: Confusion matrix for binary classification.

3.5 Data Description

Acquiring datasets for data-driven intrusion detection system (IDS) modelling poses significant challenges, often due to privacy and security concerns (Tavallaee et al., 2009). Network traffic data, rich in sensitive information, necessitates careful handling to avoid unauthorized access and potential exposure of confidential data about customers, suppliers, and business communications. To circumvent these issues, researchers frequently resort to simulated data. Nevertheless, there are notable datasets like KDDCUP'99 and NSL-KDD extensively used in intrusion detection research. This study specifically utilizes the CICIDS2017 dataset, selected for its up-

to-date representation of real-world network attack scenarios. The CICIDS2017 dataset, developed by the University of New Brunswick, addresses the shortcomings of previous datasets, such as outdated or unreliable data, lack of diversity, and issues with data monotonicity. Unlike KDD-99, known for its low detection rates and high false positives, the NSL-KDD dataset is extensive, lacks repetitive values, and has no null or empty values, making it advantageous for machine learning preprocessing. The CICIDS2017 dataset is deemed most appropriate for this study due to its relevance and comprehensive coverage of contemporary network attack patterns. Table 1 presents a summary of the data used in this study.

Table 1: CICIDS2017 Data Overview.

Day	Flow	Total Attacks	Description
Monday	529,918	0	Normal
Tuesday	445,909	7,938	FTP-Patator
		5,897	SSH-Patator
Wed.	692,703	5,796	DoS slowloris
		5,499	DoS slowhttptest
		231,073	DoS Hulk
		10,293	DoS GoldenEye
		11	HeartBleed
Thursday AM	170,366	1,507	Web Attack - Brute Force
		652	Web Attack - XSS
		21	Web Attack - SQL Injection
Thursday PM	288,602	36	Infiltration
Friday AM	191,033	1,966	Bot
Friday PM1	286,467	158,930	Portscan
Friday PM2	225,745	128,027	DDoS
Total	2,830,743	557,646	19.70% attack

4 A LIGHTWEIGHT MACHINE LEARNING IDS FOR IOT NETWORKS

This section introduces a novel, computationally lightweight machine learning model for IDS in IoT networks, focusing on detection accuracy while minimizing computational demands. The μ ML-IDS model addresses limitations in existing models by offering high precision DDoS attack detection with

minimal resource use, proving highly efficient in environments with limited computing power.

4.1 Candidate Machine Learning Models

We discuss the significance of machine learning (ML) algorithms in information security, specifically for detecting network anomalies and DDoS attacks. Given the complexity of selecting an optimal classifier for intrusion detection due to varying computational costs and scenarios, the study evaluates several supervised learning models: Multilayer Perceptron (MLP), Random Forest (RF), k-Nearest Neighbour (k-NN), and Support Vector Machine (SVM). It outlines the existence of seventeen ML classifier families, emphasizing that no single classifier excels in all situations, as supported by the No Free Lunch (NFL) theory (Wolpert & Macready, 1997). This leads to the selection of four classifiers (k-NN, RF, SVM, MLP) based on their generalization abilities across different datasets, aiming to develop a computationally efficient solution for DDoS attack detection in network traffic flows.

4.2 Experimental Results

The experiments in this study were conducted on a Windows 11 PC with an Intel Core i7 3.6GHz Quad-core, 1TB HDD, and 32GB RAM, using Python 3.6 and Scikit-learn 1.0.2. This subsection outlines the experimental setup and evaluates the performance of chosen machine learning classifiers.

4.2.1 Model Comparative Evaluation

The comparative analysis involved applying models to a uniform dataset, as detailed in Section 3.2. Results and confusion matrices for the evaluated models are summarized in Table 2 and Figure 4, respectively.

Table 2: Summary of model performance.

S/N	Model	Train time (s)	Pred time (s)	Recall (%)	F-score (%)	Precision (%)
1.	k-NN	0.24	143.62	56.1	71.81	99.90
2.	RF	14.09	0.30	55.5	71.40	99.93
3.	SVM	41.08	33.03	54.9	70.92	100
4.	MLP	74.68	0.34	93.3	96.54	99.98

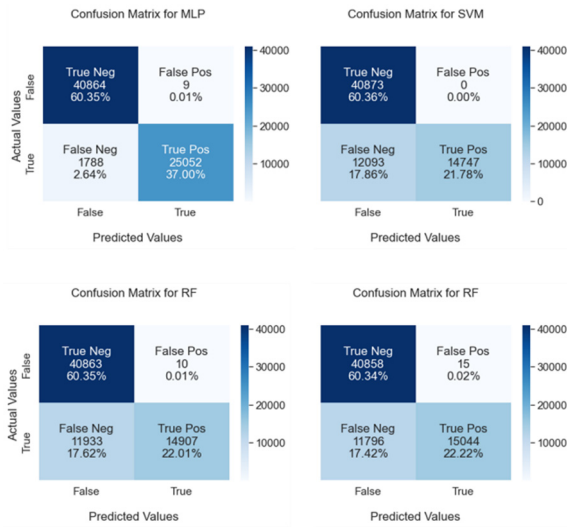


Figure 4: Confusion matrix for benchmark models.

Table 2 highlights the varying advantages and drawbacks of the various models, making it challenging to choose the best one based solely on the table. For instance, while SVM had the highest precision at 100%, it also had a significant number of false positives (Figure 4). The k-NN model was fastest in training but slow in inference, and RF had the quickest inference time but sub-optimal false positive rates (Figure 5). The MLP model emerged as the most balanced, offering low inference time, high precision (99.96%), and the best f-measure (96.54%), indicating its efficiency in DDoS attack detection with the lowest false alarm rate (Figure 6). Training and inference time analysis showed a trade-off between model complexity and performance, highlighting the importance of inference time for real-time applications. Ultimately, the MLP model was chosen as the best overall due to its optimal performance across all metrics, making it suitable for real-time network environments as a lightweight and efficient solution for classifying normal and DDoS attack traffic.

4.3 Comparison Against Related Studies

The proposed μ ML-IDS model showcased optimal accuracy and computational efficiency on test data, outperforming other models in training and inference times. This section compares μ ML-IDS with models from related studies, highlighting its competitive edge, particularly in computational requirements crucial for IoT network security. As can be seen from Table 3, a comparative analysis affirms the competitive performance of μ ML-IDS in both

accuracy and efficiency, underscoring its significance for IoT security. Despite this performance, the key gain of our proposed model is its significantly lower computational requirement evidenced by the low training and inference time.

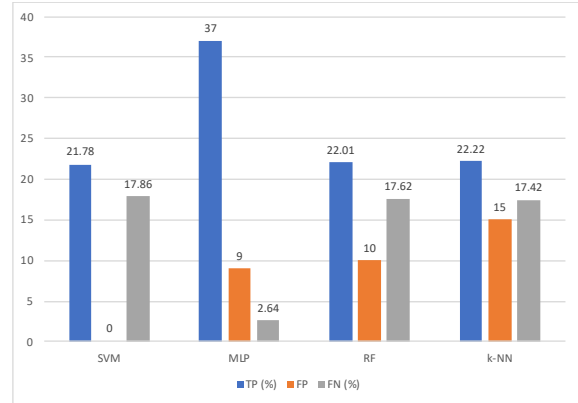


Figure 5: Performance evaluation metrics for benchmark models.

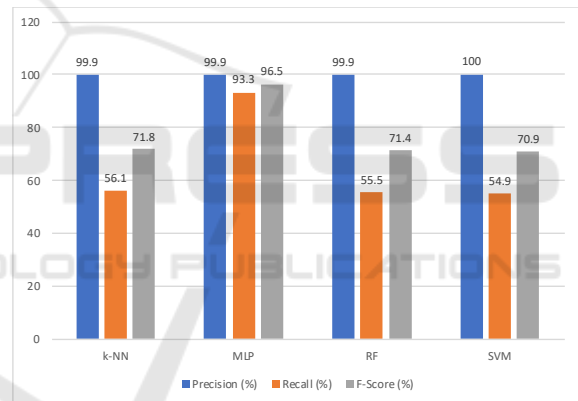


Figure 6: Precision and F-score for benchmark models.

5 CONCLUSION

The Internet of Things (IoT) permeates daily life, enhancing connectivity but presenting security challenges due to its complexity and vulnerability to attacks, as highlighted by incidents like WikiLeaks and the Dyn attack. IoT security has become a critical research area, with a focus on developing effective Intrusion Detection Systems (IDS) to combat these vulnerabilities (Bout et al., 2021). This study aimed to analyze and compare DDoS IDS for IoT networks, seeking an optimal model that is efficient, generalizable, and minimally demanding on computing resources. It addresses the urgent need to counteract DDoS threats to ensure network stability,

Table 3: Comparison of proposed model to related studies.

Source	No. of features	Model	Acc (%)	Prec (%)	F-score (%)
(J. Yu et al., 2008)	13	SVM	99.53	97.07	-
(Barati et al., 2014)	5	MLP	99.98	100	99.93
(Diro & Chilamkurti, 2018)	123	Deep learning	98.27	99.36	99.26
(Muralidharan & Janet, 2021)	80	Deep learning	99.89	100	99.96
This study	77	MLP	99.73	99.97	96.54

proposing a lightweight, high-accuracy classifier as a solution to enhance IoT security. The chapter concludes with a discussion on the study contributions, limitations, and avenues for future research.

5.1 Contributions

This study presents a significant contribution by presenting a comparative analysis of machine learning models, leading to the development of the μ ML-IDS model, a high-accuracy, precision classifier designed for efficient DDoS attack detection in IoT networks. This model addresses the challenge of balancing accuracy and computational demand, proving to be effective while requiring minimal resources, suitable for edge/fog computing environments. It employs a strategic approach combining robust feature selection, data normalization, and model training, outperforming benchmark models in accuracy, F-score, and precision with minimal processing time. Additionally, the study provides a thorough review of existing IDS for IoT, highlighting limitations and future research directions, and utilizes the CICIDS2017 dataset for a detailed evaluation, showcasing the model's exceptional performance with 99.8% accuracy, 96.5% F-score, 99.96% precision, and quick processing times.

5.2 Limitations and Future Research

Although we present a high-accuracy, lightweight model for DDoS attack detection in IoT networks, there are several areas for future exploration. A key future direction involves deploying the model within a real-time network environment for distributed monitoring, enhancing its practical applicability and efficiency. The introduction of an adaptive self-learning mechanism that allows for continuous model improvement with minimal human intervention, leveraging periods of low network activity for training, is also proposed. Although the study focuses on combating DDoS attacks due to their significant impact on IoT infrastructure, it acknowledges the necessity to address other prevalent cyber threats, such as man-in-the-middle, phishing, and DoS attacks, through the development of specialized lightweight models. Lastly, the research underlines the challenge of generalization across diverse IoT systems, suggesting the development of more universally applicable models as an avenue for future research, aiming to broaden the model's applicability to various IoT contexts.

REFERENCES

- Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in IoT-based cloud computing: A comprehensive survey. *Electronics*, 11(1), 16.
- Al-Hadhrani, Y., & Hussain, F. K. (2021). DDoS attacks in IoT networks: a comprehensive systematic literature review. *World Wide Web*, 24(3), 971–1001.
- Bace, R. G., & Mell, P. (2001). *Intrusion detection systems*.
- Barati, M., Abdullah, A., Udzir, N. I., Mahmud, R., & Mustapha, N. (2014). Distributed Denial of Service detection using hybrid machine learning technique. *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, 268–273.
- Bout, E., Loscri, V., & Gallais, A. (2021). How Machine Learning changes the nature of cyberattacks on IoT networks: A survey. *IEEE Communications Surveys & Tutorials*, 24(1), 248–279.
- Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 16(1), 266–282.
- Cvitić, I., Peraković, D., Periša, M., & Gupta, B. (2021). Ensemble machine learning approach for classification of IoT devices in smart home. *International Journal of Machine Learning and Cybernetics*, 12(11), 3179–3202.
- Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems*, 82, 761–768.

- Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J., & Siracusa, D. (2020). LUCID: A practical, lightweight deep learning solution for DDoS attack detection. *IEEE Transactions on Network and Service Management*, 17(2), 876–889.
- Fenil, E., & Mohan Kumar, P. (2020). Survey on DDoS defense mechanisms. *Concurrency and Computation: Practice and Experience*, 32(4), e5114.
- Firouzi, F., Farahani, B., Weinberger, M., DePace, G., & Alike, F. S. (2020). Iot fundamentals: Definitions, architectures, challenges, and promises. In *Intelligent internet of things* (pp. 3–50). Springer.
- Gaur, V., & Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. *Arabian Journal for Science and Engineering*, 47(2), 1353–1374.
- Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2(1), 1–22.
- Khujamatov, H., Reypnazarov, E., Khasanov, D., & Akhmedov, N. (2021). IoT, IIoT, and cyber-physical systems integration. In *Emergence of Cyber Physical System and IoT in Smart Automation and Robotics* (pp. 31–50). Springer.
- Kiran, K. S., Devisetty, R. N. K., Kalyan, N. P., Mukundini, K., & Karthi, R. (2020). Building a intrusion detection system for IoT environment using machine learning techniques. *Procedia Computer Science*, 171, 2372–2379.
- Kumar, D., & Kumar, K. P. (2023). Artificial Intelligence based Cyber Security Threats Identification in Financial Institutions Using Machine Learning Approach. *2023 2nd International Conference for Innovation in Technology (INOCON)*, 1–6.
- Latif, S., Idrees, Z., Zou, Z., & Ahmad, J. (2020). DRaNN: A deep random neural network model for intrusion detection in industrial IoT. *2020 International Conference on UK-China Emerging Technologies (UCET)*, 1–4.
- MR, G. R., Ahmed, C. M., & Mathur, A. (2021). Machine learning for intrusion detection in industrial control systems: challenges and lessons from experimental evaluation. *Cybersecurity*, 4(1), 1–12.
- Muraleedharan, N., & Janet, B. (2021). A deep learning based HTTP slow DoS classification approach using flow data. *ICT Express*, 7(2), 210–214.
- Parveen Sultana, H., Shrivastava, N., Dominic, D. D., Nalini, N., & Balajee, J. M. (2019). Comparison of machine learning algorithms to build optimized network intrusion detection system. *Journal of Computational and Theoretical Nanoscience*, 16(5–6), 2541–2549.
- Roopak, M., Tian, G. Y., & Chambers, J. (2020). An intrusion detection system against ddos attacks in iot networks. *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*, 562–567.
- Salim, M. M., Rathore, S., & Park, J. H. (2020). Distributed denial of service attacks and its defenses in IoT: a survey. *The Journal of Supercomputing*, 76(7), 5320–5363.
- Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance analysis of machine learning algorithms in intrusion detection system: a review. *Procedia Computer Science*, 171, 1251–1260.
- Schulter, A., Reis, J. A., Koch, F., & Westphall, C. B. (2006). A grid-based intrusion detection system. *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, 187.
- Sharafaldin, I., Lashkari, A. H., Hakak, S., & Ghorbani, A. A. (2019). Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy. *2019 International Carnahan Conference on Security Technology (ICCST)*, 1–8.
- Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks. *Computer Science Review*, 40, 100371.
- Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. *Information*, 11(5), 279.
- Tavallae, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*, 1–6.
- Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. *Wireless Personal Communications*, 111(4), 2287–2310.
- Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. *Ieee Access*, 7, 41525–41550.
- Vishwakarma, R., & Jain, A. K. (2020). A survey of DDoS attacking techniques and defence mechanisms in the IoT network. *Telecommunication Systems*, 73(1), 3–25.
- Willing, M., Dresen, C., Gerlitz, E., Haering, M., Smith, M., Binnewies, C., Guess, T., Haverkamp, U., & Schinzel, S. (2021). Behavioral responses to a cyber attack in a hospital environment. *Scientific Reports*, 11(1), 1–15.
- Wolpert, D. H., & Macready, W. G. (1997). No free lunch theorems for optimization. *IEEE Transactions on Evolutionary Computation*. <https://doi.org/10.1109/4235.585893>
- Yu, J., Lee, H., Kim, M.-S., & Park, D. (2008). Traffic flooding attack detection with SNMP MIB using SVM. *Computer Communications*, 31(17), 4212–4219.
- Yu, K., Tan, L., Yang, C., Choo, K.-K. R., Bashir, A. K., Rodrigues, J. J. P. C., & Sato, T. (2021). A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings. *IEEE Internet of Things Journal*.
- Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, 84, 25–37.