SSRG International Journal of Computer Science and Engineering
ISSN: 2348–8387 / https://doi.org/10.14445/23488387/IJCSE-V11I4P102

Volume 11 Issue 4, 10-18, April 2024
© 2024 Seventh Sense Research Group®

Original Article

Enhancing IoT Network Security through Prompt Intrusion Detection Using Machine Learning

Ramineni Padmasree[1], Keerthana Muthyam[2]

[1,2]*Department of ECE, Rajiv Gandhi University of Knowledge and Technologies, Basar, Telangana, India.*

[1]*Corresponding Author : r.padmasree3@gmail.com*

Received: 19 February 2024 Revised: 29 March 2024 Accepted: 16 April 2024 Published: 30 April 2024

Abstract *- This study aims to enhance IoT network security by deploying rapid intrusion detection mechanisms fortified with machine learning techniques. Addressing the escalating security concerns surrounding IoT devices, the research develops effective strategies for swift intrusion identification and mitigation, encompassing various intrusion types such as Distributed Denial of Service (DDoS), Internet Control Message Protocol (ICMP), and Transmission Control Protocol Synchronize (TCP SYN). Leveraging supervised machine learning algorithms such as Support Vector Machines (SVM), Logistic Regression, Random Forest, and K-Nearest Neighbors (KNN), a highly accurate intrusion detection model is proposed. Evaluation of the model's performance, utilizing diverse datasets sourced from platforms like Kaggle, showcases notable accuracy rates across different intrusion types. Specifically, DDOS achieves 82% accuracy, TCP SYN attains 99.96%, and ICMP reaches 99.8% accuracy on average. Notably, Random Forest exhibits the highest accuracy among the tested algorithms. This research significantly contributes to strengthening IoT network security, bolstering overall resilience against malicious activities and unauthorized access.*

Keywords *- DDoS, ICMP, Intrusion detection, IoT Network Security, Machine learning, TCP SYN.*

1. Introduction

An IoT (Internet of Things) device is a physical item equipped with sensors, software, and other elements intended to communicate and exchange Information with other devices or systems via the internet [1]. These devices can collect and transmit data, carry out pre-defined tasks, and interact with their environment or other devices independently or according to programmed instructions. Examples of IoT devices include smart thermostats, wearable fitness trackers, home surveillance cameras, connected household appliances, industrial sensors, and components of smart city infrastructure like intelligent streetlights or traffic monitoring systems.

Defects in IoT devices arising from issues in hardware, software, and network infrastructure pose significant challenges concerning security, reliability, and privacy [2]. Common problems include security vulnerabilities, leaving devices open to hacking and unauthorized access, reliability issues like hardware failures and connectivity disruptions, and interoperability barriers that impede seamless device communication [2]. Privacy concerns arise from insufficient protection of sensitive user data during collection and transmission. Additionally, inadequate update mechanisms and flawed firmware expose devices to security risks, while physical tampering also threatens device security [3]. Addressing these faults requires a comprehensive strategy involving robust security measures, dependable hardware and software design, adherence to interoperability standards, privacy safeguards, regular updates, and defences against physical tampering.

This paper primarily examines security attacks, with a particular emphasis on Distributed Denial of Service (DDoS), Internet Control Message Protocol (ICMP), and Transmission Control Protocol Synchronize (TCP SYN).

DDoS attacks represent a cyberattack method where a multitude of compromised devices, often dispersed across various locations and remotely manipulated, inundate a specific system, service, or network with an excessive traffic load. The goal is to exhaust the resources of the target, rendering it inaccessible to legitimate users. Such attacks disrupt the operations of websites, online services, and network infrastructure, causing significant downtime and financial losses for organizations [4].

ICMP attacks exploit the Internet Control Message Protocol (ICMP), which serves as a diagnostic and control protocol within IP networks. It facilitates the exchange of error messages, network status updates, and routing details among network devices. While typically used by network administrators and diagnostic tools for tasks like ping and traceroute, attackers can misuse ICMP for reconnaissance, denial-of-service attacks, and network scanning.

TCP SYN attacks target the Transmission Control Protocol SYN (TCP SYN), a specific form of network communication used to initiate TCP connections between devices. In such attacks, adversaries flood a target system with numerous TCP SYN requests, aiming to overwhelm its resources and prevent legitimate connections. By manipulating the TCP three-way handshake process, attackers send SYN packets but abandon the handshake, leaving the target system waiting for a response that never arrives. This depletes the target's resources, causing service disruption or denial of service for legitimate users.

Detecting intrusions within IoT networks is critical for identifying and mitigating unauthorized access, malicious activities, and security breaches across interconnected IoT devices and systems [5]. Intrusion detection systems (IDS) continuously monitor network traffic and device behaviors to promptly identify suspicious events, facilitating rapid incident response and mitigation efforts. This proactive approach is vital for protecting sensitive data, maintaining system integrity, complying with regulatory standards, and managing security risks in IoT deployments, ultimately strengthening the security and resilience of IoT environments [6].

Although progress has been made in IoT security research, there remains a significant gap in developing effective IDS tailored specifically for IoT environments. Current IDS solutions often lack the flexibility and scalability required to adequately monitor and protect the diverse and dynamic nature of IoT networks.

This study aims to address this gap by focusing on creating an efficient IDS specifically designed for IoT environments. The primary objective is to develop an IDS that utilizes supervised machine learning algorithms to detect and address TCP-SYN and ICMP attacks, which are prevalent threats to IoT networks.

By filling this research gap, we aim to contribute to enhancing IoT security by providing specialized intrusion detection capabilities for IoT networks. This will assist IoT stakeholders in better safeguarding their networks, mitigating security risks, and ensuring the reliability and integrity of their IoT deployments.

2. Literature Review

The literature on IoT network security highlights the increasing importance of rapid intrusion detection mechanisms powered by machine learning techniques. Researchers have emphasized the vulnerabilities inherent in IoT devices and networks, necessitating proactive measures to mitigate risks and safeguard critical infrastructure. Network Intrusion Detection Systems (NIDS) are pivotal in fortifying networks against diverse cyber threats. With the proliferation of the Internet of Things (IoT) and the interconnection of myriad devices, ensuring the security of these interconnected systems has emerged as a paramount concern. This literature review aims to consolidate recent advancements in real-time NIDS, with a focus on IoT environments.

Al-Fuqaha et al. [7] furnish a comprehensive survey delineating the enabling technologies, protocols, and applications in the IoT landscape. Although not directly addressing intrusion detection, this survey serves as foundational knowledge by spotlighting the multifaceted ecosystem of IoT devices and communication protocols, thereby underlining the imperative need for robust security mechanisms.

Ray and Mohapatra [8] delve into the security challenges inherent in healthcare applications utilizing wireless medical sensor networks. While the primary focus lies within the healthcare domain, this study underscores the significance of real-time intrusion detection in environments where data privacy and integrity are of utmost importance.

Hofstede et al. [9] proffer a framework geared towards real-time intrusion detection for NetFlow and IPFIX, accentuating the criticality of timely detection and response to network threats. The research explores techniques for scrutinizing flow data to identify anomalous behaviour, thus laying the groundwork for real-time detection mechanisms. Their results showcase promising accuracy rates in identifying intrusions in real-time network traffic, providing a solid foundation for further refinement of intrusion detection systems.

Sangkatsanee et al. [10] propose practical real-time intrusion detection employing machine learning approaches, showcasing the efficacy of machine learning algorithms in discerning malicious activities from normal network behaviour. The study underscores the potential of machine learning in achieving real-time detection accuracy, thus enhancing network security. Their results demonstrate notable improvements in detection rates compared to traditional rule-based systems, highlighting the viability of machine learning in enhancing intrusion detection capabilities.

Qiu et al. [11] delve into adversarial attacks against network intrusion detection in IoT systems, shedding light on the vulnerability of IoT environments to sophisticated attack vectors. This study accentuates the exigency for robust intrusion detection mechanisms capable of thwarting adversarial threats in real-time, thus fortifying the security posture of IoT infrastructures.

Martina and Foresti [12] introduce a continuous learning approach for real-time network intrusion detection, emphasizing adaptability and resilience against evolving threats. The study propounds a dynamic learning framework capable of updating intrusion detection models in real-time, thereby enhancing the efficacy of intrusion detection systems in mitigating emerging cyber threats. Their results demonstrate significant improvements in detection accuracy over time, showcasing the effectiveness of continuous learning approaches in bolstering network security.

Morfino and Rampone [13] propose a near-real-time intrusion detection system for IoT devices leveraging supervised learning and Apache Spark. The study demonstrates the feasibility of deploying scalable intrusion detection solutions capable of processing large volumes of IoT data in near real-time, thus ensuring proactive threat detection and mitigation.

Magán-Carrión et al. [14] endeavour to establish a reliable comparison and evaluation framework for network intrusion detection systems based on machine learning approaches. Through benchmarking various detection algorithms, the study furnishes insights into the strengths and limitations of different approaches, thereby guiding the development of effective intrusion detection systems.

The reviewed literature underscores the burgeoning significance of real-time intrusion detection systems in securing IoT environments. Leveraging advancements in machine learning, continuous learning approaches, and scalable processing frameworks, researchers are making significant strides towards building robust intrusion detection mechanisms capable of mitigating emerging cyber threats in real-time.

3. Materials and Methods

Machine learning plays a crucial role in bolstering IoT network security by effectively identifying complex threats, adjusting defensive strategies, and promptly responding to potential risks. By analyzing extensive network data and device behavior patterns, machine learning algorithms excel in detecting subtle intrusion [15,16] attempt that traditional security systems might overlook.

Moreover, these algorithms continuously learn from new data, allowing them to enhance their accuracy over time, which is vital given the ever-evolving nature of threats in IoT environments. Additionally, machine learning contributes to reducing false alarms by analyzing network data in context and distinguishing genuine security threats, thereby enabling security teams to focus on addressing legitimate incidents [17]. Its capacity to identify abnormal behavior is particularly valuable in combating insider threats and compromised devices.

Furthermore, machine learning exhibits effectiveness in managing the extensive data produced by IoT devices [18], enabling comprehensive monitoring and analysis. Utilizing historical data, machine learning [19,20] can offer predictive forecasts regarding future threats, empowering proactive security actions. When combined with automated response mechanisms, machine learning facilitates rapid and adaptive reactions to security events, such as isolating compromised devices and updating security measures in real-time. Essentially, machine learning serves as a fundamental component in strengthening IoT network security, enhancing resilience, and mitigating cyber threats in today's interconnected digital environment.

3.1. Network Traffic Data Features

In the domain of IoT implementations, the significance of network traffic data features is underscored by the unique characteristics inherent to IoT devices. Below is an elaborated and rephrased rendition of the original points:

3.1.1. Device Categorization

Identifying IoT device types based on their traffic patterns stands as a foundational element in managing IoT networks effectively.

3.1.2. Data Packet Inspection

Delving into the contents of transmitted data packets aids in discerning the nature of the exchanged Information, spanning from sensor data to operational directives, thereby facilitating well-informed decision-making processes.

3.1.3. Communication Frequency Analysis

Assessing the rate at which IoT devices communicate offers insights into their operational behavior, aiding in the identification of anomalies or potential security vulnerabilities.

3.1.4. Power Management Oversight

Careful monitoring of network traffic related to power management functions, such as sleep modes and wake-up signals, empowers organizations to optimize energy consumption patterns for improved operational efficiency.

3.1.5. Location Monitoring

Utilizing network traffic data allows for the tracking of IoT device locations based on their interactions with diverse network access points or gateways, thereby streamlining asset management and resource allocation efforts.

3.1.6. Security Protocol Examination

Scrutinizing encryption protocols and security mechanisms deployed in IoT communications ensures the integrity and confidentiality of transmitted data, mitigating risks associated with unauthorized access or data breaches.

3.1.7. Topology Mapping

Visualizing network topology based on communication patterns provides valuable insights into the interconnections among IoT devices within a deployment, facilitating network optimization and troubleshooting endeavors.

3.1.8. Validation of Sensor Data

Authenticating the integrity and credibility of sensor data through network traffic analysis is crucial for ensuring the accuracy and reliability of insights derived from IoT-generated data.

3.1.9. Command and Control Monitoring

Vigilantly monitoring traffic associated with command and control operations, such as remote configuration and device management, enables effective governance and upkeep of IoT ecosystems.

3.1.10. Evaluation of Latency and Performance

Analyzing network traffic aids in gauging latency and response times for IoT applications, ensuring prompt data delivery and optimal user experiences.

3.1.11. Assessment of Bandwidth Usage: Evaluating the bandwidth consumption by IoT devices facilitates the efficient allocation of network resources, thereby alleviating congestion and enhancing overall network performance.

3.1.12. Detection of Anomalies

Employing anomaly detection mechanisms on network traffic data enables organizations to proactively identify and address deviations from normal behavior, thereby bolstering the resilience of IoT infrastructures against potential threats and vulnerabilities.

In conjunction with the considerations above, addressing DDoS attacks involving ICMP and TCP SYN packets demands rigorous protocol scrutiny and anomaly detection methodologies fortified by robust security measures such as intrusion detection systems and DDoS mitigation solutions.

3.2. Machine Learning Algorithms

Different algorithms employed for detecting intrusions in IoT network security, with a focus on DDoS, ICMP, and TCP SYN attacks, include the following.

3.2.1. Logistic Regression

It is a statistical approach utilized in scenarios involving binary classification, where the outcome variable can take on one of two possible states. Despite its name, logistic regression is primarily a classification method rather than a regression one. Its core function involves estimating the probability that a given input falls into a particular class.

Logistic regression proves useful in detecting intrusions within IoT security setups. It categorizes network patterns or device actions as standard or irregular. Through feature extraction and model training, logistic regression estimates the chances of abnormal behaviour, triggering alerts when detected. This continuous monitoring enhances cybersecurity by pinpointing potential threats in IoT networks safeguarding devices and data from harm.

3.2.2. K-Nearest Neighbors (KNN)

It stands as a straightforward yet impactful machine learning algorithm utilized for both classification and regression tasks. Its operation hinges on the principle of similarity, where items with resembling attributes tend to cluster closely together within a feature space.

KNN is a machine learning technique useful for intrusion detection in IoT security. It discerns between normal and anomalous network activity or device behavior by assessing data point similarity. Through feature selection, data preprocessing, and model training, KNN swiftly identifies potential threats or irregularities within IoT networks. Its application aids organizations in strengthening their cybersecurity measures, safeguarding IoT devices, and protecting data from malicious activities.

3.2.3. Support Vector Machine(SVM)

It is a supervised learning method utilized primarily for classification duties. It excels especially in situations where data instances fall into two distinct classes and require a well-defined boundary between them.

The SVM classifier is a potent tool for detecting intrusions in IoT security. Through meticulous feature selection, data preparation, and model training, it can effectively discern between typical and suspicious behavior in network traffic or device operations. By employing the trained SVM classifier, organizations can continuously monitor and promptly identify potential threats or security breaches within IoT networks, thereby reinforcing their cybersecurity efforts and protecting IoT devices and data from malicious activities.

3.2.4. Random Forest

It is an algorithm utilized in machine learning for classification, regression, and anomaly detection purposes. Its process involves creating multiple decision trees during training and aggregating their predictions by calculating the mode (for classification) or mean (for regression).

Random Forest proves to be a robust and effective method for detecting intrusions in IoT security. Its ensemble learning strategy, along with its ability to select relevant features, allows for the accurate identification of both normal and suspicious activity within IoT networks. By harnessing Random Forest's scalability and efficiency, businesses can efficiently monitor extensive IoT deployments, promptly recognizing security risks and breaches as they occur. Additionally, the algorithm's capacity to handle noisy data and offer interpretability makes it particularly suitable for the intricate and evolving landscapes of IoT environments. Overall, Random Forest serves as a valuable asset in fortifying the security stance of IoT infrastructures, proactively safeguarding against cyber threats and upholding the trustworthiness and stability of IoT operations.

3.3. Research Methodology

The research methodology was executed according to the workflow illustrated in Figure 1.

Step-1: Gathering Network Traffic Data Features

This stage involves systematically collecting data from various sources within the network, such as IoT devices or network infrastructure components. The dataset used in this project contained 10,345 data points, each encompassing 25 features.

These features encompass a range of network traffic behaviors, including packet characteristics, protocol types, and timestamps. Notably, specific features aimed at identifying potential attack patterns, such as TCP-SYN and ICMP attacks commonly associated with DDoS attacks, were integrated into the dataset to enhance the machine learning models' ability to detect malicious activity.

Step 2: Integration of Features for Attack Detection

In addition to general network traffic attributes, specialized features relevant to known attack signatures were incorporated into the dataset. These features, such as the frequency of TCP-SYN packets or ICMP echo requests, serve as indicators of suspicious network behavior and aid in distinguishing normal traffic from potential threats.

Step-3: Data Pre-processing

Pre-processing the data is essential to ensure its quality and suitability for training machine learning models. Within the Jupyter Notebook environment, various pre-processing steps were undertaken, including handling missing or infinite values within the dataset. Additionally, techniques such as data normalization or standardization may have been applied to ensure consistent feature scaling.

Step-4: Considering Jupyter Notebook

While the initial implementation utilized Jupyter Notebook, considerations were made regarding its efficiency, particularly with respect to large-scale datasets. Alternative tools or distributed processing frameworks, such as Apache Spark, were acknowledged for their potential benefits in terms of computational efficiency and scalability.

Step-5: Training Diverse Machine Learning Algorithms

Multiple machine learning algorithms were trained using the pre-processed dataset to develop models capable of identifying malicious network activity. These algorithms encompassed various methodologies, including Random Forest, Logistic Regression, Support Vector Classifier, and K-Nearest Neighbor, each offering distinct advantages and suitability for different scenarios.

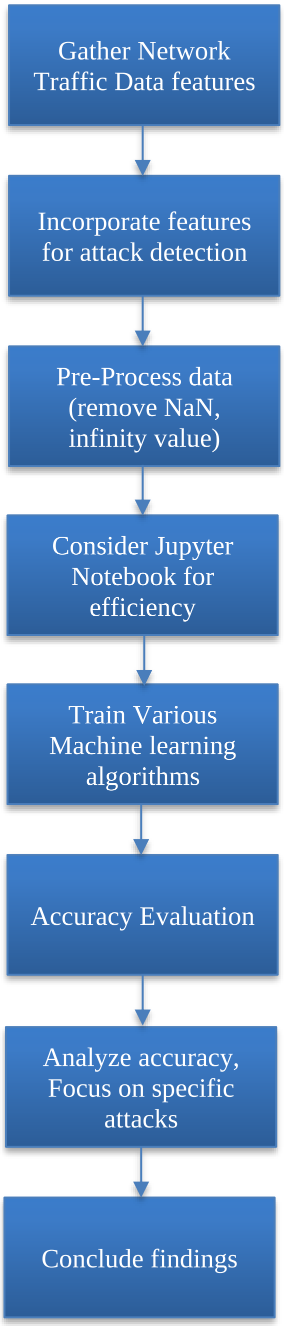
Gather Network Traffic Data features
Incorporate features for attack detection
Pre-Process data (remove NaN, infinity value)
Consider Jupyter Notebook for efficiency
Train Various Machine learning algorithms
Accuracy Evaluation
Analyze accuracy, Focus on specific attacks
Conclude findings

Fig. 1 Flowchart of research work

Step-6: Evaluation of Model Accuracy

Subsequent to model training, their performance was evaluated in terms of accuracy to assess their efficacy in detecting malicious network behavior. Comparison of algorithm accuracies provided insights into their effectiveness for intrusion detection. At the same time, performance analysis on specific attack types offered a further understanding of their strengths and weaknesses in differentiating between normal and malicious network traffic.

4. Results and Discussion

This section offers a thorough examination of employing machine learning models for detecting intrusions in IoT network security, focusing on DDoS, ICMP, and TCP SYN attacks. The accuracy of trained models, utilizing various algorithms such as Support Vector Machines (SVM), Random Forest (RF), Logistic Regression (LR), and K-Nearest Neighbor (KNN), is evaluated to discern normal network behavior from malicious activities.

Additionally, the interpretability of these models is explored to reveal the underlying patterns and features crucial for effective attack detection. This comprehensive analysis provides insights into the strengths and limitations of each algorithm, offering valuable guidance for improving intrusion detection systems in IoT environments. Figure 2 presents the accuracy of identifying DDoS attacks using various machine learning algorithms, whereas Figure 3 demonstrates the accuracy of detecting ICMP attacks. Furthermore, Figure 4 exhibits the accuracy of recognizing TCP SYN attacks.

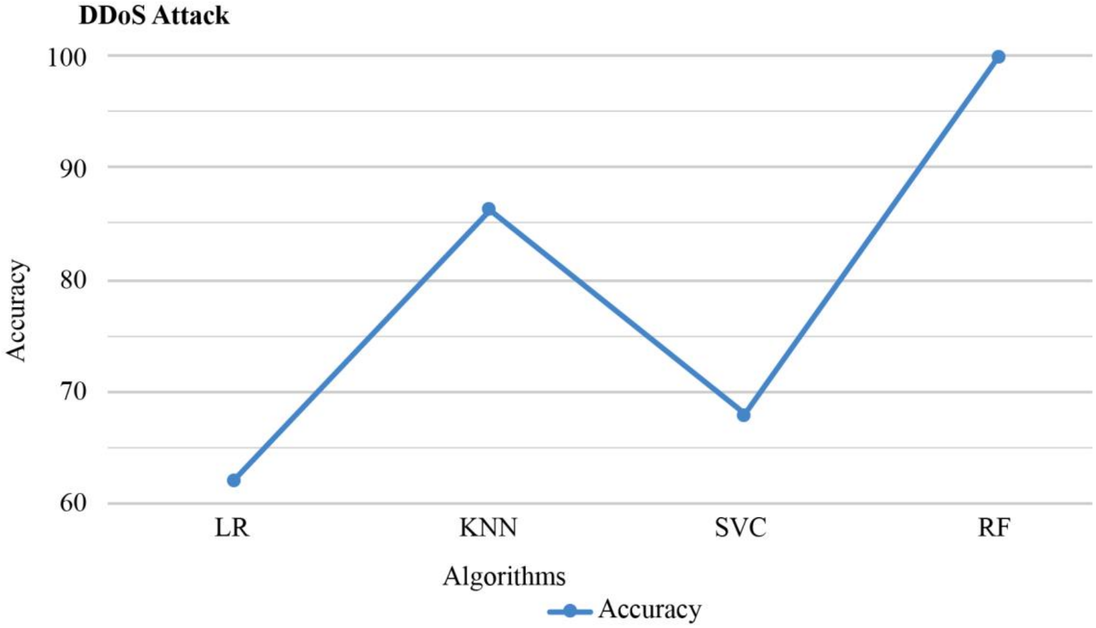

Fig. 2 Accuracy assessment of machine learning algorithms for detecting DDoS attacks

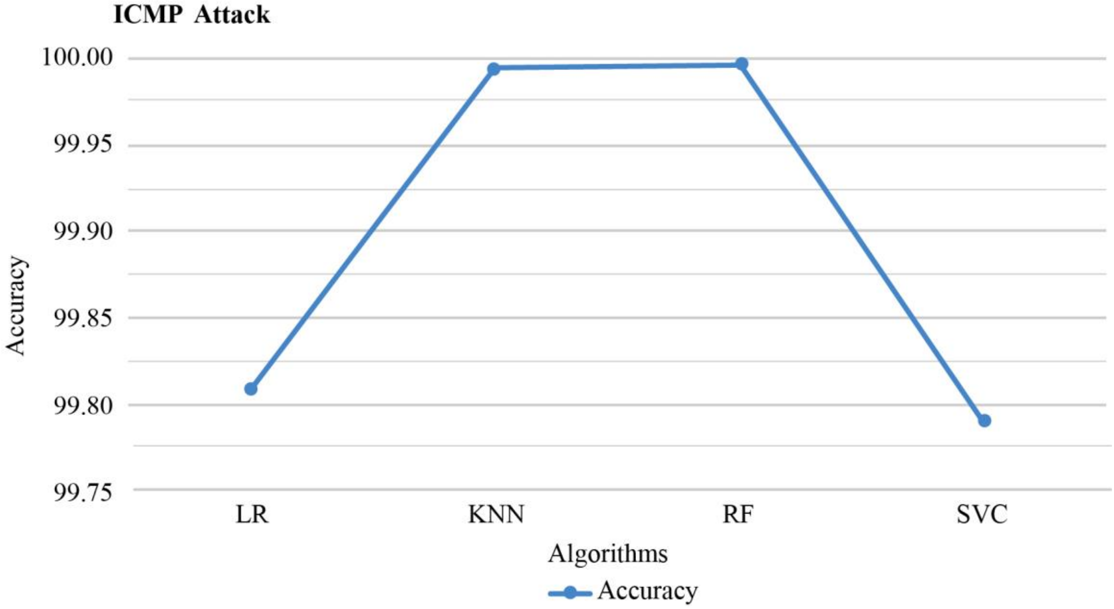

Fig. 3 Accuracy assessment of machine learning algorithms for detecting ICMP attacks

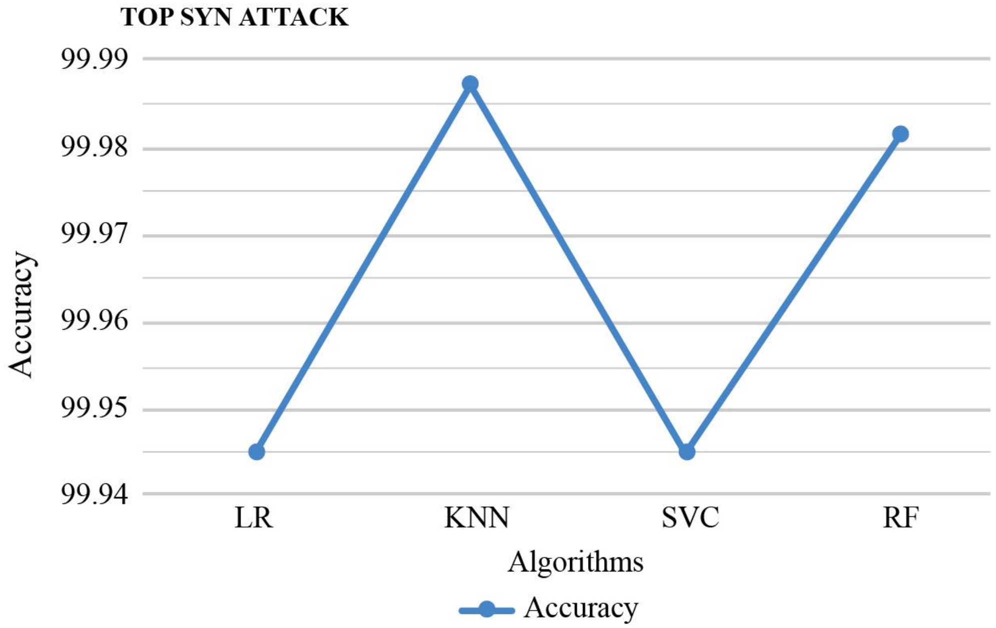

Fig. 4 Accuracy assessment of machine learning algorithms for detecting TCP SYN attacks

Table 1. Accuracies of machine learning algorithms for IoT network security

Machine Learning Algorithms	**Accuracy of IoT Network Security attacks**		
	DDoS Attacks	**ICMP attacks**	**TCP SYN attacks**
Logistic Regression	62	99.81	99.94
KNN	86	99.99	99.98
SVM classifier	68	99.79	99.94
Random forest	100	99.99	99.98

The figure-2 clearly shows that the Random Forest (RF) algorithm attained the highest accuracy rate at 100%, surpassing Logistic Regression (LR), K-Nearest Neighbour (KNN), and Support Vector Classifier (SVC), which achieved accuracies of 62%, 86%, and 68%, respectively.

The data from the figure-3 indicates that the Logistic Regression (LR), K-Nearest Neighbour (KNN), Support Vector Classifier (SVC), and Random Forest (RF) algorithms achieve accuracies of 99.81%, 99.99%, 99.79%, and 99.99%, respectively.

From the figure, it can be noted that the Logistic Regression (LR) and Support Vector Classifier (SVC) algorithms achieved accuracies of 99.94%. In comparison, the K-Nearest Neighbor (KNN) and Random Forest (RF) algorithms attained accuracies of 99.98%.

The accuracies of various machine learning algorithms in detecting DDoS attacks, ICMP, and TCP SYN attacks in IoT network security are summarized in Table 1.

The table distinctly illustrates that across all three attack scenarios, the Random Forest algorithm outperforms Support Vector Machine (SVM), K-Nearest Neighbor (KNN), and Logistic Regression (LR) in terms of performance.

Our paper demonstrates superior performance in detecting various types of attacks in IoT networks compared to existing research. This success can be attributed to several key factors: thorough feature engineering that encompasses diverse aspects of IoT communications, meticulous data pre-processing to ensure data quality, and systematic model selection.

Optimization to enhance model performance, utilization of ensemble techniques to leverage the strengths of different algorithms, and comprehensive cross-validation and evaluation to ensure the reliability and applicability of our results. Overall, our study highlights the importance of methodological rigor, effective feature engineering, and optimized model development in achieving robust intrusion detection systems for IoT security.

5. Conclusion

This study represents a substantial advancement in bolstering IoT network security by implementing rapid intrusion detection mechanisms enhanced with machine learning techniques. By tackling the rising security challenges associated with IoT devices, our research has formulated effective strategies for promptly identifying and mitigating intrusions, spanning various types such as Distributed Denial of Service (DDoS), Internet Control Message Protocol (ICMP), and Transmission Control Protocol Synchronize (TCP SYN).

Employing supervised machine learning algorithms such as Support Vector Machines (SVM), Logistic Regression, Random Forest, and K-Nearest Neighbors (KNN), we have proposed an intrusion detection model characterized by high accuracy. The assessment of this model's performance, utilizing diverse datasets obtained from platforms like Kaggle, has demonstrated notable accuracy levels across different intrusion types. Specifically, our model achieved an average accuracy of 82% for DDOS, 99.96% for TCP SYN, and 99.8% for ICMP, with Random Forest emerging as the most accurate among the algorithms tested. These results underscore a significant advancement in fortifying IoT network security, thereby enhancing overall resilience against malicious activities and unauthorized access. Through the application of machine learning techniques, our proposed approach provides a proactive and robust defense mechanism against evolving threats in the IoT domain. Looking ahead, ongoing research and implementation endeavors in this direction are imperative for safeguarding the integrity and security of IoT ecosystems.

References

[1] Ansam Khraisat et al., “Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges,” *Cybersecurity*, vol. 2, no. 1, pp. 1-22, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Nadia Chaabouni et al., “Network Intrusion Detection for IoT Security Based on Learning Techniques,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671-2701, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Bruno Bogaz Zarpelão et al., “A Survey of Intrusion Detection in Internet of Things,” *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Khalid Albulayhi et al., “IoT Intrusion Detection using Machine Learning with a Novel High Performing Feature Selection Method,” *Applied Sciences*, vol. 12, no. 10, pp. 1-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Mohamed Faisal Elrawy, Ali Ismail Awad, and Hesham F.A. Hamed, “Intrusion Detection Systems for IoT-Based Smart Environments: A Survey,” *Journal of Cloud Computin*g, vol. 7, no. 1, pp. 1-20, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Emad E. Abdallah, Wafa’ Eleisah, and Ahmed Fawzi Otoom, “Intrusion Detection Systems Using Supervised Machine Learning Techniques: A Survey,” *Procedia Computer Science*, vol. 201, pp. 205-212, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Ala Al-Fuqaha et al., “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] P. Ray, and A. Mohapatra, “Security in Healthcare Applications using Wireless Medical Sensor Networks: A Survey,” *Journal of Medical Systems*, vol. 37, no. 3, p. 9975, 2013.

[9] Rick Hofstede et al., “Towards Real-Time Intrusion Detection for NetFlow and IPFIX,” *Proceedings of the 9th International Conference on Network and Service Management (CNSM 2013)*, Zurich, Switzerland, pp. 227-234, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[10] Phurivit Sangkatsanee, Naruemon Wattanapongsakorn, and Chalermpol Charnsripinyo, “Practical Real-Time Intrusion Detection Using Machine Learning Approaches,” *Computer Communications*, vol. 34, no. 18, pp. 2227-2235, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[11] Han Qiu et al., “Adversarial Attacks against Network Intrusion Detection in IoT Systems,” *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10327-10335, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Marcello Rinaldo Martina, and Gian Luca Foresti, “A Continuous Learning Approach for Real-Time Network Intrusion Detection,” *International Journal of Neural Systems*, vol. 31, no. 12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Valerio Morfino, and Salvatore Rampone, “Towards Near-Real-Time Intrusion Detection for IoT Devices Using Supervised Learning and Apache Spark,” *Electronics*, vol. 9, no. 3, pp. 1-13, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[14] Roberto Magán-Carrión et al., “Towards a Reliable Comparison and Evaluation of Network Intrusion Detection Systems Based on Machine Learning Approaches,” *Applied Sciences*, vol. 10, no. 5, pp. 1-21, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Nahida Islam et al., “Towards Machine Learning Based Intrusion Detection in IoT Networks,” *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1801-1821, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Parag Verma et al., “A Novel Intrusion Detection Approach using Machine Learning Ensemble for IoT Environments,” *Applied Sciences*, vol. 11, no. 21, pp. 1-21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Bambang Susilo, and Riri Fitri Sari, “Intrusion Detection in IoT Networks Using Deep Learning Algorithm," *Information*, vol. 11, no. 5, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohanad Sarhan et al., “Feature Extraction for Machine Learning-Based Intrusion Detection in IoT Networks,” *Digital Communications and Network*s, vol. 10, no. 1, pp. 205-216, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[19] Dhanke Jyoti Atul et al., “A Machine Learning Based IoT for Providing an Intrusion Detection System for Security,” *Microprocess and Microsystems*, vol. 82, pp. 1-10, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Abhishek Verma, and Virender Ranga, “Machine Learning Based Intrusion Detection Systems for IoT Applications," *Wireless Personal Communications*, vol. 111, pp. 2287-2310, 2020. [CrossRef] [Google Scholar] [Publisher Link]