IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

Performance Evaluation of Machine Learning Algorithms for IoT-Based Intrusion Detection

Siddhant Sheshrao Bharade, Sanskar Sahebrao Ghongade,
Amol Ramji Paratkar, Prof. Rajeshri P. Mane
Department of Electronics and Telecommunication,
JSPM'S RSCOE, Tathawade, Pune, India
siddhantbharade02@gmail.com, sanskarghongade0526@gmail.com
amolparatkar284@gmail.com, rpmane_entc@jspmrscoe.edu.in

Abstract: *With the rapid growth of the Internet of Things (IoT), the security of connected devices and networks has become a serious issue. IoT networks are exposed to various cyber-attacks because of their distributed nature and lack of security mechanisms. This paper introduces a machine learning-based solution for identifying IoT-specific attacks using the Multi-Layer Perceptron (MLP) classifier. The RT-IoT2022 dataset with benign and adversarial network activities was used for experimentation. This dataset combines real IoT traffic from devices such as ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp and simulated attacks such as SSH brute-force, DDoS (Hping and Slowloris), and Nmap scanning. Preprocessing of the dataset was carried out to manage missing values, scale feature ranges, and filter out apt features for model training. MLP classifier, being a feedforward neural network artificial system, was implemented and trained upon the filtered dataset to segregate normal versus malicious network activity. Accuracy, precision, recall, F1-score, and confusion matrix metrics were utilized for comparison to establish how well the model performs. High detection precision showed that the proposed method indicated how the model has the potential to learn advanced network traffic patterns. The research draws attention to the significance of cognitive machine learning algorithms in enhancing IoT networks' robustness against cyber attacks. Drawing on the capacity for learning associated with neural networks, the MLP classifier offers an efficient yet efficient solution for intrusion detection in real-time. The findings of the research can facilitate the development of adaptive security mechanisms that can promptly react to adaptive threats in IoT environments.*

Keywords: IoT Security, Intrusion Detection System (IDS), Machine Learning, Multi-Layer Perceptron (MLP), RT-IoT2022 Dataset, Cyber-Attack Detection, DDoS, Brute-Force Attack, Neural Networks, Network Traffic Analysis

I. INTRODUCTION

The Internet of Things (IoT) has risen as a revolutionary technology, transforming the way devices interact, communicate, and make contributions across applications. From home automation and healthcare networks to industrial automation and smart transportation systems, the spread of IoT devices has dramatically increased connectivity and automation. These products, frequently loaded with sensors and software, produce and share tremendous amounts of information in real-time, offering critical insights and facilitating smooth operations in industries. While the use of IoT technology continues to expand exponentially, it poses a new range of security threats and vulnerabilities that conventional security controls are not prepared to address. The IoT network generally consists of a heterogeneous collection of resource-limited devices, wireless communication protocols, and decentralized architecture. The heterogeneity makes the network vulnerable to cyber-attacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MitM), spoofing, sniffing, and brute-force attacks. Additionally, the absence of standardized security protocols, the constrained computing capabilities of IoT devices, and the frequent firmware vulnerabilities render these systems vulnerable and difficult to secure. One compromised IoT device can serve as a gateway for attackers to penetrate an entire network, causing substantial data breaches and disrupting essential services.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

The necessity for smart, real-time Intrusion Detection Systems (IDS) has become essential to counter these threats. IDS solutions try to inspect network traffic, detect unusual patterns, and react to potential threats before substantial damage is caused. Conventional IDS methods depend a lot on signature-based approaches and are not effective enough in IoT. These systems are incapable of detecting new or zero-day attacks and need constant updates to keep the signature database strong. Conversely, machine learning (ML)-driven IDS presents a promising solution, which can learn from past data, generalize patterns, and identify novel attacks. This work is centered on the use of machine learning methods for IoT security improvement, with particular focus on the Multi-Layer Perceptron (MLP) classifier. MLP, a type of feedforward artificial neural network, has demonstrated considerable potential in classification problems because it can represent complex non-linear input feature relationships. Its architecture, made up of input, hidden, and output layers with non-linear activation functions, allows it to conduct strong learning over high-dimensional data sets. Training an MLP model on labelled network traffic data allows it to differentiate between malicious and benign activity effectively, therefore enabling proactive mitigation of threats.

This study employs the RT-IoT2022 dataset, a wide-ranging dataset of real and emulated IoT network traffic. The dataset contains traffic from IoT devices ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp, including their normal usage and adversarial settings with typical attack vectors such as SSH brute-force, DDoS (Hping and Slowloris), and Nmap port scan. One of the strengths of this dataset is that it mirrors realistic bidirectional network traffic accurately using Zeek and Flowmeter tools. Such diversity enables the classifier to observe fine differences in legitimate and suspicious activity. Implementation starts with aggressive data preprocessing. It involves managing missing values, categorical data encoding, feature normalization, and identifying attributes to select in order to improve classifier performance. Preprocessing guarantees that the data input into the MLP model is clean, uniform, and appropriate for successful learning. The dataset is divided into training and test sets after preprocessing to test the generalization ability of the model.

This study employs the RT-IoT2022 dataset, a wide-ranging dataset of real and emulated IoT network traffic. The dataset contains traffic from IoT devices ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp, including their normal usage and adversarial settings with typical attack vectors such as SSH brute-force, DDoS (Hping and Slowloris), and Nmap port scan. One of the strengths of this dataset is that it mirrors realistic bidirectional network traffic accurately using Zeek and Flowmeter tools. Such diversity enables the classifier to observe fine differences in legitimate and suspicious activity. Implementation starts with aggressive data preprocessing. It involves managing missing values, categorical data encoding, feature normalization, and identifying attributes to select in order to improve classifier performance. Preprocessing guarantees that the data input into the MLP model is clean, uniform, and appropriate for successful learning. The dataset is divided into training and test sets after preprocessing to test the generalization ability of the model.

The findings of this research identify that the MLPClassifier operates effectively in classifying network traffic with high accuracy in identifying known and unknown attack classes. The classification report and confusion matrix reflect an evenly distributed performance among all classes with negligible misclassifications. These findings reflect the prospect of machine learning-driven IDS as an integral element of contemporary IoT security frameworks. In addition, this study adds to the increasing literature supporting AI-based security in IoT networks. Although MLP is only one of numerous machine learning algorithms that can be used in this field, its robust performance in this study makes it relevant. Future developments may involve comparing MLP with other classifiers, including Support Vector Machines (SVM), Random Forests, Decision Trees, and ensemble methods to compare performance. Combining deep learning architectures such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs) can enhance detection abilities, particularly for time-series traffic data.

Another area for upcoming research is the use of explainable AI (XAI) methods to make models more interpretable. In security-critical domains, it is necessary to sense an attack and see why a specific decision was taken. SHAP (Shapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) are some tools that can explain model predictions through visualization, leading to higher trust and transparency. In summary, the large-scale deployment of IoT devices requires sophisticated security mechanisms specifically designed for their specific architecture and vulnerabilities. Machine learning algorithms such as MLPClassifier provide a scalable, adaptive, and efficient way to detect intrusion in IoT networks. Utilizing real-world datasets such as RT-IoT2022 and intelligent

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

preprocessing and model-tuning methods, efficient IDS solutions can be constructed to protect critical IoT infrastructures. This study is a step in combining AI with cyber security to create the next generation of intelligent, self-protecting networks.

II. LITERATURE SURVEY

Ramya Prakash et al. [1] provided a paper on the security threats and attacks in the Internet of Things (IoT). The paper discusses IoT security vulnerabilities throughout its layers of architecture, ranging from physical to network and application levels. It points out key challenges like device heterogeneity, restricted computational capabilities, and non-standardized protocols. The paper describes various kinds of attacks—physical, software, network, and encryption—and stresses the importance of having strong countermeasures such as strong authentication, secure communication protocols, and firmware updates. The authors present a layered taxonomy and address existing mitigation techniques, including learning-based and encryption methods. This survey has a major impact on comprehending the changing dynamics of IoT security and the requirement for dynamic, adaptive, and multi-layered solutions. The authors advocate that efforts should be aimed towards integrated and self-sufficient security solutions custom-suited to large-scale IoT systems.

Anurag Tiwari et al. [2] shared a paper on IoT-based smart home cyber-attack detection and defense. The paper suggests an integrated system using machine learning and network traffic analysis to identify, classify, and counter cyber threats in real-time. The authors tackle major types of attacks including malware infections, unauthorized access, and DDoS attacks by using algorithms such as Decision Trees, SVM, and Deep Learning techniques. A testbed consisting of eight types of IoT devices and a smart home environment was employed for testing. The system also enables policy customization and automated attack response mechanisms such as device isolation and traffic blocking. Experimental results confirm the effectiveness of the system in detecting attacks and reducing their impact. The research highlights the importance of data-driven defense mechanisms in IoT environments. Future improvement areas include edge computing integration and privacy-preserving methods. This book is a solid foundation for the protection of IoT-enabled smart homes using micro-adaptive and scalable solutions.

Tehseen Mazhar et al. [3] gave a paper on the use of artificial intelligence for analyzing IoT security issues and their solutions. The paper elaborately discusses vulnerabilities in the entire IoT architecture—perception, network, support, and application layers—and analyzes how cyber threats such as DDoS, spoofing, and malware influence smart environments. Machine learning and deep learning are pointed out as viable countermeasures in the research. These are implemented through algorithms such as KNN, SVM, Decision Trees, and LSTM for anomaly detection and system robustness. The research suggests security models based on clustering, regression, feature selection, and rule-based methods. A multi-layer approach is developed as a whole-system strategy to secure IoT infrastructures. Continuous adaptation of the model to dynamic threats and intrusion detection through real-time data analysis is emphasized by the research. Future work on hybrid models and feature engineering methods is suggested in order to maximize security performance. The review helps in incorporating AI into smart and scalable IoT defense mechanisms.

S. Nandhini et al. [4] reported a cyber-attack detection scheme in IoT-WSN devices based on cutting-edge neural network architectures optimized by threat intelligence. The authors suggest Equilibrium Optimizer Neural Network (EO-NN), Particle Swarm Optimization Neural Network (PSO-NN), and Single Candidate Optimizer Long Short-Term Memory (SCO-LSTM) models for the detection of sophisticated attacks such as False Data Injection, Brute Force, and Hybrid Brute Force. These models include connecting and hidden neural layers and leverage threat intelligence information to evolve with changing attacker behaviors. The SCO-LSTM model resulted in the maximum classification accuracy of 99.89%. The paper overcomes the shortcomings of conventional IDS systems by proposing adaptive algorithms that act in response to constant node behavior alterations in IoT-WSN environments. The research proves strong detection with low processing overhead and energy expenditure through the inclusion of threat intelligence and multiple validation methods. Future work could be to extend to real-time deployment as well as hybrid learning methods for improved resilience.

Rajakumaran Gayathri et al. [5] introduced a research paper on detection and counteracting IoT-based attacks by SNMP and Moving Target Defense (MTD) techniques. In this paper, an innovative two-layer framework has been put forward to defend against distributed denial-of-service (DDoS) and false data injection attacks. Detection is done with Simple

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

Network Management Protocol (SNMP) and Kullback–Leibler Distance (KLD) to detect abnormal traffic patterns, and mitigation is done with Access Control Lists (ACLs) and MTD techniques deployed in the AWS cloud. The MTD mechanism provides dynamic IP handling and server migration between availability zones, reducing attack likelihood to 0.15% and switching time to 0.076 seconds. The design successfully secures IoT cloud environments by minimizing attack surfaces and verifying minimal data breach threat. Experimental evaluation shows enhanced system performance with slight migration latency. The work emphasizes the merit of dynamic defense approaches for improving IoT security and suggests future work on larger attack categories and mixed AI-based techniques.

Jingyi Su et al. [6] described an experiment on feature selection and prediction of IoT attacks via machine learning algorithms. The paper compares tree-based classifiers—Decision Tree (DT), Random Forest (RF), and Gradient Boosting Machine (GBM)—on an exhaustive IoT2020 intrusion dataset. The research investigates attack types such as Mirai, DoS, MITM, and Scan by pre-processing 625,783 samples considering top-ranked features. Random Forest always returned high AUC scores (a maximum of 0.9999), and Decision Tree returned improved classification precision. GBM, though powerful, incurred increased computational cost. The paper highlights the importance of feature selection for anomaly detection and stresses the value of model comparison over binary data sets. It concludes that tree-based models are ideal for detecting IoT attacks due to their explainability and scalability. Future research is focused on hyperparameter optimization and generalizing classification to real-time detection in dynamic IoT systems.

Ritika Raj Krishna et al. [7] performed a thorough review of IoT attacks and threats, including their taxonomy, challenges, and possible mitigation approaches. The article presents an enhanced IoT architecture—three-, five-, and seven-layer models—and discusses related communication protocols and security vulnerabilities. It categorizes systematically threats and attacks at different architectural layers, i.e., perception, network, and application. The research emphasizes the inadequacies of current frameworks and the need for embracing pervasive technologies such as Blockchain (BC), Fog Computing (FC), Edge Computing (EC), and Machine Learning (ML) for strengthening IoT security. Furthermore, the survey gives a comparative overview of the existing work, recognizing open issues such as interoperability, standardization, and real-time response. The research provides an informative guide to IoT developers and researchers for the development of fault-tolerant and secure systems through presenting a multidimensional taxonomy of threats and correlating it with pertinent countermeasures.

Resul Daş et al. [8] have shared a study on the evaluation of cyber-attacks on IoT-based critical infrastructures, highlighting their growing susceptibility due to connectivity with the internet. The paper presents an exhaustive taxonomy of attacks like malware injection, phishing, DDoS, APT, and SCADA-targeted intrusions in industries like energy, water, transport, and healthcare. In the light of real-world case studies spanning 2008 to 2019, the authors identify disastrous consequences, ranging from service disruptions, financial costs, to safety hazards. The research proposes a layered model of shared attack vectors and discusses countermeasures, such as encryption, access control, intrusion detection systems (IDS), IP fast hopping, and periodic firmware update. The authors stress the role of hybrid IDS techniques for real-time detection and proactive defense. This thorough survey emphasizes the necessity for nations to implement strong cybersecurity frameworks for securing critical IoT-based infrastructures.

Tinshu Sasi et al. [9] carried out a thorough survey of IoT attacks, introducing a multidimensional taxonomy and exhaustive detection mechanisms. The research categorizes IoT attacks into domains, types of threats, methods of execution, software surfaces, protocols, device attributes, adversary locations, and levels of information damage. It stresses that resource scarcity, non-standardization, and inadequate update mechanisms greatly impede IoT security. The authors also examine various vulnerabilities from public repositories and real-world CVEs to point out significant threats such as malware injection, replay attacks, and DDoS. Detection techniques such as machine learning, honeypots, and intrusion detection systems are thoroughly discussed. This paper is unique in integrating Industrial IoT (IIoT) insights and sketching open research challenges centered around security, privacy, and real-time threat response. The survey provides a systematic framework for future work, calling for the implementation of lightweight security measures, context awareness, and hybrid detection mechanisms to enhance IoT resilience.

Amit Jaykumar Chinchawade et al. [10] provided an exhaustive account of threats and attacks within the Internet of Things (IoT) system. The chapter classifies threats into unstructured, structured, internal, and external and studies types of attacks in all seven OSI layers ranging from physical manipulation to application-layer exploits. It also emphasizes vulnerabilities of device communication protocols and illustrative attack instances like ARP spoofing, MAC spoofing,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

and VLAN hopping. Every OSI layer is complemented by real-world mitigation techniques like biometric authentication, BPDU guards, encrypted sessions, and application-level firewalls. The authors highlight the growing number of attacks and severity due to the extensive deployment of IoT devices and minimal security integration. They support the need for stronger multi-layered security architectures and greater awareness of physical and network-level threats. The chapter lays a solid groundwork for understanding how the stacked vulnerabilities in IoT can be dealt with through systematic and preventive cybersecurity steps.

III. METHODOLOGY

This section discusses the methodology of deploying a machine learning-based Intrusion Detection System (IDS) for IoT networks based on the Multi-Layer Perceptron (MLP) classifier. The methodology consists of several steps: dataset choice, data preprocessing, feature extraction, model selection, training, testing, and evaluation.

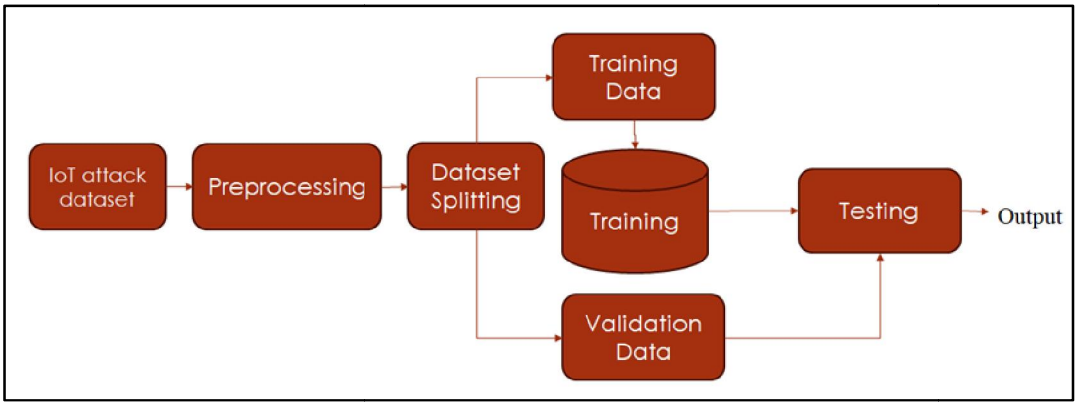

Figure : Block diagram of the IoT attack detection using ML

The blocks of the proposed system are explained below.

Dataset Description

The data used in this research is the RT-IoT2022 dataset, which is specially formulated for IoT security research. The dataset contains exhaustive network traffic information collected from IoT devices like ThingSpeak-LED, Wipro-Bulb, and MQTT-Temp. The dataset features benign traffic and different cyber-attacks like SSH brute-force attacks, Hping and Slowloris-based DDoS attacks, and Nmap scanning patterns. The realistic and varied nature of the dataset renders it especially useful since it records bi-directional network properties with the Zeek network sensor tool and Flowmeter plugin. Some of these properties are flow duration, total bytes, packets per second, and other vital network properties. The RT-IoT2022 dataset therefore presents a complete and realistic portrayal of IoT network traffic under real-world conditions, and it is therefore well-suited for training and testing machine learning algorithms for intrusion detection.

Data Preprocessing

Data preprocessing plays a significant role in preparing the raw data for training an efficient machine learning model. The initial step was to clean the dataset to remove missing or null values in order to keep it consistent and intact. Categorical variables like labels describing attack types were encoded into numerical values using label encoding methods. Feature scaling was subsequently performed using Min-Max normalization to scale all numeric values into a common range of 0 to 1, which aids in speeding up convergence when training the model. Lastly, the cleaned and normalized dataset was split into training and test sets with a 70:30 ratio to allow the model to be tested on unseen data to determine generalization performance.

Feature Selection

In order to enhance model efficiency and cut down on computational overhead, feature selection was utilized to select the most important features from the data. A correlation matrix was first created to represent relationships between features and target labels. Features that were highly redundant or had low variance were dropped. Aside from correlation analysis, domain knowledge was utilized to preserve features important in identifying network anomalies like packet length, flow duration, and bytes transferred. This operation assisted in lowering dimensionality and enhancing the training speed of the model without diminishing its effectiveness in identifying attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

MLPClassifier: Model Architecture

The model that is utilized in this research is the Multi-Layer Perceptron (MLP) classifier, which is a feedforward artificial neural network that provides output labels for input data by going through multiple layers of neurons. The architecture features an input layer for receiving preprocessed features, one or more hidden layers in which actual learning occurs through non-linear activation functions, and an output layer that identifies whether traffic is benign or of one of the attack classes. The Rectified Linear Unit (ReLU) function was used to activate the hidden layers for this deployment. Conversely, the output layer used the softmax or logistic activation function, depending on whether the classification was multi-class or binary. The MLPClassifier was selected because it could learn intricate non-linear patterns, which made it appropriate for real-time intrusion detection in dynamic IoT environments.

Model Training and Optimization

The classification and training portion of our research involves applying variant machine learning techniques, i.e., SVM and KNN, to feature sets preprocessed from the IoT network traffic dataset. There is something good for every technique when it comes to classification. SVM is, in the best sense, producing the optimal hyperplane between classes and efficiently dealing with non-linear decision surfaces with the help of kernels. On the other hand, KNN classifies data based on the spatial proximity of data points and labeling according to the most common class among the k-nearest neighbors.

Evaluation Metrics

The performance of the model was measured with a robust set of metrics to get an overall view of its classification capacity. Accuracy was computed to get an idea of the overall accuracy of predictions, and precision calculated how many of the predicted attacks were actually attacks. Recall estimated the model's capacity to recognize all the applicable instances of attack, and the F1-score gave a harmonic mean of precision and recall. A confusion matrix was also created in order to display the values of true positives, false positives, true negatives, and false negatives. These test metrics played a crucial role in the analysis of the resilience and consistency of the SVM and KNN for application in actual IoT networks.

IV. RESULT AND DISCUSSION

This section presents a detailed comparison of the performance outcome of the proposed system for classifying IoT attacks through machine learning algorithms, i.e., SVM (Support Vector Machines) and KNN (k-nearest Neighbors). Table 1 is a comparison of two machine learning algorithms, Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), in terms of four performance metrics: Precision, Recall, F1-Score, and Accuracy. These are important metrics for measuring how well the models recognize and classify IoT network traffic as benign or malicious.

Table 1 Performance of ML algorithm

Algorithms	Precision	Recall	F-1 score	Accuracy
SVM	0.93	0.93	0.92	0.93
KNN	0.94	0.94	0.94	0.94

The accuracy of a model is the ratio of accurately classified instances of attacks to all instances labeled as attacks. High precision would mean low false positives. For this research, the KNN algorithm yielded a slightly higher precision rate of 0.94 than SVM's 0.93, which implies that KNN performed slightly better in correctly labeling malicious behavior without classifying benign traffic as threats.

The recall measure, or sensitivity, assesses the model's capacity to correctly identify all real attack occurrences in the dataset. It is particularly important in intrusion detection systems, as an inability to detect an attack will have catastrophic implications. KNN once more proved to be the top performer with a recall of 0.94, just a fraction above SVM's 0.93, suggesting that KNN was better at catching more attack situations.

The F1-score, which is the harmonic mean of recall and precision, is a well-balanced measure of the accuracy of a model, particularly when applied to imbalanced data. In this case, KNN exhibited a consistently strong F1-score performance of 0.94, while SVM had an F1-score of 0.92. It indicates that not only did KNN have a strong balance between precision and recall, but it also had more stable classification outcomes for all categories of attacks.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

Lastly, as for overall accuracy, which counts the ratio of correctly classified instances (attack and benign combined), KNN again performed better than SVM at 0.94 compared to 0.93. Even though the difference in accuracy is small, it supports the comment that KNN had a minor advantage in terms of classification performance in all measured metrics.
SVM and KNN worked well in detecting IoT-based cyber-attacks, though KNN demonstrated slightly superior performance in all measures considered. Therefore, it is a slightly better option for IoT network intrusion detection in the scope of this work. However, computational complexity and execution time must be analyzed while implementing these models in real-time scenarios.

V. CONCLUSION

This paper suggested a machine learning-based intrusion detection system to protect IoT networks using the RT-IoT2022 dataset. Two popular algorithms, Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), were used and compared in terms of key performance metrics such as precision, recall, F1-score, and accuracy. The result proved that the performance of both models was excellent and that KNN outperformed SVM on all the metrics. KNN maintained a 94% accuracy rate, indicating its effectiveness in separating malicious and benign traffic in IoT settings. The study proves the ability of light data-driven models to detect diverse and changing patterns of attacks in real time, making them well-suited for deployment in IoT systems that are resource-constrained. In short, the study confirms that intelligent machine learning algorithms are capable of enhancing the security position of IoT networks through timely and accurate threat detection.
Though the current work has encouraging results, certain possibilities can be investigated to further develop the system more effectively and pragmatically. The future could involve testing and exploring different machine learning and deep learning techniques such as Random Forests, Gradient Boosting Machines, Convolutional Neural Networks (CNNs), and Recurrent Neural Networks (RNNs) in order to advance the classification capability, especially concerning time-evolving attack patterns. Moreover, integrating Explainable AI (XAI) techniques like SHAP or LIME would improve interpretability of the model, bringing about more trust in autonomous decisions. Integration into edge computing environments is another potential domain space that could utilize real-time detection with zero latency. Lastly, more work in the future can involve the model being tested on bigger and more diverse datasets involving newer and more complex cyber-attacks to improve the robustness and generalization capacity of the model over different IoT ecosystems.

REFERENCES

[1]. Prakash, R., Neeli, J., & Manjunatha, S. (2024). A survey of security challenges attacks in IoT. *E3S Web of Conferences, 491*, 04018. https://doi.org/10.1051/e3sconf/202449104018

[2]. Tiwari, A., & Waoo, A. A. (2023). IoT-based smart home cyber-attack detection and defense. *TIJER - International Research Journal, 10*(8), 73–88. https://ssrn.com/abstract=4537209

[3]. Mazhar, T., Talpur, D. B., Al Shloul, T., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using artificial intelligence. *Brain Sciences, 13*(4), 683. https://doi.org/10.3390/brainsci13040683

[4]. Nandhini, S., Rajeswari, A., & Shanker, N. R. (2024). Cyber attack detection in IoT-WSN devices with threat intelligence using hidden and connected layer based architectures. *Journal of Cloud Computing: Advances, Systems and Applications, 13*(159). https://doi.org/10.1186/s13677-024-00722-9

[5]. Gayathri, R., Usharani, S., Mahdal, M., Vezhavendhan, R., Vincent, R., Rajesh, M., & Elangovan, M. (2023). Detection and mitigation of IoT-based attacks using SNMP and moving target defense techniques. *Sensors, 23*(3), 1708. https://doi.org/10.3390/s23031708

[6]. Su, J., He, S., & Wu, Y. (2022). Features selection and prediction for IoT attacks. *High-Confidence Computing, 2*, 100047. https://doi.org/10.1016/j.hcc.2021.100047

[7]. Krishna, R. R., Priyadarshini, A., Jha, A. V., Appasani, B., Srinivasulu, A., & Bizon, N. (2021). State-of-the-art review on IoT threats and attacks: Taxonomy, challenges and solutions. *Sustainability, 13*(18), 9463. https://doi.org/10.3390/su13169463

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 7, March 2025

[8]. Daş, R., & Gündüz, M. Z. (2019). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security Science, 8*(4), 122–133. https://www.researchgate.net/publication/350374715

[9]. Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms, and challenges. *Journal of Information and Intelligence, 2*(2024), 455–513. https://doi.org/10.1016/j.jiixd.2023.12.001

[10]. Chinchawade, A. J., & Lamba, O. S. (2023). Internet of Things (IoT): Treats and Attacks. In *Multidisciplinary Research Trends* (Vol. 4, pp. 198–203). https://www.researchgate.net/publication/370778279