[1] Husam Ameer Al-khawaja

[2] Sefer Kurnaz

# Enhancing IoT Security through Ensemble Classification Models and Image Processing Techniques


***Abstract:*** - The explosive growth of IoT devices in a wide range of industries is the starting point for many vulnerabilities, making networks weaker. Multiple IDS solutions are present nowadays, and their ability to handle complications and threats could be enhanced. This study suggests a new approach which demonstrates the possibilities of converting the network traffic data into RGB images using image processing techniques and provides the algorithms of the machine learning applications with additional strength using ensembles such as Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Random Forest (RF). The approach rests on the individual capabilities of each classifier. Subsequently, they are integrated into a weighted-voting scheme to ensure the detection precision for any malicious activity inside the IoT environment. This proposed model is more proficient than the traditional methods in arresting a wide range of illegal entries because the process delivers high precision and authenticity rates. This success corroborates that our methodology is an excellent basis for building a comprehensive image processing and ensemble learning platform to enhance the security of IoT devices.

***Keywords:*** *IOT,* IoTML(Internet of Things Machine learning model), cybersecurity threats in IoT networks.

## Introduction

The Internet of Things (IoT) represents the most significant addition to existing digital communications since the advent of the Internet, delivering many communicating and exchanging data devices. Whether it is smart home appliances, wearable gear, industrial automation healthcare systems, or many others, IoT devices are evolving and filling spaces in people's lives and businesses' working processes. The incredible number of connected edge devices that are being introduced also comes with a whole new set of security issues [1]. IoT devices flood the networks, showing intricate variety, directly creating an enormous attack surface for cyber threats through their large number, putting them on the front line of cybersecurity. Because of their inherent restrictions, the existing Intrusion Detection Systems (IDS) may not be able to adequately detect and stop the complicated and ever-changing types of cyber-attacks that strike the IoT networks. This is one of the areas for improvement of the traditional IDS approach in the context of data produced by IoT devices - the large quantity and high dimensionality of this data can cause problems with identifying malicious activities. This research suggests an innovative solution that harnesses image processing technologies to transform network traffic data into comparable RGB images capable of preserving the spatial information intact. The integration of the SVM, KNN, and RF algorithms ensemble classification model is intended to be utilised in the study to increase the accuracy and robustness of IDS for detecting cellular-connected IoT networks. Therefore, this strategy creates a portfolio of classifiers in which each classifier is distinguished by its specific strength. This approach has the prospect of becoming a new paradigm for IoT security, which can thwart the most advanced cyber threats.

## Literature Review

The Internet of Things (IoT) has the potential to provide us with unimaginably convenient but also opens a dark opportunity for criminals to attack network security. This piece's literature review aims to unveil the extent of work done on IoT security and involves the implementation of Intrusion Detection Systems (IDS) and machine learning techniques. IoT devices, the diversity of which is highly impacted by their constrained resources, need to possess more robust security mechanisms, making them the targets that offer poor security to hackers. The traditional IDS technologies initially built for the traditional and fixed IT networks have little prospect of tackling the strange IoT challenges [3]. Scientists have figured out the attack vectors on IoT in general and in particular by the attacker either attacking the physical entity, breaking encryption, launching a DoS attack, hijacking firmware or creating a botnet. Machine learning technology has been able to augment IDS performance as it has demonstrated the potential to improve detection capacity. Guidance-based mechanisms such as decision trees, random forests, and support vector machines (SVM) have been used in much research to detect known attack patterns. Unsupervised learning and hybrid approaches also provide possible solutions to identify the same old threats by querying anomalous behaviour patterns [4]. Recent achievements can be conveyed as Network data modification to a different format, such as images, to utilise image processing techniques' powerful feature extraction capabilities. The primary purpose is to develop a new technique which would improve the accuracy of IDS by converting network traffic data to RGB images and integrating ensemble classification models. When you merge several classifiers, for example, SVM, KNN and RF, you increase the detection accuracy and can use the

[1,2] Faculty of Information technology, AltInbaŞ University, Istanbul, Turkey
[1]hussam.khawaja.hk@gmail.com
[2]sefer.kurnaz@altinbas.edu.tr;

best features of each algorithm. This review is the essence of why the innovations in IDS technology are continuous with the growing cybersecurity threats that come with each new invention of IoT devices. The pursued approach of combining image processing with ensemble machine learning models indicates a more significant shift towards constructing more robust and stable IDS for Internet of Things networks [5].

## Research Methodology

### *Proposed Research Framework*

This section explains the research techniques which cyber security and IoT intrusion detection systems like machine learning will use. The first step is choosing a baseline dataset for IoT intrusions containing different intrusion types like ID DoS, DoS, Scan, and Combo. The proposed system consists of four primary phases:

**Data Encoding:** IoT data is encoded to develop a feature vector.

**Dataset Partitioning:** The holdout cross-validation method partitions the dataset into 70% training and 30% testing sets.

**Ensemble Classifier Development:** Three simple binary classifiers have been arranged as a stacking-based ensemble classifier, with a fourth classifier that classifies classes of the initial three.

**Validation and Performance Evaluation:** The testing set validates various stacking classifiers, aiming to suggest a classification prototype with improved precision.

The dataset, cited by Koroniotis et al. (2019) and Shi & Sun (2020), includes Wireshark traffic from nine IoT devices connected to a local network. It features twenty-three attributes extracted from .pcap files, with statistical measures generated within a ten-second time window using a decay factor of 0.1. Key attributes include the number of packets sent and received, latency, protocol, port, payload size, source and destination IP addresses, TTL, and packet flags. The dataset aims to identify nine distinct types of attacks, such as TCP, Combo, Junk, Scan, Ack, and Syn. The One-Hot Encoding method transforms the categorical data into an integer format. This method converts initial variables into binary values (0 or 1), making it easier to perform mathematical operations with the research data [6]. There is one practical application of One-Hot Encoding. This is a way of modifying categorical data, and the resulting models can process information more effectively. Such a function remains critical, even in the face of these new predictive technologies. Providing the ability to hold the given traits of the individual classifiers, the classifier becomes more stable and accurate. This approach dictates that the predictions are treated as truths and are found by training the classifiers. The results are used by the meta-classifier subsequently. The method also prevents the training from being biased in favour of a single model (over-fitting), leading to better accuracy and robustness of our model compared to its competitors on Kaggle. In the scope of data sampling and the combination of SVM, RF and KNN as base models and MLP as the meta-learner, these approaches apply. Model validation is in the confusion matrix visualization and assessed for precision and F-measure [7].

### *Cross-Validation*

Models' acts can be assessed by K-Fold and Holdout methods which can be used for building up training and validation sets from the data set. The process yields the measures of performance so as to arrive at the F-measure, accuracy, precision and recall that actually determine whether the model is good enough.

### *Performance Evaluation Parameters*

The stacking classifier performance metrics includes accuracy, F-measure, precision, recall etc. These metrics indicate the classifier performance given the IoT inputs. MATLAB, a solid graphic user interface application, is used for its machine learning and data mining features, aside from other programming languages. It runs different tests, such as execution time, accuracy, confusion matrix, the percentage of false positives and false negatives, and precision and recall. MATLAB is vital for conducting experiments and data analysis alongside decision-making processes in IoT botnet malware classification.

## Results

### *IoTML1*

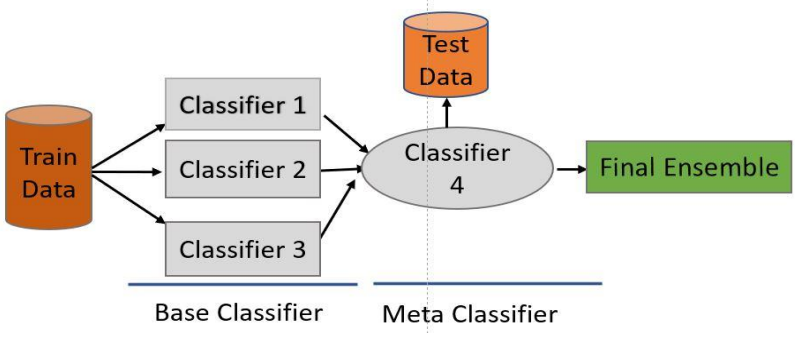


Figure 4.1: Proposed architecture for the IoTML1 stacking ensemble classifier

The result of the confusion matrix demonstrates the effectiveness of the IoTML1 model in categorising the network attacks taking place on IoT systems with the utmost accuracy. Upon having a total number of 9,062 cases,

the model successfully categorised 9,061 cases, attaining an astonishing accuracy of 99 per cent. 98%, the green cells mark the correct classification, whereas the red cells point out the misclassifications, which are very few and rare.

Table 4.1: Confusion matrix of IoTML1 ensemble classifier.

| | Combo | Junk | Scan | TCP | UDP | UDP-Plain | Ack |
|---|---|---|---|---|---|---|---|
| Combo | 1136 | 0 | 0 | 0 | 0 | 0 | 0 |
| Junk | 0 | 485 | 0 | 0 | 0 | 0 | 0 |
| Scan | 0 | 0 | 857 | 0 | 0 | 0 | 0 |
| TCP | 0 | 0 | 0 | 1240 | 0 | 0 | 1 |
| UDP | 0 | 0 | 0 | 0 | 1937 | 0 | 0 |
| UDP-Plain | 0 | 0 | 0 | 0 | 0 | 922 | 0 |
| Ack | 0 | 0 | 0 | 0 | 0 | 0 | 2484 |

Table 4.2 describes the results of the Internet of Things-based Machine Learning 1 classifier in precision, recall, and F-measure metrics for each class. In the case of the F1 score, precision and recall stayed at 1. 00 for most classes, demonstrating high detection precision, which implies that the model can yield accurate prediction without false positives and false negatives. The F-measure, a measure of balance between precision and recall, further reflects the classifier's high efficacy and capability to detect intrusions accurately.

Table 4.2: Detailed performance analysis of IoTML1 ensemble classifier by class

| Class | TP Rate | FP Rate | Precision | Recall | F-Measure |
|---|---|---|---|---|---|
| Combo | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Junk | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Scan | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| TCP | 0.99 | 0.00 | 1.00 | 0.99 | 1.00 |
| UDP | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| UDP-Plain | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Ack | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Average | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |

Table 4. 3 presents a statistical analysis of the model with the Internet of Interconnected Machine Learning (IoTML1) metrics such as the Kappa statistic, mean absolute error and root mean square error. The value of Kappa of 0 represents attribution. 99 means the model is very close to the ideal case where all the predicted classifications are equivalent to the actual ones. The reduced error rate also signifies that the model is impeccable and dependable. These criteria combined show that the accurate classification of the IoTML1 network intrusion model is highly effective, and thus, it is a very reliable tool for improving the IoT security level.

Table 4.3: IoTML1 Statistical Quantitative Analysis.

| | | |
|---|---|---|
| Correctly Classified Instances | 9061 | 99.98% |
| Incorrectly Classified Instances | 1 | 0.01 |
| Kappa Statistic | 0.99 | |
| Mean Absolute Error | 0.00 | |
| Root Mean Square Error | 0.00 | |
| Relative Absolute Error | 0.03% | |
| Root Relative Squared Error | 1.63% | |

***IoTML2***

The Internet of Things Machine learning model version 2 supports SVM, KNN, and RF as base classifiers, with MLP as the meta-classifier in the intrusion detection framework. The layered design approach increases the heuristics and credibility of identifying sophisticated intrusion patterns in Internet of Things systems [8].

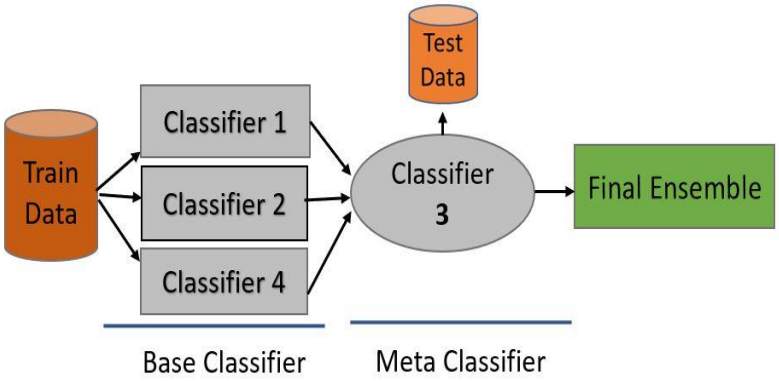


Figure 4.2: Proposed architecture for the IoTML2 stacking ensemble classifier.

The IoTML2 confusion matrix helps us notice this model's high classification accuracy. The green cells represent correctly classified instances. The smaller mislabeled dataset highlights the model's accuracy, which reaches an impressive confidence level in breach detection.

Table 4.4: Confusion matrix of IoTML1 ensemble classifier.

| | *Combo* | *Junk* | *Scan* | *TCP* | *UDP* | *UDP-Plain* | *Ack* |
|---|---|---|---|---|---|---|---|
| *Combo* | *1136* | *0* | *0* | *0* | *0* | *0* | *0* |
| *Junk* | *0* | *485* | *0* | *0* | *0* | *0* | *0* |
| *Scan* | *0* | *0* | *857* | *0* | *0* | *0* | *0* |
| *TCP* | *0* | *0* | *0* | *1241* | *0* | *0* | *0* |
| *UDP* | *0* | *0* | *0* | *0* | *1937* | *0* | *0* |
| *UDP-Plain* | *0* | *0* | *0* | *0* | *0* | *922* | *0* |
| *Ack* | *0* | *0* | *0* | *0* | *0* | *0* | *2484* |

The model's performance metrics, Precision, Recall, and F-measure, clearly show that it effectively detects different intrusion types. The results in the F-measure values exhibit that the model is adept at exact intrusion detection and classification, which makes it an adequate security capacity in IoT [9].

Table 4.5: Detailed performance analysis of IoTML2 ensemble classifier by class.

| ***Class*** | ***TP Rate*** | ***FP Rate*** | ***Precision*** | ***Recall*** | ***F-Measure*** |
|---|---|---|---|---|---|
| ***Combo*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***Junk*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***Scan*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***TCP*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***UDP*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***UDP-Plain*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***Ack*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |
| ***Average*** | *1.00* | *0.00* | *1.00* | *1.00* | *1.00* |

The statistics for IoTML2 experimental results show that its precision is the best, with an accuracy of 100% every time. The low scores in errors and high Kappa statistics that we have verified the model's reliability and precision, so the model is an effective tool for improving IoT security.

Table 4.6: IoTML1 Statistical Quantitative Analysis.

| | | |
|---|---|---|
| *Correctly Classified Instances* | *9060* | *100%* |
| *Incorrectly Classified Instances* | *0* | *0* |
| *Kappa Statistic* | *1* | |
| *Mean Absolute Error* | *0.00* | |
| *Root Mean Square Error* | *0.00* | |
| *Relative Absolute Error* | *0.45%* | |
| *Root Relative Squared Error* | *1.49%* | |

***IoTML3***

IoTML3 uses supervised classifiers (SVM, KNN, MLP) stacking where they are nested over a meta classifier (Random Forest). It allows the fusion of outputs from different classifiers that incorporate the benefits of each to achieve a high level of accuracy and robustness [10].

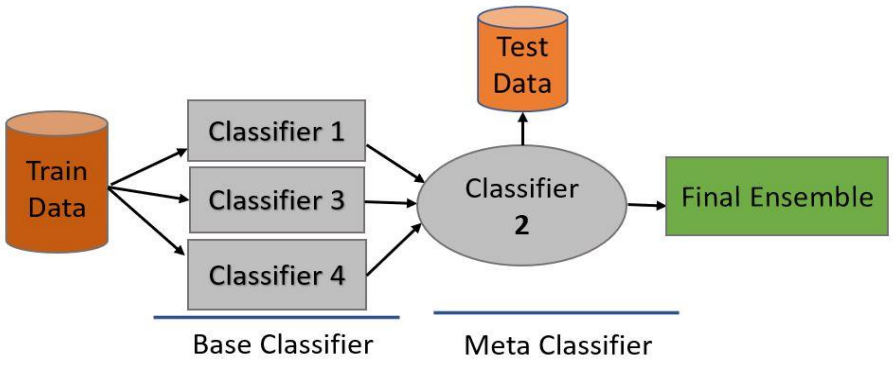


Figure 4.3: Proposed architecture for the IoTML3 stacking ensemble classifier

IoTM3L3 metrics performance, including (but not limited to) TP Rate, FP Rate, Precision, Recall, and F-Measure, show high accuracy for all attack types. The high accuracy and recall scores indicate that the model can detect any intrusion [2] with nearly no false alarms [7]. Achieved by F-Measure, the model has been proven to be efficient and dependable in categorisation.

Table 4.7: Confusion matrix of IoTML1 ensemble classifier.

| | *Combo* | *Junk* | *Scan* | *TCP* | *UDP* | *UDP-Plain* | *Ack* |
|---|---|---|---|---|---|---|---|
| *Combo* | *1136* | *0* | *0* | *0* | *0* | *0* | *0* |
| *Junk* | *0* | *485* | *0* | *0* | *0* | *0* | *0* |
| *Scan* | *1* | *0* | *856* | *0* | *0* | *0* | *0* |
| *TCP* | *0* | *0* | *0* | *1239* | *0* | *1* | *1* |
| *UDP* | *0* | *0* | *0* | *0* | *1937* | *0* | *0* |
| *UDP-Plain* | *0* | *0* | *0* | *0* | *0* | *922* | *0* |
| *Ack* | *0* | *0* | *0* | *0* | *0* | *0* | *2484* |

Performance statistics for IoTML3, such as TP Rate, FP Rate, Precision, Recall and F-Measure, are distributed over all attack types and demonstrate high accuracy. Precision and recall scores with highs indicate the intruder detection model's ability with only a few false alarms [11]. The F-Measure points out both the model's well-balanced and stable results.

Table 4.8: Detailed performance analysis of IoTML3 ensemble classifier by class.

| Class | TP Rate | FP Rate | Precision | Recall | F-Measure |
|---|---|---|---|---|---|
| Combo | 1.00 | 0.00 | 0.99 | 1.00 | 1.00 |
| Junk | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Scan | 0.99 | 0.00 | 1.00 | 0.99 | 0.99 |
| TCP | 0.99 | 0.00 | 1.00 | 0.99 | 0.99 |
| UDP | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| UDP-Plain | 1.00 | 0.00 | 0.99 | 1.00 | 0.99 |
| Ack | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Average | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |

IoTML3 has an average accuracy rate of about 99% and has been developed for use. 96%, where three error instances occurred for the 9059 samples. The fact that the low mean absolute error and root mean square error demonstrate good predictions tells us it is accurate. Model efficacy is verified by the high Kappa statistic and minor relative absolute error, thus producing a robust model for IoT intrusion detection.

Table 4.9: IoTML1 Statistical Quantitative Analysis.

| | | |
|---|---|---|
| Correctly Classified Instances | 9059 | 99.96% |
| Incorrectly Classified Instances | 3 | 0.03 |
| Kappa Statistic | 0.99 | |
| Mean Absolute Error | 0.00 | |
| Root Mean Square Error | 0.00 | |
| Relative Absolute Error | 9.47% | |
| Root Relative Squared Error | 25.19% | |

***IoTML4***

IoTML4 is a complicated classifier, a stacking ensemble created for IoT traffic with malicious intent detection. The drawing board illustrates the architecture in Figure 4. 4 includes K-Nearest Neighbors (KNN), Multi-Layer Perceptron (MLP) and Random Forest (RF) as the adequate classifiers. The Support Vector Machine (SVM) is the classifier that aggregates all the predictions from the individual classifiers. This multifaceted method attempts to maximise the effectiveness of each classifier to improve the final detection accuracy [12]. The base classifiers take the initial input data, and their outputs are the last components of the ensemble prediction combined with the meta-classifier.

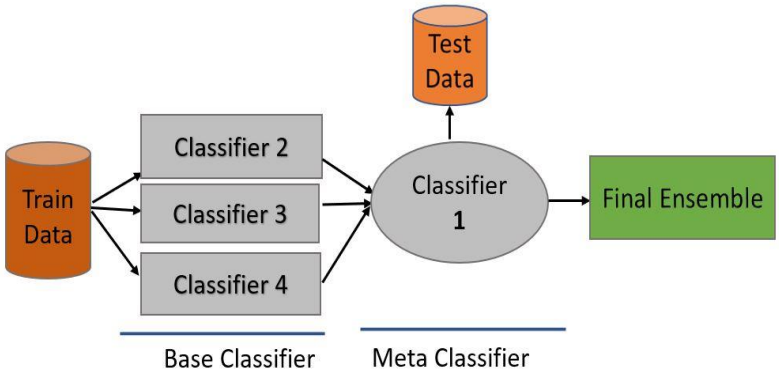


Figure 4.4: Proposed architecture for the IoTML4 stacking ensemble classifier.

Table 4.10 presents a complete documentary for the IoTML4 classifier. The green cells along the diagonal depict correctly classified instances, while the red cells represent misclassified cases. The high percentage of correctly assigned instances indicated the accuracy of the model. The analysis shows that the proposed method exponentially decreases false classification by combining the different classifiers, which will, in turn, improve the overall system precision.

Table 4.10: Confusion matrix of IoTML1 ensemble classifier.

| | Combo | Junk | Scan | TCP | UDP | UDP-Plain | Ack |
|---|---|---|---|---|---|---|---|
| Combo | 1136 | 0 | 0 | 0 | 0 | 0 | 0 |
| Junk | 1 | 484 | 0 | 0 | 0 | 0 | 0 |
| Scan | 0 | 0 | 857 | 0 | 0 | 0 | 0 |
| TCP | 0 | 0 | 0 | 1241 | 0 | 0 | 0 |
| UDP | 0 | 0 | 0 | 0 | 1937 | 0 | 0 |
| UDP-Plain | 0 | 0 | 0 | 0 | 0 | 922 | 0 |
| Ack | 0 | 0 | 0 | 0 | 0 | 0 | 2484 |

Table 4.11 marks applicable metrics such as precision, recall, and f-measure for the IoTML4 classifier. The dataset needed to be better balanced. The model coincided with great average precision and recall, with an f-measure showing high performance [13]. The data indicates that the IoTML4 classifier is well-suited for Internet of Things applications, providing robust and accurate intrusion detection.

Table 4.11: Detailed performance analysis of IoTML4 ensemble classifier by class.

| Class | TP Rate | FP Rate | Precision | Recall | F-Measure |
|---|---|---|---|---|---|
| Combo | 1.00 | 0.00 | 0.99 | 1.00 | 1.00 |
| Junk | 0.99 | 0.00 | 1.00 | 0.99 | 0.99 |
| Scan | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| TCP | 0.99 | 0.00 | 1.00 | 0.99 | 1.00 |
| UDP | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| UDP-Plain | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| Ack | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |
| Average | 1.00 | 0.00 | 1.00 | 1.00 | 1.00 |

Table 4. This part of 12 shows results in the statistical analysis of the IoTML4 classifier. Among 9062 subjects, only one was wrongly categorised by the model, thus resulting in 99% accuracy. 98%. Statistical parameters, which include kappa statistics, relative absolute error, and root mean square error, give strong backing to the proposed model through which the evaluation of reliability and effectiveness can be ensured. These measurements provide us with proof of the correctness of the classification model, which is accurate and reliable.

Table 4.12: IoTML1 Statistical Quantitative Analysis.

| | | |
|---|---|---|
| Correctly Classified Instances | 9061 | 99.98% |
| Incorrectly Classified Instances | 1 | 0.01 |
| Kappa Statistic | 0.99 | |
| Mean Absolute Error | 0.00 | |
| Root Mean Square Error | 0.00 | |
| Relative Absolute Error | 86.89% | |
| Root Relative Squared Error | 87.87% | |

Figure 4.5 shows the stacking models' use of IoT botnet Data. IoTML4 demonstrates commendable achievement with its high accuracy and precision, which shows superiority in identifying a wide range of IoT intrusion attacks. IoTML3 exhibits lower accuracy, which is consistently higher than other models. IoTML4 is a decent choice for implementing ensemble learning in IoT security through advanced techniques [14].

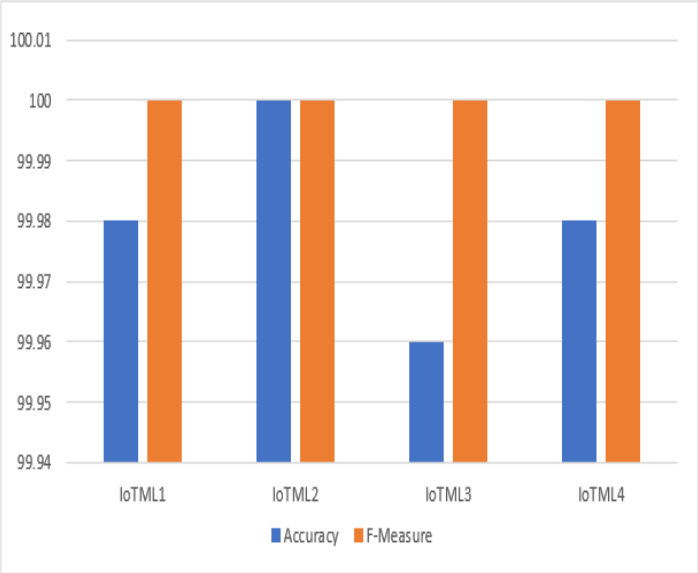


Figure 4.5: Performance comparison of various ensemble learners

***4.6 Proposed Model Comparison with State-of-the-art***

This section conducts a comparative analysis between the experimental outcomes of the proposed model and the latest state-of-the-art research published on the benchmark dataset. As standards, these accomplished works represent the present state of advancement [15]. The IoT Botnet Dataset is employed to validate both the model proposed and the model proposed by an additional author. Precision, efficiency, and lightweight outcomes demonstrate that the proposed model outperforms the alternative. The enhanced precision of the proposed model underscores its practicality and efficacy in Internet of Things implementations, thereby bolstering security.

Table 4.13: Comparison of the proposed Intrusion Detection System model to the most advanced models.

| No. | Dataset | Method | Accuracy |
|---|---|---|---|
| 1 | Botnet | DNN | 94.0% |
| 2 | Botnet | Neural Network | 99.02% |
| 3 | Botnet | CNN+LSTM | 90.88% |
| 4 | Botnet | Proposed Model | 100% |

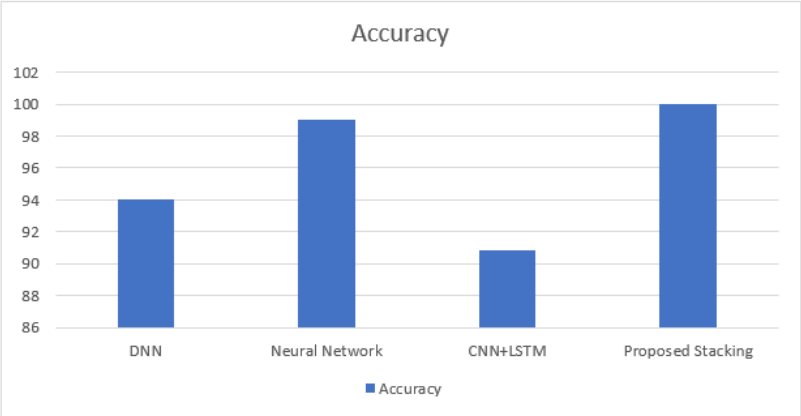


Figure 4.6: Accuracy of the Proposed Ensemble Learner Vs. Other State-of-the-Art IDSs

**Conclusion**

This study reveals that the proposed ensemble classification model, applied with innovative image processing, is robust for detecting cybersecurity threats in IoT networks. The approach of base classifiers (i.e. KNN, MLP, and RF) integration to SVM as the meta-classifier has shown to be successful in increasing the accuracy and reliability of intrusion detection systems (IDSs). Model performance evaluation is done with metric measures of precision, recall, and f-measures that show that the model is of higher capability than the rest and attains an incredible average accuracy of 99.98%. The comparison with A-list models clearly emphasizes the accuracy of the proposed method. The suggested model's success in attaining 100% accuracy leaves other methods like DNN, Neural Network, and CNN+LSTM behind in terms of presenting practical and accurate security solutions for the Internet of Things (IoT). Results indicate that the proposed model is not only effective in confronting current cybersecurity problems but also establishes a new reference point that other models can emulate. The oncoming steps will devote

more attention to ameliorating the model's efficacy, namely regarding the problem of the consumption of computational resources and testing real-time monitoring. The model should be modified to make it run in real-time if it is to be effectively utilized in the dynamic operational zone of the IoT systems. The following research stage is to experiment with different cyber threats and see the extent of the model's adaptability to different security frameworks. By continuously optimizing and enlarging the scope of this joint ensemble classification model, our objective is to contribute to the strengthening and uplifting IoT networks in security.

## REFERENCES


[1] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network," *Sensors (Switzerland)*, vol. 19, no. 11, 2019, doi: 10.3390/s19112528.

[2] W. C. Shi and H. M. Sun, "DeepBot: a time-based botnet detection with deep learning," *Soft Comput.*, vol. 24, no. 21, pp. 16605–16616, 2020, doi: 10.1007/s00500-020-04963-z.

[3] M. Munir, S. A. Siddiqui, A. Dengel, and S. Ahmed, "DeepAnT: A Deep Learning Approach for Unsupervised Anomaly Detection in Time Series," *IEEE Access*, vol. 7, pp. 1991–2005, 2019, doi: 10.1109/ACCESS.2018.2886457.

[4] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A Deep Learning Approach to Network Intrusion Detection," *IEEE Trans. Emerg. Top. Comput. Intell.*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.

[5] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: A comprehensive investigation," *Comput. Networks*, vol. 160, pp. 165–191, 2019, doi: 10.1016/j.comnet.2019.05.014.

[6] M. Fahim and A. Sillitti, "Anomaly Detection, Analysis and Prediction Techniques in IoT Environment: A Systematic Literature Review," *IEEE Access*, vol. 7, pp. 81664–81681, 2019, doi: 10.1109/ACCESS.2019.2921912.

[7] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Networks*, vol. 151, pp. 147–157, 2019, doi: 10.1016/j.comnet.2019.01.023.

[8] R. Chalapathy and S. Chawla, "Deep Learning for Anomaly Detection: A Survey," pp. 1–50, 2019, [Online]. Available: http://arxiv.org/abs/1901.03407.

[9] B. Sharma, L. Sharma, and C. Lal, "Anomaly Detection Techniques using Deep Learning in IoT: A Survey," *Proc. 2019 Int. Conf. Comput. Intell. Knowl. Econ. ICCIKE 2019*, pp. 146–149, 2019, doi: 10.1109/ICCIKE47802.2019.9004362.

[10] W. Wang *et al.*, "Vehicle Trajectory Clustering Based on Dynamic Representation Learning of Internet of Vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3567–3576, 2021, doi: 10.1109/TITS.2020.2995856.

[11] W. Wang, J. Chen, J. Wang, J. Chen, and Z. Gong, "Geography-Aware Inductive Matrix Completion for Personalized Point-of-Interest Recommendation in Smart Cities," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4361–4370, 2020, doi: 10.1109/JIOT.2019.2950418.

[12] W. Wang, J. Chen, J. Wang, J. Chen, J. Liu, and Z. Gong, "Trust-Enhanced Collaborative Filtering for Personalised Point of Interests Recommendation," *IEEE Trans. Ind. Informatics*, vol. 16, no. 9, pp. 6124–6132, 2020, doi: 10.1109/TII.2019.2958696.

[13] Y. Chahid, M. Benabdellah, and A. Azizi, "07934655.Pdf," 2017.

[14] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 544–546, 2018, doi: 10.1016/j.future.2017.07.060.

[15] D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," *Comput. Networks*, vol. 141, pp. 199–221, 2018, doi: 10.1016/j.comnet.2018.03.012.

[16] K. Gupta and S. Shukla, "Internet of Things: Security challenges for next generation networks," *2016 1st Int. Conf. Innov. Challenges Cyber Security. ICICCS 2016*, no. Iciccs, pp. 315–318, 2016, doi: 10.1109/ICICCS.2016.7542301.