

# Intrusion Detection in IoT Using Ensemble Approach

Elijah M. Maseno<sup>1</sup>, and Zenghui Wang<sup>2</sup>

<sup>1</sup> Department of Computer Science, University of South Africa, Florida 1709, South Africa

<sup>2</sup> Department of Electrical Engineering, University of South Africa, Florida 1709, South Africa

## Abstract

Protection of the Internet of Things (IoT) devices is an area of concern, even with the success that has been achieved in this area. IoT involves configuring and deploying smart devices to send and share information. Some IoT devices carry sensitive information, which attracts the attention of cybercriminals. Intrusion detection systems have been widely proposed as one measure of defending networks against any malicious activities. This work proposes a stacked ensemble intrusion detection technique based on extreme learning machine (ELM), support vector machine (SVM), and KNeighbors (KNN) classifiers as base learners, and logistic regression (LR) as the meta-learning algorithm. Firstly, the dataset is cleaned and then grouped using the cross-validation procedure. Secondly, hyperparameter tuning of the algorithms is done using the grid search technique. Finally, with the tuned parameters, the classification job is done. The evaluation of the model is performed using the IoT\_ToN network dataset. The performance of the proposed stacked ensemble method is compared with that of single algorithms. The obtained results clearly show the outstanding performance of the proposed stacked ensemble approach with respect to accuracy, precision, recall, and f1-score. The proposed model scored 96% across all the measured metrics outperforming the standalone algorithms. This study concludes that the stacked ensemble approach can potentially improve the performance of intrusion detection systems.

## Keywords

Intrusion detection system; stacked; genetic algorithm; IoT\_ToN network data set; ensemble learning

## 1. Introduction

Over the last decade, we have seen rapid growth in IoT devices [1][2]. These devices can send and receive information from people and things without human control. IoT technology is the reason behind the explosion of smart devices, which have been adopted in the health sector, industries, and farming, among other fields. According to [3] the number of interconnected devices in the IoT environment is expected to increase to around 41.6 billion by the year 2025. The exponential increase in integrated devices brings with it cyber security challenges. According to [4], IoT architecture has three layers: perception, network, and application. The researchers went a step further to outline the security issues affecting these layers.

An IoT innovation report by Deloitte [4] reported that hackers in 2013 took advantage of IoT-integrated devices, such as smart heating controls, ventilation systems, and air-conditioning systems in specific stores, and exposed 40 million credit card numbers from the U.S. retailer. In addition, the researchers reported an IoT attack, the 2016 Mirai attack, which brought the internet down in Europe and North America. According to the research, this caused the US to suffer almost USD 110 million in loss.


---

The 5th International Symposium on Advanced Technologies and Applications in the Internet of Things (ATAIT 2023), August 28-29, 2023, Kusatsu, Japan

✉ 13090879@mylife.unisa.ac.za (E. M. Maseno); wangzengh@mail.com (Z. Wang)

ORCID 0000-0001-5684-5043 (E. M. Maseno); 0000-0003-3025-336X (Z. Wang)

© 2023 Copyright for this paper by its authors.  
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0)

 CEUR Workshop Proceedings (CEUR-WS.org)

The integration of these devices into the wider internet has attracted the attention of cybercriminals [1][6]. Cybercriminals have shifted their focus to IoT devices as they offer easy entry to the larger network for exploitation. The diversity of integrated devices makes IoT devices more vulnerable to attacks and makes it hard to develop a single protection solution. Research done by [7], broadly classified IoT attacks into, physical attacks, network attacks, software attacks, and encryption attacks. The researchers admitted that, due to the unique nature of IoT, researchers should focus on developing security solutions that can be used to mitigate most security issues on IoT platforms. In addition, due to this peculiarity, traditional intrusion detection systems cannot effectively and efficiently be used to defend IoT devices against malicious activities.

According to researchers, most traditional intrusion detection approaches lack the ability to protect IoT devices [1][8]. The traditional approaches can be broadly classified as anomaly and signature based. The mentioned approaches have the problem of high false alarm rates (FARs) and inadequate detection of zero-day attacks respectively [8]. To make the IoT environment more secure, there is a need for the development of more advanced intrusion detection systems with learning capabilities. To achieve this aim, researchers have proposed the adoption of machine learning algorithms to improve the security of IoT devices [9]. The use of single-machine algorithms in model development is becoming limited in solving evolving problems [10][11]. The researchers have proposed integrating different machine algorithms to develop more powerful models capable of dealing with emerging issues effectively.

The ensemble method is one of the most recommended methods for integrating machine learning algorithms [12] [13] [14]. Ensemble learning is a technique for combining several machine learning algorithms together to solve a given task. One of the early research projects in this area was published in the early 1990s by Hansen and Salamon [15], the researchers observed that the combination of several classifiers had the potential to perform better than a single classifier. This technique has been applied to solve problems in different fields such as, but not limited to, biometrics [16], power systems [17][18], seizure detection [19], and intrusion detection systems [20][21]. In this study, an ensemble approach is proposed for intrusion detection in the IoT environment.

The development of the ensemble model consists of two major components, namely, base learners and ensemble integration [22][23][24]. The first phase involves the combination of several learning algorithms. This can be achieved either by using different learning algorithms to form 'heterogeneous' base learners or by using the same learning algorithm to form 'homogeneous' base learners. The second phase is ensemble integration, which involves integrating the base learner's output to generate the final output.

The ensemble's performance is as good as the base learners, [23], which suggests that the base learners should be as correct and diverse as possible. Diversity becomes a major issue when a single learning algorithm is applied as a base learner, this can be attributed to the similarity of the learning algorithm. Several techniques have been proposed to achieve diversity in the homogenous ensemble; these include, but are not limited to, input data manipulation, feature subsets, and hyperparameter tuning. On the other hand, diversity is not a major issue in the heterogeneous ensemble due to the different structures of the base learners, which inform their learning process. Due to this advantage, this research focused on the development of heterogeneous ensemble models. A systematic review study done by [24] pointed out a great interest among researchers in the heterogeneous ensemble.

The two major techniques used for the creation of heterogeneous ensembles are stacking and voting [10][24]. This study focused on the development of a stacked ensemble due to its promising potential for improving the efficiency and effectiveness of intrusion detection systems [25]. This paper integrated extreme learning machine (ELM), support vector machine (SVM), and KNeighbors classifiers as base learners and logistic regression as the meta-learning algorithm. Research shows that traditional machine learning algorithms can achieve strong results. This research proves that classical machine learning algorithms achieve high performance.

The rest of the paper is organized as follows: Section 2 of the paper explains earlier works related to the current research. Section 3 gives the proposed work, Section 4 describes the experiments, and Section 5 gives the result discussions. Lastly, Section 6 concludes the paper with a discussion of the contributions and prospects for future work.

## 2. Related work

According to [26], the construction of good ensemble classifiers is an area of interest to many researchers. Several studies have been done on the integration of machine learning algorithms to improve accuracy and reduce the false alarm rate of intrusion detection systems. This section focuses on some of the existing works on this matter.

The study by [12], compared two hybrid ensemble techniques, namely, weighted voting-based AdaBoost ensemble and stacking-based ensemble. The researchers adopted Random Forest as the base learner in the weighted voting based AdaBoost ensemble, and the aggregation of the base learners was done through the weight voting method. On the other hand, different learning algorithms were adopted to develop the stacking-based ensemble. Evaluation of the model was done using the NSL-KDD and UNSW-NB15 datasets. According to this study, both techniques had a better detection rate and accuracy rate, with a low false alarm rate. In the future, the researcher proposed the development of a model for big data. In a similar approach [25], developed and analyzed the performance of different ensemble techniques such as stacking, XGBoost, CatBoost, RF, and deep feature extraction techniques in the detection of DDoS (distributed denial of service) attacks. The researchers concluded that stacking was among the top-performing ensemble methods. The study proposed the inclusion of other deep learning techniques in the future. In [27], researchers investigated the effectiveness of various anomaly intrusion detection techniques in imbalanced datasets. One of the techniques applied in this study is the stacked ensemble approach. On the stacked ensemble, the researchers used naïve bayes and OneR classifiers. The models were evaluated using an up-to-date dataset known as the CIDDS-001 dataset. This technique recorded an accuracy of 99.80%. The researchers strongly believe that the results of this study cannot be generalized, and that further research can be done on different problems.

Rajadurai and Gandhi [11] proposed the use of gradient boosting machine (GBM) and random forest (RF) algorithms as the base classifiers in the development of a stacked ensemble intrusion detection system for the wireless network. The motivation is that the existing individual classifiers are insufficient for network protection. The model is evaluated using a publicly available dataset known as NSL-KDD. The model had better performance compared to other models such as ANN (Artificial Neural Network), CART, random forest, and SVM. The model can be evaluated using another form of the dataset to verify its performance. In [28], several classification algorithms are stacked with support vector machine (SVM) for the intrusion detection system. In many studies, SVM has been categorized as one of the best classification algorithms. Despite these findings, the researchers conducted this study with the aim of increasing its effectiveness. SVM is combined with different algorithms, such as BayesNet, AdaBoost, Logistic, IBK, J48, RandomForest, JRip, OneR, and SimpleCart. to form the base learners. When tested using the NSL-KDD\_99 dataset, SVM and RF recorded the best accuracy of 97.50%, which is above all other combinations, as well as individual SVM, which has an accuracy of 91.81%. The study focused only on anomaly detection.

Research done by [29] proposed adaBoost, bagging, and stacking ensemble techniques with different feature selection techniques for intrusion detection. In the first phase of this work, the research applies different feature extraction techniques such as Cfs, Chi-square, SU, Gain Ratio, Info Gain, and OneR to reduce the number of features. The obtained optimal feature subset is used as input to the above-mentioned ensemble techniques. The results show that AdaBoost improves classification accuracy. In the future, other classifiers can be adopted as base learners. The researchers [30], combined Ordering Points to Identify the Clustering Structure (OPTICS) and ensemble learning for database intrusion detection. All the database transactions are passed through OPTICS for clustering. The generated outliers are passed through the ensemble models. The three ensemble methods applied in this study are bagging, boosting, and stacking. The researchers adopted Naïve Bayes, Decision Tree (DT), Rule Induction (RI), k-Nearest Neighbor (k-NN), and Radial Basis Function Network (RBFN) as base classifiers. These classifiers were tested in different combinations as both base classifiers and meta classifiers. According to the researchers, the adoption of RBFN as a meta-classifier and the rest as the base classifiers in the stacking ensemble had a better performance compared to all other ensembles. The authors [31] compared the performance of boosting, bagging, and stacking. J48 and instance-based

knowledge (IBk) classifiers are used as the base learners, while the logistic regression algorithm is used as a meta classifier. With J48 as the base classifier in the boosting ensemble, it proved to be the best classification technique.

The authors in [32] proposed the use of ensemble learners to be adopted as the base learners in the development of a stacked ensemble for anomaly intrusion detection in a web environment. Some of the proposed base learners are random forest, gradient boosting machines, and XGBoost. The model was evaluated using different datasets, namely CSIC-2010v2, CICIDS-2017, NSL-KDD, and UNSWNB15. According to the researchers, the model scored a good accuracy and false positive rate (FPR). The researchers proposed the inclusion of more intrusion datasets and the adoption of multi-class classification. Research by [33] proposed a semi supervised hierarchical stacking temporal convolutional network (HS-TCN) for anomaly detection in an IoT environment. The researchers saw that the hierarchical temporal convolutional network (H-TCN) had a weakness of poor labeling, which affected the performance of the classifier. To solve this issue, the researchers proposed the integration of H-TCN with the stacked ensemble. The main aim of the stacked ensemble is twofold: first, to assess the unlabeled dataset, and second, to remove any outliers. The researchers reported that the model was effective and efficient in anomaly detection in an IoT environment. In the future, the researchers recommended an improved version of the model. In this study, the researchers proposed anomaly intrusion detection in software-defined networks based on the stacked ensemble. In this study, NetFlow was used for data collection in real time. On the other hand [34], the researchers applied IGR for feature reduction. To develop the base learners, the researchers combined NB (Naive Bayes), GBT, random forest, W-BayesNet, W-DecisionStump, and LG classifiers and adopted the W-BayesNet learner as the meta classifier. According to the authors, the model had better performance compared to other existing methods. The authors in [35] applied the principle of evolution for the selection of best base classifiers in a stacked ensemble model for an intrusion detection system. In this work, the researchers applied a different type of stacked ensemble referred to as StackingC which applies probability in the choice of classifiers. Non-dominated Sorting Genetic Algorithm II (NSGA-II) was used in this study as the evolutionary algorithm. The model was evaluated using a modern dataset known as the ISCX2012 dataset. The evolved ensemble performed better than individual classifiers, but the choice of best base learners was dependent on the dataset. The researchers proposed further investigation on the idea of base learners selection on the bases of the dataset.

### **3. Proposed work**

With the existing hostile digital environment, single intrusion detection systems are not effective for intrusion detection in IoT environments. To solve this problem, this work integrates several machine algorithms using a stacked ensemble approach. The aim is to develop a superior intrusion detection system by using the strength of single-machine algorithms.

#### **3.1. Data Pre-Processing**

The TON\_IoT network dataset, which holds 461,043 records, is used for the evaluation of the model [36]. The dataset was adopted because it addresses the problems found in traditional intrusion detection datasets such as KDD-99 and NSL-KDD, which are outdated. In addition, they don't possess IoT sensor data, hence making them ineffective for the evaluation of modern intrusion detection systems. The researchers performed data cleaning by replacing missing values. Secondly, all categorical data was converted into a numerical format. Finally, IP (Internet Protocol) addresses and ports were dropped as per the suggestion made by [37].

#### **3.2. Stacked ensemble technique**

Stacking ensemble is a machine learning technique that aims to combine different machine algorithms to boost their performance. This approach combines different machine learning algorithms

as base learners, which improves generalization. The meta-learner finds the best way of dealing with the predictions from the base learners. The base learners are trained using the original training dataset. In this study, extreme learning machine (ELM), support vector machine (SVM), and K-neighbor classifiers will be used as the base learners, while logistic regression (LR) will be the meta-learner for classification using the predictions of the base learners, as shown in figure 1. The aim of the base learners is to perform the first predictions and produce a new set of data from the dataset. The goal of the meta-learner is to perform the final prediction using the output from the base learners. Algorithm 1 presents the pseudocode for the stacked ensemble with K-cross validation. The performance-stacked ensemble algorithm is as good as its individual algorithms. ELM was selected due to its proven classification performance. ELM is a single feed-forward neural network that was first proposed by Huang et al. in 2004 [38]. ELM has a fast-learning ability compared to other gradient-based algorithms. In addition, ELM has better generalization ability compared to other neural network algorithms [39]. SVM is a supervised classification algorithm widely used to solve problems in different fields, including intrusion detection. The major advantage of SVM is its generalization capability, even in high-dimensional datasets. In addition, SVM possesses the ability to handle high-dimensional datasets with low computational requirements [40]. Stacked ensemble methods are known to have high computational requirements if not professionally managed. KNN is regarded as one of the simplest supervised machine learning algorithms. The idea behind KNN is the assumption that similar things are found near each other. Training samples that are closely related are grouped together and marked as nearest neighbors." The new points are compared to the marked labels of K neighbors to be classified using majority voting. LR, on the other hand, is a machine-learning algorithm extensively used in binary classification [41]. This study applied LR to classify the dataset as either normal or malicious.

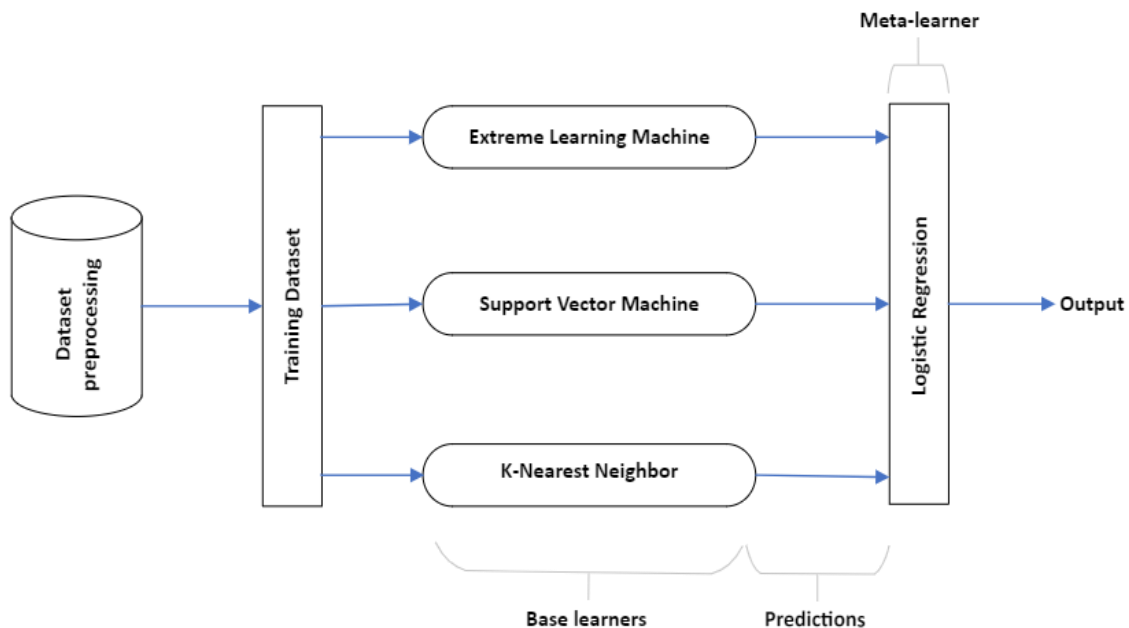


Figure 1. Stacked ensemble based on ELM, SVM, KNN, and LR

**Algorithm 1.** Stacked Ensemble with K-cross validation.

- 1: *Inputs: Training Dataset  $D:(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k)$  with Features  $f_1, f_2, \dots, f_k$*
- 2: Perform dataset preprocessing
- 3: Perform cross-validation on the training Dataset  $D: \{D_1, D_2, D_3, \dots, D_k\}$
- 4: Set the stacked ensemble
- 5: Base learners
- 6: Meta-learner

- 7: Apply the split dataset  $\{D_1, D_2, D_3, \dots, D_k\}$  into the base learners for  $K$  iterations
- 8: For each base learner get the prediction to form the new dataset:  $\hat{D}$
- 9: Apply the new Dataset  $\hat{D}$  into the meta-learner for classification
- 10: Output: normal or attack
- 11: End procedure

## 4. Experiments

This section presents the experimental implementation and significant results evaluations.

### 4.1. Experimental Setup

After data preprocessing, the training dataset was divided into 10-fold cross-validation to train the base learners. This is done to avoid overfitting the model. This procedure involves splitting the training dataset into 10 equal groups. One-fold can be used for validation, and the model is fit on the remaining  $k-1$  folds.

In this study, we adopted a grid search approach for hyperparameter tuning. Grid search is a technique that tries to find the best values of machine learning algorithms. It applies an exhaustive search to specific values of the algorithm. In this study, the goal was to get the best values of the parameters for each of the algorithms, as shown in Table 1.

**Table. 1**  
hyperparameter tuning.

Algorithm	Parameter
KNN	n_neighbors
SVM	max_iter
ELM	n_hidden
LR	C

To achieve the above, we used the following code:

```
params = {'knn__n_neighbors': [3,5,11,19,25],
         'svm__max_iter': list(range(10, 100,100)),
         'elm__n_hidden': list(range(100,200,300)),
         'final_estimator__C': [0.1, 10.0]}
```

The results were as follows for each parameter:

```
{'final_estimator__C': 0.1, 'knn__n_neighbors': 3, 'elm__n_hidden': 100, 'svm__max_iter': 10}
```

### 4.2. Performance Measure Indices

The metrics used to test the performance of the classifier were accuracy, precision, and recall. These four metrics are derived from five parameters: the true positive (TP), false positive (FP), false negative (FN), and true negative (TN) rates:

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

$$Precision = \frac{(TP)}{(TP + FP)} \quad (2)$$

$$Recall = \frac{(TP)}{(TP + FN)} \quad (3)$$

$$F1 = \frac{(2TP)}{(2TP + FP + FN)} \quad (4)$$

## 5. Results and Discussion

The researchers evaluated the models independently and compared the results with the stacked ensemble approach. Table 2 is the results of individual algorithms.

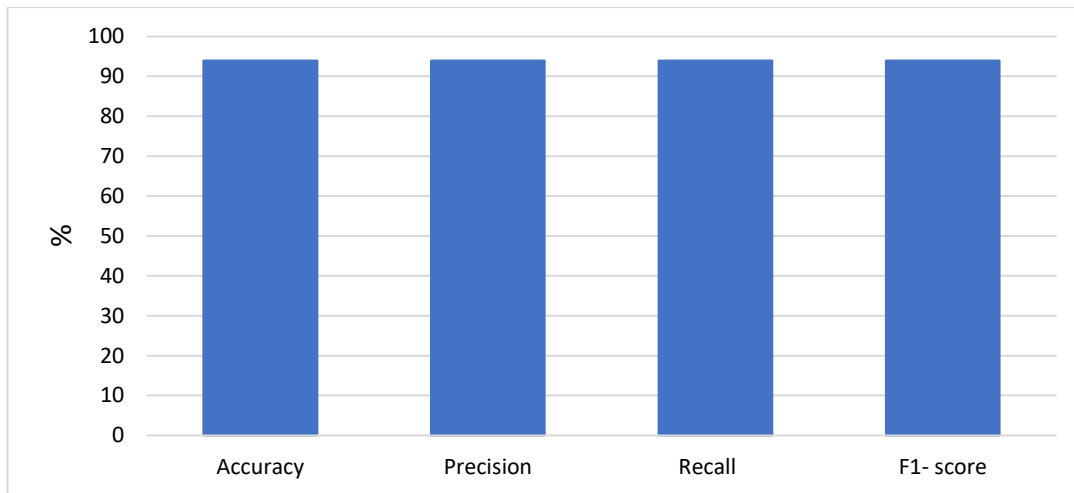
**Table 2**

Performance results of independent algorithms.

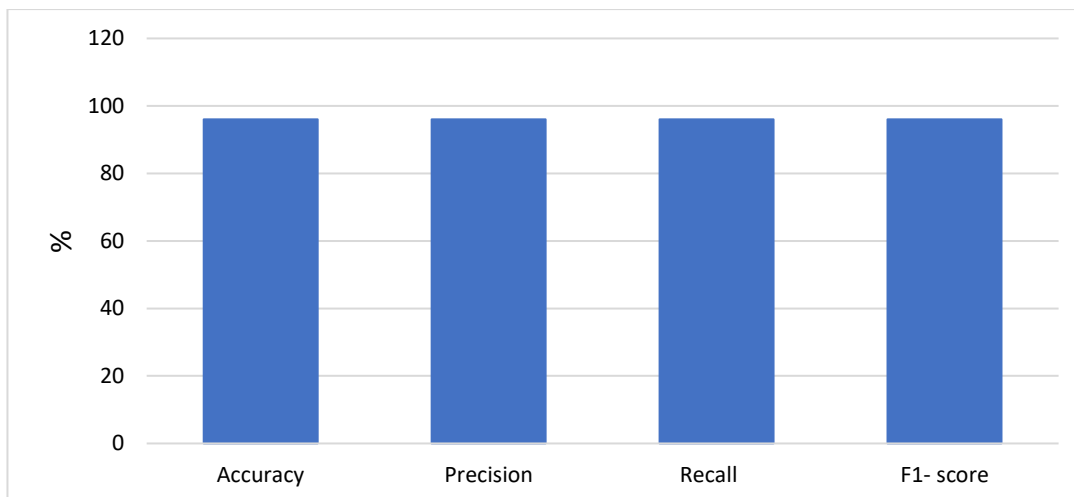
Algorithm	Accuracy%	Precision%	Recall%	F1 score%
KNN	95	95	95	95
SVM	88	89	88	87
ELM	56	79	56	66
LR	88	89	88	87

The researchers evaluated the performance of a stacked ensemble without hyperparameter tuning. The model had a constant performance of 94% across all the measured metrics, namely: accuracy, precision, recall, and F1-score, as shown in Fig 2.

The model had better performance with hyperparameter tuning compared to the single algorithms and the stacked ensemble without hyperparameter tuning. The tuned stacked ensemble scored 96% across all the measured metrics, as shown in Fig 3.



**Figure 2:** Performance of the stacked ensemble without hyperparameter tuning.



**Figure 3:** Performance of the stacked ensemble with hyperparameter tuning.

## 6. Conclusion

This study has explored the use of a stacked ensemble approach to combine multiple classifiers, i.e., extreme learning machine (ELM), support vector machine (SVM), K-neighbors, and logistic regression (LR), for intrusion detection in IoT devices. To prove the effectiveness and efficiency of the proposed model, we tested it using up-to-date IDS datasets, namely the TON\_IoT network dataset. Unlike the traditional stacking technique that usually considers weak individual classification algorithms, our proposed model is built based on a combination of strong classifier ensembles that work as base learners. To build the best machine learning algorithms, each learner undergoes hyperparameter tuning using the grid search approach. Our proposed approach yields better detection performance in terms of accuracy, precision, recall, and the F1- score measure. This study has several limitations, such as the use of one evaluation dataset, and focus on only one hyperparameter tuning. In the future, these areas can be further investigated for further improvement of the IDS.

## Acknowledgements

This research is partially supported by the South African National Research Foundation (Grant Nos. 132797 and 137951), the South African National Research Foundation incentive grant (No. 114911), and the South African Eskom Tertiary Education Support Programme.

## References

- [1] A. Abbas, M.A. Khan, S. Latif, M. Ajaz, A.A. Shah, & J. Ahmad, A New Ensemble-Based Intrusion Detection System for Internet of Things. *Arabian Journal for Science and Engineering*, 47(2) (2022) 1805–1819. doi:10.1007/s13369-021-06086-5.
- [2] O. I. Abiodun, E.O. Abiodun, M. Alawida, R. S. Alkhalaf, & H. Arshad, A Review on the Security of the Internet of Things: Challenges and Solutions. In *Wireless Personal Communications* Vol. 119, Issue 3 (2021). doi:10.1007/s11277-021-08348-9.
- [3] International Data Corporation. (2019). The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. Retrieved October 06, 2020, from <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>.
- [4] M. El-Hajj, A. Fadlallah, M. Chamoun, & A. Serhrouchni, A survey of internet of things (IoT) authentication schemes, *Sensors (Switzerland)*, 19(5), (2019). doi:10.3390/S19051141.
- [5] IoT innovative report. Deloitte, 2018. URL: <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/Internet-of-Things-Innovation-Report-2018-Deloitte.pdf>.
- [6] S. Zafar, K. M. Bhatti, M. Shabbir, F. Hashmat, & A. H. Akbar, Integration of blockchain and Internet of Things: challenges and solutions, *Annales Des Telecommunications/Annals of Telecommunications*, 77(1–2) (2022) 13–32. doi:10.1007/s12243-021-00858-8.
- [7] J. Deogirikar & A. Vidhate, Security attacks in IoT: A survey, In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017, pp. 32-37.
- [8] B. Gopalakrishnan, & P. Purusothaman, A new design of intrusion detection in IoT sector using optimal feature selection and high ranking-based ensemble learning model, *Peer-to-Peer Networking and Applications*, 15(5), (2022), 2199–2226. doi:10.1007/s12083-022-01336-1.
- [9] R. Malik, Y. Singh, Z. A. Sheikh, P. Anand, P. K. Singh, & T. C. Workneh, An Improved Deep Belief Network IDS on IoT-Based Network for Traffic Systems, *Journal of Advanced Transportation* (2022) 17. doi:10.1155/2022/7892130.
- [10] Y. Shen, K. Zheng, C. Wu, M. Zhang, X. Niu, & Y. Yang, An Ensemble Method based on Selection Using Bat Algorithm for Intrusion Detection, *Computer Journal*, 61(4) (2018) 526–538. doi:10.1093/comjnl/bxx101.



- [11] H. Rajadurai, & U. D. Gandhi, A stacked ensemble learning model for intrusion detection in wireless network, *Neural Computing and Applications*, 34(18) (2022) 15387–15395. doi:10.1007/s00521-020-04986-5.
- [12] G. Kaur, A comparison of two hybrid ensemble techniques for network anomaly detection in spark distributed environment, *Journal of Information Security and Applications*, 55(September) (2020) 102601. doi:10.1016/j.jisa.2020.102601.
- [13] O. Sagi, & L. Rokach, Ensemble learning: A survey. *Wiley Interdisciplinary Reviews, Data Mining and Knowledge Discovery*, 8(4) (2018) 1–19. doi:10.1002/widm.1249.
- [14] Y. Zhou, T. A. Mazzuchi & S. Sarkani, M-AdaBoost-A based ensemble system for network intrusion detection, *Expert Systems with Applications*, 162(August) (2020) 113864. doi:10.1016/j.eswa.2020.113864.
- [15] L. K. Hansen and P. Salamon, "Neural network ensembles," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 12, no. 10, (Oct. 1990) pp. 993-1001. doi: 10.1109/34.58871.
- [16] M. Choras, Ear Biometrics. In: Li, S.Z., Jain, A.K. (eds) *Encyclopedia of Biometrics*, Springer, Boston, MA (2015). doi:10.1007/978-1-4899-7488-4\_173.
- [17] M. Singh, & S. Chauhan, A hybrid-extreme learning machine-based ensemble method for online dynamic security assessment of power systems, *Electric Power Systems Research*, 214(PB) (2023) 108923. doi:10.1016/j.epsr.2022.108923.
- [18] M. Panthi, & T. Kanti Das, Intelligent Intrusion Detection Scheme for Smart Power-Grid Using Optimized Ensemble Learning on Selected Features, *International Journal of Critical Infrastructure Protection*, 39 (2022) 100567. doi:10.1016/j.ijcip.2022.100567.
- [19] S. Panda, S. Mishra, M. N. Mohanty, & S. Satapathy, Seizure detection using integrated metaheuristic algorithm based ensemble extreme learning machine, *Measurement: Sensors* 25 (2023) 100617. Doi:10.1016/j.measen.2022.100617.
- [20] O. Bukhari, P. Agarwal, D. Koundal, & S. Zafar, Anomaly detection using ensemble techniques for boosting the security of intrusion detection system, *Procedia Computer Science*, 218 (2023) 1003–1013. doi: 10.1016/j.procs.2023.01.080.
- [21] C. A. de Souza, C. B. Westphall, & R. B. Machado, Two-step ensemble approach for intrusion detection and identification in IoT and fog computing environments, *Computers and Electrical Engineering*, 98 (2022) 107694. doi:10.1016/j.compeleceng.2022.107694.
- [22] Y. Yang, H. Lv, & N. Chen, A Survey on ensemble learning under the era of deep learning. *Artificial Intelligence Review* (2022). doi:10.1007/s10462-022-10283-5.
- [23] Z-H. Zhou, Ensemble Learning. *Encyclopedia of Biometrics*, (2009) 270–273. doi:10.1007/978-0-387-73003-5\_293.
- [24] B. A. Tama, & S. Lim, Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation, *Computer Science Review*, 39 (2021) 100357. doi:10.1016/j.cosrev.2020.100357.
- [25] Y. Gormez, Z. Aydin, R. Karademir, & V. C. Gungor, A deep learning approach with Bayesian optimization and ensemble classifiers for detecting denial of service attacks, *International Journal of Communication Systems*, 33(11) (2020) 1–16. doi:10.1002/dac.4401.
- [26] T. G. Dietterich, Ensemble Methods in Machine Learning. In: *Multiple Classifier Systems*. vol 1857 of *Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, 2000. doi:10.1007/3-540-45014-9\_1.
- [27] R. Abdulhammed, M. Faezipour, A. Abuzneid & A. Abumallouh, Deep and Machine Learning Approaches for Anomaly-Based Intrusion Detection of Imbalanced Network Traffic, *IEEE Sensors Letters*, 3(1) (2019) 2–5. doi:10.1109/LSENS.2018.2879990.
- [28] N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, & M. C. Govil, A comparative analysis of SVM and its stacking with other classification algorithm for intrusion detection, in: *Proceedings - 2016 International Conference on Advances in Computing, Communication and Automation, ICACCA 2016*. doi:10.1109/ICACCA.2016.7578859.
- [29] H. P. Vinutha & B. Poornima, An ensemble classifier approach on different feature selection methods for intrusion detection, In *Advances in Intelligent Systems and Computing Vol. 672 2018*. doi:10.1007/978-981-10-7512-4\_44.

- [30] S. Subudhi, & S. Panigrahi, Application of OPTICS and ensemble learning for Database Intrusion Detection. *Journal of King Saud University - Computer and Information Sciences*, 34(3) (2022) 972–981. doi:10.1016/j.jksuci.2019.05.001.
- [31] S. Choudhury, & A. Bhowal, Comparative Analysis of Machine Learning Algorithms along with Classifiers for AF Detection using a Scale, 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, T.N., India., 2015, pp.89-95.
- [32] B. A. Tama, L. Nkenyereye, S. M. R. Islam, & K. S. Kwak, An enhanced anomaly detection in web traffic using a stack of classifier ensemble. *IEEE Access*, 8 (2020) 24120–24134. doi:10.1109/ACCESS.2020.2969428.
- [33] Y. Cheng, Y. Xu, H. Zhong, & Y. Liu, Leveraging Semisupervised Hierarchical Stacking Temporal Convolutional Network for Anomaly Detection in IoT Communication. *IEEE Internet of Things Journal*, 8(1) (2021) 144–155. doi:10.1109/JIOT.2020.3000771.
- [34] T. Jafarian, M. Masdari, A. Ghaffari, & K. Majidzadeh, Security anomaly detection in software-defined networking based on a prediction technique, *International Journal of Communication Systems*, 33(14) (2020) 1–23. doi:10.1002/dac.4524.
- [35] M. Milliken, Y. Bi, L. Galway, & G. Hawe, Multi-objective optimization of base classifiers in StackingC by NSGA-II for intrusion detection, 2016 IEEE Symposium Series on Computational Intelligence, SSCI 2016, 2017, pp. 8–15. doi:10.1109/SSCI.2016.7849977.
- [36] N. Moustafa, The TON\_IoT Datasets, 2020. URL:<https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cyberse%0Acurity/ADFA-ton-iot-Datasets/>
- [37] N. Moustafa, A new distributed architecture for evaluating AI-based security systems at the edge: Network TON\_IoT datasets. *Sustainable Cities and Society*, 72 (2021) 102994. <https://doi.org/10.1016/j.scs.2021.102994>
- [38] Huang, G. Bin, Zhu, Q. Y., & C. K. Siew, Extreme learning machine: A new learning scheme of feedforward neural networks. *IEEE International Conference on Neural Networks - Conference Proceedings*, 2, 2004, pp. 985–990. doi:10.1109/IJCNN.2004.1380068. 38
- [39] A. Alharbi, & M. Alghahtani, Using genetic algorithm and ELM neural networks for feature extraction and classification of type 2-diabetes mellitus, *Applied Artificial Intelligence*, 33(4) (2019) 311–328. doi:10.1080/08839514.2018.1560545.
- [40] C. C. Chang, & C. J. Lin, LIBSVM: A Library for support vector machines. *ACM Transactions on Intelligent Systems and Technology*, 2(3) 2011. doi:10.1145/1961189.1961199.
- [41] M. M. S. Raihan, A. B. Shams & R. B. Preo, Multi-Class Electrocardiogram (ECG) Signal Classification Using Machine Learning Algorithms. *ICCIT 2020 - 23rd International Conference on Computer and Information Technology, Proceedings*, 2020, pp.19–21. doi:10.1109/ICCIT51783.2020.9392695.