HEADS: hybrid ensemble anomaly detection system for Internet-of-Things networks.

AHMAD, Z., PETROVSKI, A., ARIFEEN, M., KHAN, A.S. and SHAH, S.A.

2024

HEADS: Hybrid Ensemble Anomaly Detection System for Internet-of-Things Networks

Zeeshan Ahmad[1(✉)], Andrei Petrovski[1], Murshedul Arifeen[1], Adnan Shahid Khan[2], and Syed Aziz Shah[3]

[1] National Subsea Centre, Robert Gordon University, Aberdeen, UK
{z.ahmad1,a.petrovski,m.arifeen}@rgu.ac.uk
[2] Faculty of CS and IT, Universiti Malaysia Sarawak, Kota Samarahan, Sarawak, Malaysia
skadnan@unimas.my
[3] Research Centre for Intelligent Healthcare, Coventry University, Coventry, UK
syed.shah@coventry.ac.uk

Abstract. The rapid expansion of Internet-of-Things (IoT) devices has revolutionized connectivity, facilitating the exchange of extensive data within IoT networks via the traditional internet. However, this innovation has also increased security concerns due to the presence of sensitive nature of data exchanged within IoT networks. To address these concerns, network-based anomaly detection systems play a crucial role in ensuring the security of IoT networks through continuous network traffic monitoring. However, despite significant efforts from researchers, these detection systems still suffer from lower accuracy in detecting new anomalies and often generate high false alarms. To this end, this study proposes an efficient Hybrid Ensemble learning-based Anomaly Detection System (HEADS) to secure an IoT network from all types of anomalies. The proposed solution is based on a novel hybrid approach to improve the voting strategy for ensemble learning. The ensemble prediction is assisted by a Random Forest-based model obtained through the best F1 score for each label through dataset subset selection. The efficiency of HEADS is evaluated using the publicly available CICIoT2023 dataset. The evaluation results demonstrate an F1 score of 99.75% and a false alarm rate of 0.038%. These observations signify an average 4% improvement in the F1 score while a reduction of 0.7% in the false alarm rate comparing other anomaly detection-based strategies.

Keywords: Anomaly Detection System · Ensemble-based learning · Gradient Boosting Machine · Internet-of-Things · Machine Learning

1 Introduction

The Internet-of-Things (IoT) has transformed a wide range of technological sectors, such as smart transportation, homes, healthcare, and logistics, to name a few [1]. IoT is an innovative computing paradigm consisting of a network of numerous IoT devices called “Things”. These devices are equipped with sensors, actuators, limited storage, and communication capabilities to exchange and share data over the traditional internet

[2]. However, the presence of the sensitive nature of data in IoT networks such as the health records of patients in the healthcare sector and the road safety information in the transportation domain, demands robust security measures. Different traditional security mechanisms such as firewalls, authentication methods, encryption schemes, etc. are employed as the first defensive shield against IoT anomalies. However, they are often insufficient to protect IoT against evolving anomalies (that are either novel or the mutation of an old anomaly). To enhance IoT security, intrusion detection systems (IDSs) can be deployed, that act as a second defensive shield against IoT network anomalies [3].

An IDS secures the IoT network by detecting anomalies through continuous network traffic monitoring for any suspicious behavior. IDS can be either host-based or network-based depending upon its deployment strategy. Additionally, It can be signature-based, anomaly detection-based, specification-based, or hybrid detection-based depending upon the type of detection scheme it adopts [4]. Our primary focus in this study is to propose a security solution for IoT networks based on a network-based IDS deployment strategy. This proposed methodology aims to secure the entry points of the IoT network by utilizing the anomaly-based detection strategy.

The rapid expansion of the IoT network has also led to a proportional increase in frequently evolving new anomalies. As a result, the performance of anomaly detection-based IDS methodology (AIDS) employing a network-based deployment strategy has observed a decline in detection accuracy and an increase in false alarm rates (FAR). The researchers have addressed these limitations by integrating artificial intelligence (AI) techniques such as machine learning (ML) and deep learning (DL) within AIDSs. AI-based AIDSs employ different ML schemes such as Decision Tree (DT), Random Forest (RF), Support Vector Machine (SVM), and Gradient Boosting Machine (GBM), among others. Further, the effectiveness of ML-based AIDS can be boosted through ensemble-based approaches, which combine learning from multiple models to enhance anomaly detection in IoT networks.

Ensemble approaches enhance the model's robustness by employing strategies such as bagging, boosting, and stacking [5]. Bagging involves training multiple models on different subsets of data and then combining their predictions to reduce variance and enhance generalization. Whereas, boosting utilizes an iterative process to adjust the weights of misclassified data points to improve the model's performance [6]. Also, stacking combines the predictions from different base models using a meta-learner, allowing the ensemble to utilize the strength of each individual model [7]. All these strategies enhance the performance and robustness of ensemble models by combining the predictive learning of base models.

Additionally, the final prediction of the ensemble methods is often drawn by utilizing the voting mechanisms such as hard and soft voting, that combine the predictions of all individual models [8]. In hard voting, each model's prediction is counted as an individual vote and the final prediction is based on majority votes. Whereas, in soft voting, the final prediction is derived based on the highest average probability of a label across all models [8]. The robustness of these ensemble methods by mitigating the model's overfitting makes them ideal for preventing IoT networks from all types of anomalies.

To this end, this study focuses on proposing an effective AIDS-based security solution for IoT networks by refining the voting strategy for ensemble learning.

The main contributions of this research are 3-fold. (1) To extensively discuss the state-of-the-art ensemble-based approaches for IoT networks. (2) To propose an efficient Hybrid Ensemble Anomaly Detection System (HEADS) by enhancing the voting strategies to improve anomaly detection in IoT networks. (3) To evaluate the performance of HEADS on the publicly available dataset CICIoT2023 [9] and compare its performance against various ML-based and ensemble AIDS methodologies.

The rest of the paper is organized as; Sect. 2 provides the state-of-the-art relevant work on ensemble-based AIDS methodologies for IoT networks. Section 3 details the preliminary concepts and the proposed methodology. Section 4 presents the dataset and experimental results with a discussion. Finally, Sect. 5 concludes this article.

2 Related Work

The researchers have widely explored ensemble-based techniques based on ML and DL methods to propose effective anomaly detection schemes for the IoT. This section discusses some notable ensemble-based IDSs proposed in the literature.

Cao et al. [7] proposed an efficient IDS strategy utilizing stacked ensemble learning models and the tree-structured Parzen estimator-based optimization method. The proposed model demonstrated superior performance, achieving an average accuracy rate of 99.99% on the N-BaIoT dataset and 99.37% on the UNSW-NB15 dataset. These results emphasize the model's potential to enhance the security of IoT networks.

Luo et al. [10] proposed an ensemble DL-based web attack detection system (EDL-WADS) designed to identify anomalous queries within IoT networks. They employed MRN, LSTM, and CNN models in parallel to generate intermediate vectors. These vectors are then fed into the comprehensive check and an MLP model, that acts as an ensemble classifier to combine all intermediate vectors to make the final decision. The proposed solution is evaluated on the synthetic dataset. The results showed demonstrated the model's efficiency by achieving an accuracy of 99.47%.

Alghanam et al. [11] proposed an enhanced pigeon-inspired optimization approach for the feature selection. The optimization block is then followed by an ensemble methodology based on multiple one-class classifiers such as one class support vector machine (OC-SVM), Isolation Forest (IF), and Local Outlier Factor (LOF) for the IDS. The proposed solution exhibited effectiveness by achieving impressive accuracy scores of 99.82%, 94.7%, 94.45%, and 97.37% on the KDDCup99, NSL-KDD, UNSW-NB15, and BoT-IoT datasets respectively.

Verma et al. [12] proposed a binary classification approach that is developed from the ML ensemble method. It is aimed at filtering and isolating malicious traffic to safeguard IoT networks. The ensemble approach used the GBM and RF models to improve the classification accuracy of individual models to 98.27% on the CSE-CIC-IDS2018-V2 dataset.

Abbas et al. [13] proposed a new ensemble-based IDS model for the IoT. Their proposed ensemble method used three supervised classification models such as DT, naïve Bayes, and logistic regression followed by a stacking classifier employing hard

voting. The proposed model was evaluated on the CICIDS2017 dataset and exhibited an accuracy of 88.92% and 88.96% for the binary and multiclass classification scenarios.

Thakkar et al. [14] proposed a highly effective IDS designed specifically for IoT networks. Their approach relies on a bagging-Deep Neural Network (DNN)-based ensemble learning strategy, which is designed to tackle the challenge of class imbalance issues in IDS applications. The DNN classification capabilities are enhanced by integrating the bagging technique with carefully calibrated class weights to address the skewed class distribution in the training set. The proposed methodology exhibited model efficiency across different datasets, highlighting accuracy scores of 98.9%, 98.74%, 96.70%, and 98.99% across the NSL-KDD, CIC-IDS2017, UNSW-NB-15, and BoT-IoT datasets respectively.

This study adopts a slightly different approach by proposing a novel hybrid ensemble-based methodology for detecting anomalies in IoT networks. The ensemble prediction is assisted by the prediction of the RF model obtained through the best F1 score for each label through dataset subset selection. The final ensemble prediction then employs the hybrid hard and soft voting strategy to enhance prediction capability for effective IoT protection.

3 Proposed Solution

This section outlines the preliminary concepts, followed by the details of the proposed HEADS for the IoT network.

3.1 Base ML Models

The ensemble learning approach involves combining predictions from multiple individual base models to make a final decision based on certain voting criteria. To achieve this, we utilized RF, GBM, Extreme GBM (XGB), Light GBM (LGBM), and Category Boosting (CB) as our base models.

Random Forest (RF)
RF is a powerful ML-based ensemble learning approach used for both classification and regression tasks. It operates by constructing numerous DTs (forest) during the training phase. Each tree in the forest independently predicts the output. The final prediction is then obtained by a majority vote or averaging, depending on the task [15]. RF's capability to effectively mitigate overfitting and handle high-dimensional data makes it a popular choice for AIDS-based methodologies.

Gradient Boosting Machine (GBM)
GBM is another technique that sequentially constructs an ensemble of DTs. In the process, each subsequent tree aims to correct the errors made by the previous ones [6]. By optimizing a differentiable loss function through gradient descent, GBM gradually minimizes residuals. Hence it captures the complex relationships in data and achieves high predictive accuracy. However, GBM is sensitive to overfitting and requires careful tuning of hyperparameters to prevent it.

Extreme Gradient Boosting Machine (XGB)
XGB is an efficient variant of GBM, that is used for both classification and regression tasks. It improves model generalization by applying many regularization techniques to mitigate overfitting [16]. It is famous for its speed and performance by outperforming other ML algorithms working on structured and tabular data. It is highly customizable and allows fine-tuning of parameters to achieve optimal results.

Light GBM (LGBM)
LGBM is a gradient-boosting framework developed by Microsoft. It aims to achieve high efficiency and speed by using a novel tree-growing algorithm, which can handle large-scale datasets efficiently [17]. It can deal with categorical features directly without requiring one-hot encoding. It employs leaf-wise tree growth and histogram-based algorithms to achieve faster training times and lower memory usage.

Category Boosting (CB)
CB is also a powerful gradient-boosting-based ML technique [18]. It automatically handles missing data and does not require manual encoding of categorical features. It integrates advanced techniques for faster convergence. It also utilizes GPU acceleration for faster training when handling large datasets.

To sum up, RF, GBM, XGB, LGBM, and CB are all ensemble learning techniques that take advantage of the decision trees as base learners. They are effective in handling complex datasets and can capture nonlinear relationships between features and targets. However, they differ in their underlying algorithms and optimizations.

3.2 Methodology

In this study, we propose an efficient ensemble-based methodology HEADS for securing the IoT networks, as depicted in Fig. 1. The proposed solution consists of two phases, (1) Data Interception and Preparation Phase and (2) Hybrid Ensemble Anomaly Detection Phase.

Data Interception and Preparation Phase
The first stage of HEADS is the Data Interception and Preparation Phase, which provides the framework for the important task of intercepting data from IoT networks and preparing it to be in a suitable format for the ML process. The various steps performed in this phase include:

Step-1: The network traffic is captured using network sniffing tools such as tcpdump, which offer platforms for acquiring, examining, analyzing, and visualizing network packets [2, 19]. The sniffer thoroughly analyzes the captured network flows to generate raw packet features. These features are then stored to create an IoT Network dataset.
Step-2: The collected data undergoes a cleaning process that begins with the removal of redundant instances containing infinite or empty fields. Then all the categorical features excluding the target labels are encoded using a one-hot encoding scheme. Then each feature value is normalized between 0 and 1 using Min-Max scaling [2].

Step-3: The pre-processed IoT Network Dataset is then split into 80% Train Dataset for training the ML model and 20% Test Dataset for the evaluation on unseen data.

Hybrid Ensemble Anomaly Detection Phase.
This is the main anomaly detection phase designed for the detection of network anomalies within an IoT network. The main approach adopted here involves implementing hard and soft voting concepts within a hybrid setting to enhance model efficiency. The various steps performed in this phase are:

Step-4: We utilized five base models RF, GBM, XGB, LGBM, and CB. Each of these models is individually trained using the Train dataset to create trained models. Afterward, these trained models are independently tested using the Test Dataset to predict the test labels. For each instance in the Test Dataset, we recorded the predicted label and the corresponding confidence score of each model in the Predictions. The confidence score is the probability value of each model in predicting the label, to show its confidence in the prediction.
Step-5: To assist the ensemble prediction, we opted for the RF model and further trained and evaluated it using subsets of both the Train and Test datasets. Our main objective is to store the predictions made by the RF model, corresponding to the best F1 score for each label in the dataset. To accomplish this, we extracted a subset of the dataset containing only two labels. Following this, we trained the RF model on this subset and then tested the trained model to obtain the F1 scores. The predicted label and its associated confidence score from the RF model are also recorded in the Predictions for each label that corresponds to the highest F1 score.
Step-6: After obtaining predictions and confidence scores for each test instance in steps 4 and 5, we determine the final predictions using a hybrid approach involving both hard and soft voting:

i) If all classifiers predict the same label, the final predicted label follows the hard voting rule and adopts that label.
ii) However, if the classifiers do not reach a consensus on a single label, we employ a soft voting strategy. In this case, the final predicted label is selected based on the one with the highest average confidence score.
iii) If there is a tie in the highest average confidence score, the final predicted label is the one with the highest individual confidence score.

4 Experimental Results and Analysis

This section details the dataset, evaluation metrics, experimental setup, and a comprehensive analysis of the obtained experimental results.

4.1 Dataset Description

To evaluate the performance of the HEADS with other ML-based AIDSs, we used the publicly available CICIoT2023 dataset [9]. This dataset is collected by the Canadian Institute for Cybersecurity, University of New Brunswick, Canada from the real IoT topology composed of 105 devices. The dataset contains network flows for the Benign

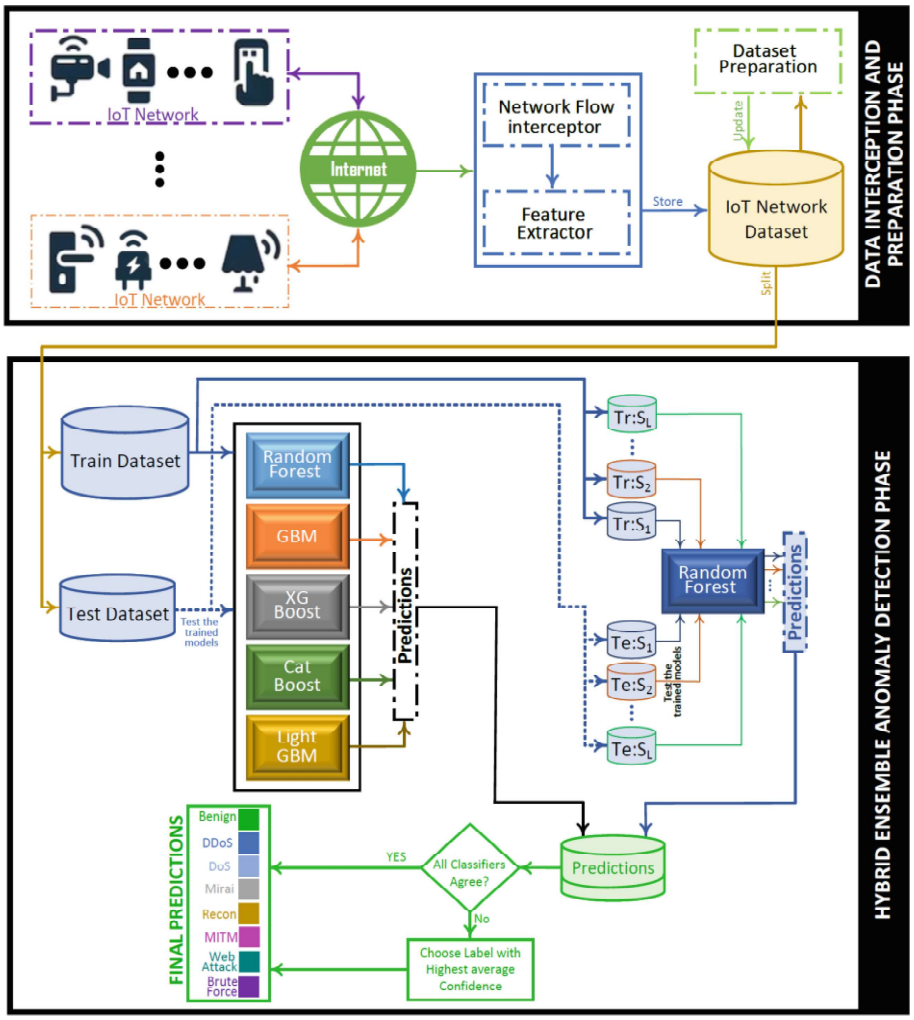


Fig. 1. Proposed HEADS

traffic and 33 attacks on IoT devices which are classified into seven categories, namely DDoS, DoS, Mirai, Reconnaissance, Spoofing, Web-based, and Brute force. The dataset files are publicly available in the PCAP and CSV formats. The CSV file contains 46 numerical features and one categorical label feature. For this study, we randomly selected instances for each label, ensuring that instances for all 33 types of attacks are included. The total number of instances considered in this study are detailed in Table 1.

Table 1. Dataset Distribution

Label	Instances	Train dataset	Test dataset
Benign	50000	39979	10021
DDoS	25000	20018	4982
DoS	15000	12049	2951
Mirai	10000	7930	2070
Reconnaissance	8000	6340	1660
Spoofing	7000	5656	1344
Web-based	3000	2417	583
Brute Force	2000	1711	289
Total Flows	***120000***	***96100***	***23900***

4.2 Evaluation Metrics

In this study, the performance evaluation of the HEADS and other ML/DL models considers evaluation metrics such as Accuracy, Precision, Recall, F1 score, and False Alarm Rate (FAR). All these metrics are calculated from various elements of the confusion matrix [19] and are given as,

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{2}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{3}$$

$$\text{F1 score} = \frac{2(\text{Pr})(\text{Re})}{\text{Pr} + \text{Re}} \tag{4}$$

$$\text{FAR} = \frac{FP}{FP + TN} \tag{5}$$

where, the correctly predicted Anomaly and Benign instances are represented as True Positive (TP) and True Negative (TN) respectively. Also, the incorrectly predicted labels as Benign and Anomaly are given as False Negative (FN) and False Positive (FP) respectively.

4.3 Experimental Setup

All performance evaluation experiments were conducted on an HP laptop featuring an Intel Core i9-10885H processor, 32 GB RAM, and a 64-bit Windows 10 operating system. Python (version 3.10.12) served as the main programming language to implement and evaluate all AIDS methodologies within the Google Colab environment.

4.4 Results and Discussion

In this research, the performance of the HEADS is compared with five supervised ML approaches such as RF, XFB, LGBM, CB, and GBM, followed by their ensemble models employing the hard and soft voting strategies. Each experiment is performed 5 times, with a random selection of train and test split each time to obtain evaluation metric scores.

Table 2 presents the average evaluation metric score in percentages for all the considered ML-based AIDS models. We can observe that all models, including the ensembles, perform well, with accuracy scores ranging from approximately 95.7% to 96.1%. However, our proposed methodology HEADS performs exceptionally well by obtaining an accuracy of 99.75%, highlighting its effectiveness in correctly predicting network instances. Additionally, the precision, recall, and F1 scores obtained by HEADS indicate its effectiveness in identifying both positive and negative instances with minimal FP and FN. Also, the lower FAR further confirms the reliability of the HEADS, which is a crucial factor for the performance of AIDS. Overall, our proposed HEADS methodology exhibited better performance over other considered ML-based AIDS approaches.

Table 2. Performance Evaluation Metric Score [%]

ML Model	Accuracy	Precision	Recall	F1 score	FAR
RF	95.667	95.589	95.667	95.458	0.813
XGB	95.929	95.850	95.929	95.805	0.735
LGBM	95.792	95.678	95.792	95.654	0.761
CB	95.963	95.884	95.963	95.828	0.739
GBM	95.696	95.642	95.696	95.507	0.818
Ensemble (Hard)	96.029	95.971	96.029	95.870	0.748
Ensemble (Soft)	96.063	96.009	96.063	95.915	0.738
HEADS	**99.750**	**99.752**	**99.750**	**99.751**	**0.038**

The results depicted in Fig. 2 illustrate the percentage improvement of the HEADS compared to other ML-based AIDS methodologies for all the considered performance evaluation metrics. HEADS highlighted approximately 3.7% to 4.1% improvement in terms of accuracy and 3.8% to 4.3% in terms of F1 score comparing other methodologies. Additionally, HEADS obtained improvement in FAR reduction of around 0.7% comparing the other AIDS methodologies. Overall HEADS achieves higher accuracy, precision, recall, and F1 score compared to the other models, while also maintaining a lower FAR. These results highlight the effectiveness and superiority of the HEADS in accurately predicting the label with minimized FAR.

Figure 3 depicts the confusion matrices for the ensemble learning approaches employing hard/soft voting and HEADS. Comparing these results, we observe distinct patterns in the performance of different models. Across all three models, we observe

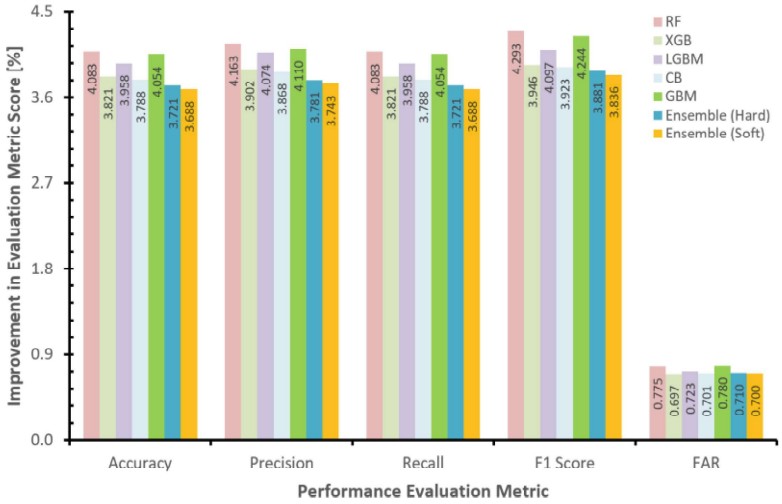
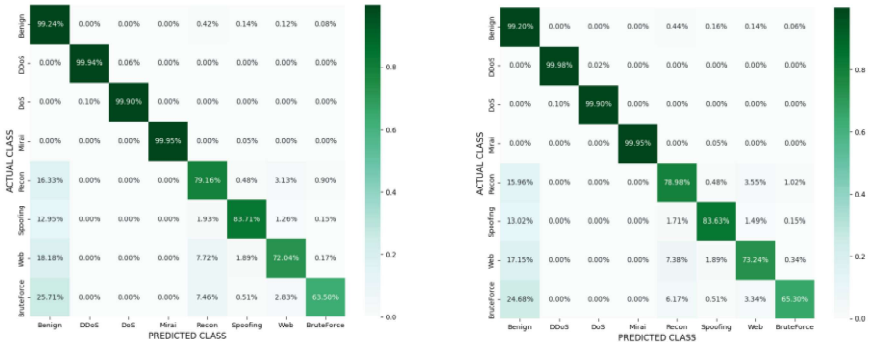


Fig. 2. Percentage improvement in the HEADS performance over other ML models.

the correct classification of instances labeled as Benign, DDoS, DoS, and Mirai, as indicated by high percentage values along the diagonal. However, both ensemble approaches exhibit degraded performance in correctly classifying instances labeled as Reconnaissance, Spoofing, web-based, and brute force, indicated by the higher misclassification rates reflected in off-diagonal percentage values. In contrast, the HEADS demonstrate higher percentage scores in the diagonal and significantly fewer off-diagonal percentages which indicate its superior accuracy in predicting class labels. Furthermore, comparing the HEADS to the ensemble approaches, we observe notable improvements in the correct classification percentages: Benign by 0.6%, DDoS by 0.1%, DoS by 0.07%, Reconnaissance by 19%, Spoofing by 16.8%, Web-based by 25.6%, and brute force by 36.5%. These results underscore the enhanced performance of the HEADS compared to the ensemble-based approaches across various labels.

Table 3 details the comparison of results in this study directly with the results obtained in DL-BiLSTM [20] and Blending [21] based AIDS approaches, on the CICIoT2023 dataset. F1 score and Accuracy are selected as the evaluation metric. We notice that the DL-BiLSTM model achieves a reasonable F1 score of 91.94% and an accuracy of 93.13%. The Blending model outperforms DL-BiLSTM significantly, achieving an impressive F1 score of 99.07% and an accuracy of 99.51%. In contrast, the HEADS surpasses both DL-BiLSTM and the Blending approach. It achieved an exceptional F1 score of 99.751% and an accuracy of 99.750%. These results highlight the effectiveness and superiority of the HEADS in accurately predicting class labels, making it a promising approach for detecting anomalies in IoT networks.

To sum up, the proposed HEADS improves AIDS performance by enhancing the voting strategy for ensemble learning. The proposed solution performed exceptionally well to not only improve the detection accuracy but also reduce FAR. However, this improvement comes at the expense of more complexity. In an IoT network scenario,



Ensemble (Hard) Ensemble (Soft)

HEADS

Fig. 3. Confusion Matrix

Table 3. Comparison with other studies [%]

Model	F1 score	Accuracy
DL-BiLSTM [20]	91.94	93.13
Blending [21]	99.07	99.51
HEADS [This Study]	**99.751**	**99.750**

where computing resources are limited, the possible solution will be the deployment of the HEADS at the cloud edge.

5 Conclusions

This paper proposes an effective Hybrid Ensemble-based Anomaly Detection System to strengthen the security at the entry points of the IoT network through monitoring the network traffic. The proposed solution improves ensemble learning by introducing

a novel hybrid approach by combining the hard and soft voting strategies. Additionally, the detection accuracy is improved by including the predictions of the RF model corresponding to the best F1 score for each label obtained using the dataset subset selection. The proposed methodology is evaluated on the publicly available CICIoT2023 dataset, which exhibits the model's effectiveness by achieving high evaluation metric scores in correctly detecting the network anomalies while minimizing the FAR.

For future research, we aim to extend this work by implementing and evaluating HEADS performance in real-time IoT scenarios. Additionally, we also plan to explore the hybrid ensemble concept employing unsupervised ML/DL methodologies.

References

1. Ahmad, F., Ahmad, Z., Kerrache, C.A., Kurugollu, F., Adnane, A., Barka, E.: Blockchain in Internet-of-Things: architecture, applications and research directions. In: 2019 International Conference on Computer and Information Sciences, ICCIS 2019 (2019). https://doi.org/10.1109/ICCISCI.2019.8716450
2. Ahmad, Z., et al.: S-ADS: spectrogram image-based anomaly detection system for IoT networks. In: Proceedings - AiIC 2022: 2022 Applied Informatics International Conference: Digital Innovation in Applied Informatics During the Pandemic, pp. 105–110 (2022). https://doi.org/10.1109/AIIC54368.2022.9914599
3. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., Faruki, P.: Network intrusion detection for IoT security based on learning techniques. IEEE Commun. Surv. Tutor. **21**, 2671–2701 (2019). https://doi.org/10.1109/COMST.2019.2896380
4. Khan, A.S., Ahmad, Z., Abdullah, J., Ahmad, F.: A spectrogram image-based network anomaly detection system using deep convolutional neural network. IEEE Access **9**, 87079–87093 (2021). https://doi.org/10.1109/ACCESS.2021.3088149
5. Keshk, M., Koroniotis, N., Pham, N., Moustafa, N., Turnbull, B., Zomaya, A.Y.: An explainable deep learning-enabled intrusion detection framework in IoT networks. Inf. Sci. **639**, 119000 (2023). https://doi.org/10.1016/J.INS.2023.119000
6. Louk, M.H.L., Tama, B.A.: Dual-IDS: a bagging-based gradient boosting decision tree model for network anomaly intrusion detection system. Expert Syst. Appl. **213**, 119030 (2023). https://doi.org/10.1016/J.ESWA.2022.119030
7. Cao, Y., Wang, Z., Ding, H., Zhang, J., Li, B.: An intrusion detection system based on stacked ensemble learning for IoT network. Comput. Electr. Eng. **110**, 108836 (2023). https://doi.org/10.1016/J.COMPELECENG.2023.108836
8. Mohammed, A., Kora, R.: A comprehensive review on ensemble deep learning: opportunities and challenges. J. King Saud Univ. Comput. Inf. Sci. **35**, 757–774 (2023). https://doi.org/10.1016/J.JKSUCI.2023.01.014
9. Neto, E.C.P., Dadkhah, S., Ferreira, R., Zohourian, A., Lu, R., Ghorbani, A.A.: CICIoT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors **23**, 5941 (2023). https://doi.org/10.3390/S23135941
10. Luo, C., Tan, Z., Min, G., Gan, J., Shi, W., Tian, Z.: A novel web attack detection system for Internet of Things via ensemble classification. IEEE Trans. Ind. Inform. **17**, 5810–5818 (2021). https://doi.org/10.1109/TII.2020.3038761
11. Abu Alghanam, O., Almobaideen, W., Saadeh, M., Adwan, O.: An improved PIO feature selection algorithm for IoT network intrusion detection system based on ensemble learning. Expert Syst. Appl. **213**, 118745 (2023). https://doi.org/10.1016/J.ESWA.2022.118745
12. Verma, P., et al.: A novel intrusion detection approach using machine learning ensemble for IoT environments. Appl. Sci. **11**, 10268 (2021). https://doi.org/10.3390/APP112110268

13. Abbas, A., Khan, M.A., Latif, S., Ajaz, M., Shah, A.A., Ahmad, J.: A new ensemble-based intrusion detection system for Internet of Things. Arab. J. Sci. Eng. **47**, 1805–1819 (2022). https://doi.org/10.1007/S13369-021-06086-5/TABLES/12
14. Thakkar, A., Lohiya, R.: Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep neural network. IEEE Internet Things J. **10**, 11888–11895 (2023). https://doi.org/10.1109/JIOT.2023.3244810
15. Ahmad, I., Basheri, M., Iqbal, M.J., Rahim, A.: Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE Access **6**, 33789–33795 (2018). https://doi.org/10.1109/ACCESS.2018.2841987
16. Saheed, Y.K.: Performance improvement of intrusion detection system for detecting attacks on Internet of Things and edge of things. In: Misra, S., Kumar Tyagi, A., Piuri, V., Garg, L. (eds.) Artificial Intelligence for Cloud and Edge Computing. IT, pp. 321–339. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-80821-1_15
17. Tang, C., Luktarhan, N., Zhao, Y.: An efficient intrusion detection method based on LightGBM and autoencoder. Symmetry **12**, 1458 (2020). https://doi.org/10.3390/SYM12091458
18. Kayode Saheed, Y., Idris Abiodun, A., Misra, S., Kristiansen Holone, M., Colomo-Palacios, R.: A machine learning-based intrusion detection for detecting internet of things network attacks. Alex. Eng. J. **61**, 9395–9409 (2022). https://doi.org/10.1016/J.AEJ.2022.02.063
19. Ahmad, Z., Khan, A.S., Zen, K., Ahmad, F.: MS-ADS: multistage spectrogram image-based anomaly detection system for IoT security. Trans. Emerg. Telecommun. Technol. **34**, e4810 (2023). https://doi.org/10.1002/ett.4810
20. Wang, Z., Chen, H., Yang, S., Luo, X., Li, D., Wang, J.: A lightweight intrusion detection method for IoT based on deep learning and dynamic quantization. PeerJ Comput. Sci. **9**, e1569 (2023). https://doi.org/10.7717/PEERJ-CS.1569/SUPP-1
21. Le, T.T.H., Wardhani, R.W., Catur Putranto, D.S., Jo, U., Kim, H.: Toward enhanced attack detection and explanation in intrusion detection system-based IoT environment data. IEEE Access **11**, 131661–131676 (2023). https://doi.org/10.1109/ACCESS.2023.3336678