Ensemble-based Intrusion Detection for Internet of Things Devices

Conference Paper · December 2022

DOI: 10.1109/HONET56683.2022.10019140

6 authors, including:

Priscilla Danso
Stony Brook University
5 PUBLICATIONS **135** CITATIONS
SEE PROFILE

Sajjad Dadkhah
University of New Brunswick
59 PUBLICATIONS **933** CITATIONS
SEE PROFILE

Alireza Zohourian
University of New Brunswick
10 PUBLICATIONS **375** CITATIONS
SEE PROFILE

2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET) | 978-1-6654-6197-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/HONET56683.2022.10019140

Ensemble-based Intrusion Detection for Internet of Things Devices

Priscilla Kyei Danso
Canadian Institute for Cybersecurity
University of New Brunswick
Fredericton, Canada
priscilla.danso@unb.ca

Euclides Carlos Pinto Neto
Canadian Institute for Cybersecurity
University of New Brunswick
Fredericton, Canada
e.neto@unb.ca

Sajjad Dadkhah
Canadian Institute for Cybersecurity
University of New Brunswick
Fredericton, Canada
sdadkhah@unb.ca

Alireza Zohourian
Canadian Institute for Cybersecurity
University of New Brunswick
Fredericton, Canada
alireza.zohourian@unb.ca

Heather Molyneaux
National Research Council Canada
Fredericton, Canada
heather.molyneaux@nrc-cnrc.gc.ca

Ali A. Ghorbani
Canadian Institute for Cybersecurity
University of New Brunswick
Fredericton, Canada
ghorbani@unb.ca

***Abstract*—Security, privacy, and interoperability challenges have arisen as the Internet of Things (IoT) devices proliferate and become increasingly connected. IoT devices have resource constraints such as computational capabilities, power consumption, onboard storage, and network bandwidth, which limit the implementation of cryptographic solutions. The heterogeneous nature of IoT devices makes them an avenue for attackers to exploit threats like spoofing, routing, MITM, and DoS attacks. With the current sophistication of threats IoT devices are subjected to, an Intrusion Detection System (IDS) is the preferred solution for IoT devices. An IDS continuously monitors incoming traffic and discovers potential threats in incoming and outgoing traffic. This research proposes a novel intelligent ensemble-based IDS that will reside in the IoT gateway. The uniqueness of our approach lies in an ensemble learning approach that combines multiple machine learning methods to improve prediction performance and detection accuracy. Ensemble learning has been studied to increase the detection rate while obtaining better generalization performance due to combining several Machine Learning (ML) models, also known as base learners. Three popularly known ensemble models (i.e., boosting, stacking, and voting) are employed to assess our proposed IDS performance. The proposed method use algorithms such as Naïve Bayes (NB), Support Vector Classification (SVC), and *k*-Nearest Neighbors (*k*NN). Lastly, the proposed approach will be evaluated on two publicly available datasets; Intrusion Detection Evaluation Dataset (CIC-IDS2017) and N-BaIoT.**

***Keywords*—** Internet of Things, Machine Learning, Ensemble Technique, Intrusion Detection System

I. Introduction

Internet of Things (IoT) has become present in our daily lives, with research estimating 75 billion connected devices in use by 2025 [7]. As Figure 1 shows, between 2015 and 2025, almost 60 billion IoT devices will be utilized worldwide. Based on the forecast by McKinsey Global Institute, we may witness an economic impact of potentially $11.1 trillion worth by the year 2025 [19].

An IoT application commonly comprises inexpensive resource-constrained devices, or "Things", that are locally connected to a gateway for the data gathered by these devices to go through the gateway to and from the Internet [15]. Securing these devices before deployment should be the core focus of manufacturers. However, these devices are insecurely deployed without the optimum security requirements, hence they undergo several cyberattacks such as Denial of Service [11], botnet [4], infiltration attack [18], among others.

Due to the heterogeneous nature of IoT devices, several entry points and types of attacks could disrupt their operation and performance. Some of the largest and most famous Cyberattacks performed on vulnerable IoT devices have caused severe damage. A case in point is the Dyn DNS provider attack. The October 2016 Mirai botnet attack is still ranked the most significant distributed denial of service (DDoS) attack on IoT devices to date [1]. The attack targeted Dyn infrastructure shutting down the Dyn DNS servers. This resulted in Mirai, a cyberattack that enlisted connected devices plucked from smart homes into "botnets" (also known as "zombie armies") [4]. Several popular websites such as Amazon, CNN, Github, Netflix, Paypal, and Twitter were rendered unreachable for several hours [8].

The Federal Office for Information Security of the German government stated in December 2014 that a hostile actor had breached a steel facility using a spear phishing email to obtain access to the corporate network before moving into the plant network. After gaining a foothold in the plant network, the adversary caused several system components to malfunction. As a result, this affected critical process components to become unregulated, resulting in substantial physical damage

[14].

The proposed approach in this study aims to address the risk of IoT devices by detecting and mitigating potential attacks. Data streams produced by various sources are monitored and analyzed to identify possible cyber threats using an IDS. There are two primary procedures for threat detection, namely anomaly-based and signature-based. The former extracts/stores signatures from attacks and detects attackers by validating their signatures in the database, known as rule-based [27].On the other hand, the latter compares definitions of what activity is deemed normal to observed events to find apparent discrepancies [24].

The primary motivation of this research stems from the limitation of signature-based IDS detecting only known attacks. Hence, this research proposes an intelligent ensemble-based IDS framework that can detect the cyber threats of IoT. The proposed ensemble-based IDS is intended to reside in the IoT gateway to protect IoT devices within the network because the gateway serves as an access portal to give IoT devices access to the Internet. With this approach, the resource-constrained IoT devices will be relieved of the computational processing of the proposed IDS.

The uniqueness of our approach is that it employs an ensemble learning technique, which integrates various machine learning approaches to improve predictive performance and detection accuracy. The major contributions of this research are:

- A novel ensemble-based intrusion detection approach located directly in the IoT gateway to detect incoming and outgoing attacks;
- An evaluation on how the three main ensemble models i.e. boosting, voting and stacking techniques perform in this task;
- A demonstration of the applicability of the proposed approach using two datasets, i.e., CIC-IDS2017 and N-BaIoT.

The remainder of the paper is structured as follows. Section II investigates the previous literature using ensemble techniques for intrusion detection. Section III reviews the experimental system flow of the proposed IDS framework. Section IV illustrates the experimental results of the proposed models. Finally, Section V discusses the conclusion and the future works.

.

II. Literature Review

Tama et al. [26] propose an Intrusion Detection System (IDS) that relies on a hybrid feature selection approach and ensemble classifiers with two levels. Three modules comprise the suggested framework: feature selection, classifier modeling, and validation. For the purpose of training the machine learning model to increase the classifier's detection rate, a hybrid technique is employed to selectively choose the most important features while reducing the overall feature size during the feature selection process. The second module is a two-stage meta classifier that combines Rotation Forest (RF) and bagging (BG), two different types of meta classifiers. In their model training 10-fold, cross-validation is utilized. When employed on the UNSW-NB15 and NSL-KDD datasets, the proposed method's accuracy, sensitivity, and detection rates were 85.8%, 86.8%, and 88.8%, respectively.

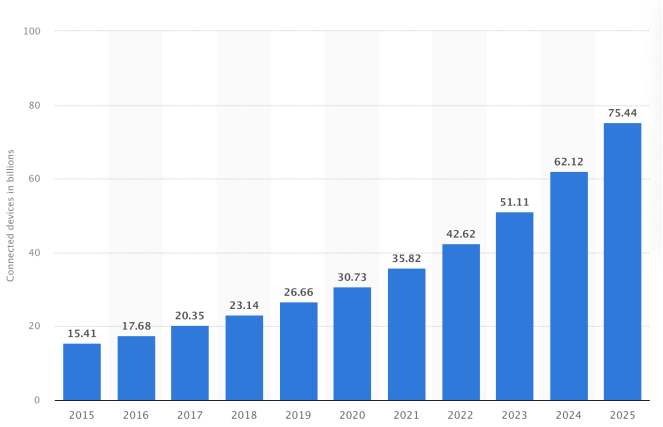

Fig. 1: IoT devices used worldwide from 2015 and predicted to be used by 2025 (in billions) [7]

In [21], the authors provide new statistical features generated from the flow of the protocols. Three ML model acting as base learners was employed to work with the AdaBoost ensemble technique. Bro-IDS developed flow-based features from MQTT, DNS, and HTTP protocols. The correlation coefficient determines the strength of the proposed feature, whereas the correntropy measure estimates how similar the proposed feature vectors are to one another. The ensemble approach is then used to classify normal and suspicious cases using the selected attributes. The AdaBoost classifier divides the data among three ML approaches that serve as base learners: Decision Tree, Artificial Neural Network Decision Tree, and Naïve Bayes. Respective results for accuracy, detection rate (DR), and false positive rate (FPR) are 98.97%, 97.02%, 2.58%, and 98.29%, 97.38%, 2.01%, for evaluating UNSW-NB15 and NIMS datasets.

Khraisat et al. use a C5 classifier in conjunction with a One-Class Support Vector Machine to model a Hybrid Intrusion Detection System (HIDS) framework for detecting known and unknown attacks in a network. The proposed hybrid paradigm is divided into Signature Anomaly-based Intrusion Detection System (AIDS) and Intrusion Detection System (SIDS). In the SIDS phase, the C5 decision tree is used to perform binary classification of malware and benign attacks. In order to train the AIDS to distinguish unidentified attacks, the output from the SIDS is subsequently utilized. The model is trained using only benign samples, and any patterns that deviate from those developed using benign samples will be marked as anomalous. One-Class SVM is used to train only the normal data during the AIDS phase. The third phase, HIDS, uses an ensemble technique to combine the C5 classifier and one-class SVM with improving prediction accuracy. Evaluating the findings on

the Bot-IoT dataset yields an approximate accuracy of malware detection in SIDS, AIDS, and HIDS of 94%, 92.50%, and 99.97%.

Pinkey et al. [5] propose to employ LGBM, Extra Tree, Random Forest, XGBoost tree-based ensemble approaches, and Gradient Boost to detect anomalous behavior. This method starts with 14 features extracted in addition to the 32 existing features in the dataset. Pearson's Correlation Coefficient and entropy select the dataset's most relevant set of elements. Ten distinct features were used for training each of the five ensemble methods by scaling for normalization using the MinMax scaler. Five tree-based ensembles, Light Gradient Boosting Machine (LGBM), Random Forest (RF), Gradient Boosting (GB), eXtreme Gradient Boosting, and ExtraTree (ET), were used to train the top 10 features (XGB). Employing 10-fold cross-validation on the BoT-IoT dataset, LGBM outperformed RF, ET, GB, and eXtreme Gradient Boosting.

III. The Experimental System Flow of the Proposed IDS Framework

This research introduces an ensemble-based intrusion detection system (IDS) deployed in an IoT gateway. The IDS can be placed on the IoT gateway to detect and secure threats in the IoT network to detect all incoming and outgoing traffic and ensure the devices are not compromised. An IDS approach is the dominant IoT defense because it runs as an independent entity on the IoT gateway and does not burden the resource-constrained interconnected devices [3], [6]. An Intrusion Detection System (IDS) is a detective control mechanism designed to mitigate and prevent the attack from taking effect [2]. An ensemble learning technique ultimately aims to create a robust, efficient, and effective classifier by combining the strengths and skills of several weak learners. This will increase the accuracy of detection and decrease false alarm rates [17].

This section overviews the proposed IDS framework. A detailed explanation of the feature selection and classifier modelling methods used is provided. Figure 2 depicts the proposed framework. The framework is composed of three modules, i.e., data pre-processing, feature selection, and model training which we briefly discuss below and elaborate on in the section that follows.

1) *Data Pre-processing:* During this stage, missing values are handled, the dataset is normalised before training, and the dataset is encoded and transformed. Additional features are collected from the dataset provided during the data acquisition stage. A set of the top statistical attributes for our IDS framework is collected in order to deploy our proposed approach more effectively and yield good performance. The detailed description of the data pre-processing module is explained in subsection III-A.
2) *Feature selection module:* During this stage, a carefully chosen set of feature vectors are selected and passed to the ensemble learning technique to perform the intrusion detection task at hand. The feature selection approach used in the research is explained in details in subsection III-B.
3) *Model Training:* This research employs an ensemble technique to learn and detect different types of attacks and also normal traffic. Voting, Stacking and Boosting ensemble models are explored to find the best technique for our approach. The base learners used in this research are; Naïve Bayes (NB), Support Vector Classification (SVC), and *k*-Nearest Neighbor (*k*NN). Subsection III-C describes the ensemble machine learning training scheme proposed in this research.

A. Data pre-processing

In this stage, all incomplete data entries for the observed variables in the dataset are handled. To fit the data within a predefined boundary between zero and one, Min-Max normalization is employed [22]. Furthermore, a common challenge in ML classification is the unequal proportion of the samples in each class distribution. This scenario, often known as the imbalanced problem, has an impact on how well many ML algorithms function. The minority class samples are frequently misclassified by the model that was trained on unbalanced data [13]. To prevent overfitting, a number of records are equally sampled from each target class during training the classifier.

B. Feature selection

A crucial stage in any ML training, but particularly in the proposed approach in this study, is feature selection. Feature selection relies on selecting the fewest number of attributes required to accurately represent the data [16]. The SelectKbest technique is used to choose the most reliable and effective features to identify legitimate and malicious network data. A feature selection approach called SelectKbest is used to enhance prediction performance or accuracy [10] by classifying a dataset's features according to how important they are in relation to the desired outcome, with the importance determined by a score function. Chi Square is a univariate feature selection approach because it only evaluates one variable and ignores the effects of many variables' interactions on the output [9].

In this study, a univariate feature selection algorithm called SelectKbest was combined with the Chi Square score function. The Chi Square module obtains each feature's score based on its reliance and correlation with the target label. The SelectKbest module chooses the best feature set for training the ML model using the score values from the Chi Square module.

C. Model Training

In this phase, the ensemble technique is employed to classify the normal and attack traffic using three ML techniques acting as base learners. The ML models employed are:*k*-Nearest Neighbor (*k*NN), Support Vector Classification (SVC), and Naïve Bayes (NB). To obtain the best performance for constructing an adaptive IDS, the ML models are applied

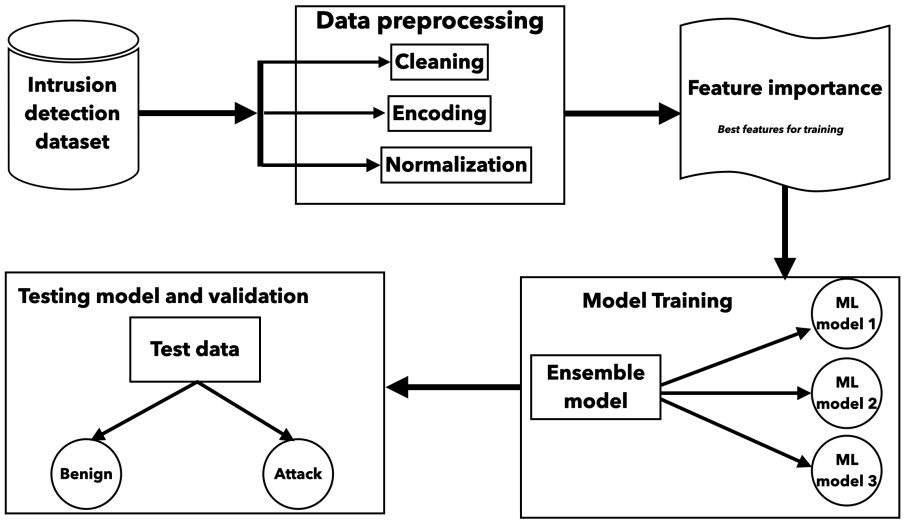

Fig. 2: The Experimental System Flow of the Proposed ensemble-based IDS Framework.

.

as an ensemble method with the three ensemble models: Voting, Boosting, and Stacking. The chosen ML models were employed in the ensemble technique because they have a range of decision-making styles and domain expertise [12].

The three most well known ensemble methods are:

Voting: Each base-level classifier votes for its own prediction. The final prediction is the one with the most votes [23].

Stacking: To combine the predictions in the Voting process, a learning algorithm is used in stacking. Then, the ensued meta-level classifier is used to form the final prediction from the ones predicted by the base classifiers.

Boosting: Starting with the original data set, boosting initially creates a classifier using a learning algorithm. After increasing the weights of the incorrectly categorised instances, a new classifier is created using the same learning method. Several times are spent repeating the process. Following this, classifiers are blended using weighted voting [28].

IV. Experiments, Results and Analysis

This section explains how the experiments were evaluated. In the final section, the ensemble learning framework and the techniques it uses are explained in detail, as well as the findings and experimental results.

A. Experiments

This section examines the performance measures, the training and testing of the ensemble methods, and the data sampling methodology used.

1) ***Reduction of dataset size***

CIC-IDS2017 dataset after data pre-processing contained 2659039 number of rows and 78 columns. 20 features were selected using the process explained in Section III-B. The baseline number of records for each class is set at the target label with the fewest records. Hence 5499 is the number of records sampled after pre-processing for training the proposed IDS. Equal number of records from each class are sampled in order to prevent overfitting, which would cause benign traffic to outnumber the DoS Slowhttptest, for example.

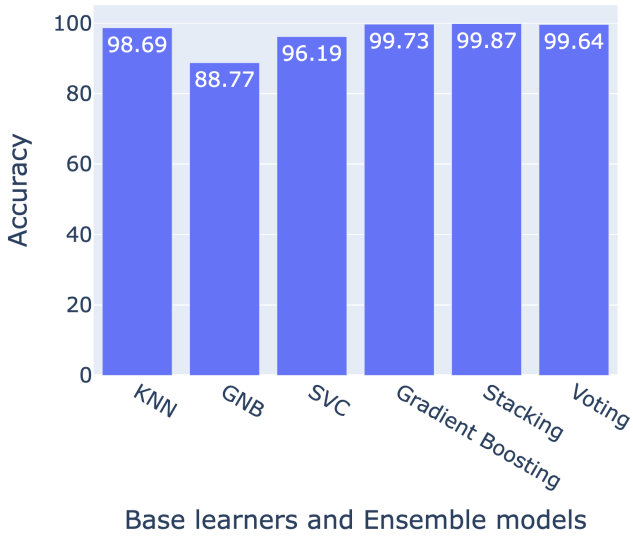

Fig. 3: Comparison of the accuracy of the base learners and the ensemble technique proposed for the IDS on the CIC-IDS2017 dataset [25].

Similarly, in the N-BaIot dataset, 6000 records was selected for each class to avoid overfitting. The data set has 836891 rows and 116 columns after data pre-processing. The most important features will be sampled to training our proposed IDS.

2) ***Training and Testing of the ensemble methods***

Each base learner is trained and performed evaluated. When training the different base learners, k-fold cross validation was performed. With 90% of the data for training and 10% for

TABLE I: Performance of Ensemble methods for the proposed IDS on CIC-1DS2017 dataset [25].

	Base Leaners			Ensemble Methods		
Metric	**KNN**	**GNB**	**SVC**	**Boosting (GradientBoosting)**	**Stacking (With Base Learners)**	**Voting (With BaseLearners)**
Accuracy(%)	98.69	88.77	96.19	99.73	99.87	99.64
DR(%)	99.73	89.68	95.23	91.98	99.36	98.28
FPR(%)	0.15	1.25	0.42	0.02	0.073	0.20
F1-Score(%)	99.56	87.45	95.24	89.56	99.34	98.19
Precision(%)	99.67	90.78	96.19	90.23	94.79	97.40

TABLE II: Performance of Ensemble methods for the proposed IDS on N-BaIoT dataset. [20]

	Base Leaners			Ensemble Methods		
Metric	**KNN**	**GNB**	**SVC**	**Boosting (GradientBoosting)**	**Stacking (With Base Learners)**	**Voting (With BaseLearners)**
Accuracy(%)	89.83	72.47	75.05	90.69	90.87	78.68
DR(%)	90.54	73.69	75.55	91.03	90.88	78.33
FPR(%)	5.53	2.753	6.07	5.43	6.74	5.82
F1-Score	87.11	69.55	71.33	88.56	87.83	73.78
Precision	85.98	69.23	69.45	86.79	85.67	72.23

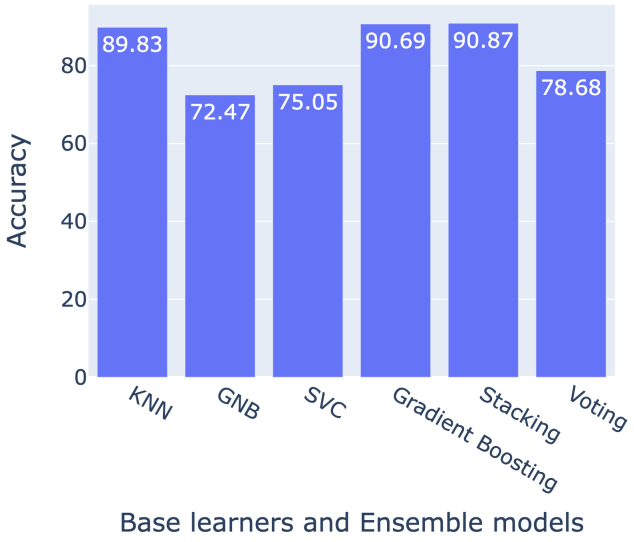

Fig. 4: Comparison of the accuracy of the base learners and the ensemble technique proposed for the IDS on the N-BaIoT dataset [20].

testing on the data exclusively for three times. As a result, the results obtained after three fold cross validation will be more precise [5]. In this study, k is set to 3 because the training set is insufficiently large, and increasing the k value will result in an infinitesimal change in the size of the training and re-sampled subsets.

3) ***Performance measuring metrics***

Accuracy, Precision, Detection Rate, False Positive Rate, and F1-score are the four performance metrics calculated for all classifiers. All of these metrics are calculated using the following formula:

Accuracy is a metric for evaluating classification models that represents the proportion of correct predictions to total model observation.

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

Precision is the ratio of correctly identified "Benign" to the total number of correctly or incorrectly predicted instances of "Benign" by the classifier.

$$Precision = \frac{TP}{TP + FP}$$

Detection Rate represents the number of actual "Benign" that the classifier correctly identified as such.

$$Recall = \frac{TP}{TP + FN}$$

F1-score is a geometric average of precision and recall.

$$F1 - score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

False Positive Rate (FPR) is the relative frequency of not "Benign" when "Benign" is predicted.

$$FalsePositiveRate = \frac{FP}{TN + FP}$$

B. Results and Analysis

This section discusses the performance of the proposed ensemble approach using metric described in Section IV-A3.

1) ***CIC-IDS2017***

The individual base learners are evaluated before the ensemble method is evaluated.

*k*NN outperformed the other base learners in terms of accuracy, DR, FPR, F1-score, and precision as shown in Table I. DR, FPR, and F1-score values were 98.69%, 99.73%, 0.15%, 99.56%, 99.67%, respectively.

The performance of the ensemble approaches, including the boosting, stacking, and voting models, is displayed in Table Table I. With scores of 99.87%, 99.36%, and 99.34%, the stacking model outperformed the other two models in accuracy, DR, and F1-score.

Figure 3 shows the stacking model performs better than the other ensemble models and ultimately the base learners with an accuracy of 99.87%.

2) ***N-BaIoT***

In comparison to the N-BaIoT [20] dataset, the CIC-IDS2017 [25] dataset performed better overall. As can be observed from Table II, *k*NN performs better than SVC and NB in accuracy, DR, F1-score, and Precision, with respective values of 89.83%, 90.54%, 87.11%, and 85.98%. According to Table II, among the three ensemble strategies used to analyze the N-BaIoT dataset, the stacking ensemble

method outperforms the others with an accuracy of 90.87% and a the boosting with a detection rate of 91.03%. Figure 4 illustrates how the stacking ensemble technique outperforms the other ensemble models and the base learners with an accuracy of 80.87

In general, for both datasets, the stacking ensemble method had a 99.87% accuracy, the *k*NN base learner had a 99.73% detection rate. The Gradient Boosting ML model acting a boosting ensemble method had a 0.02% false positive rate, and *k*NN had F1-score and precision values of 99.56% and 99.67% respectively.

V. Conclusion and Future Works

Due to how computationally-expensive deep learning-based IDS can be on the resource-constrianed IoT devices, a novel intelligent ML-based ensemble IDS approach is proposed in this study. To extract and evaluate the most effective features, simulated IoT devices were used, their network traffic was monitored and the features were selected using the SelectKbest and Chi Squared techniques. Multiple ensemble techniques are evaluated, and the best one is chosen as the preferred for our proposed IDS. As a result, the performance of these ensemble frameworks is examined. *k*NN, NB, and SVM ML models acted as the base learners for the stacking and voting ensemble methods. Furthermore, Gradient Boosting ML model was employed as the boosting ensemble method. These techniques were used to improve the overall performance, i.e. accuracy, rate of detection, and FPR. The stacking approach was therefore recommended for our IDS because it performed better than the base learners and the other ensemble approaches. The experimental results indicate that the proposed ensemble method proved to be effective in detecting different benign and attack traffic when applied to two publicly available IDS datasets. This research will be expanded in the future in order to implement an IDS using an anomaly-based approach, in which normal or benign behaviour is modelled and any divergence from normal behaviour is flagged as an anomaly. Finally, future initiatives will aim to improve the overall performance shown in this work.

Acknowledgment

The authors graciously acknowledge the support from the Canadian Institute for Cybersecurity (CIC), the funding support from the National Research Council of Canada (NRC) through the AI for Logistics collaborative program, the NSERC Discovery Grant (no. RGPIN 231074), and Tier 1 Canada Research Chair to Dr. Ghorbani.

References

[1] Kishore Angrishi. Turning internet of things (iot) into internet of vulnerabilities (iov): Iot botnets. *arXiv preprint arXiv:1702.03681*, 2017.

[2] M. Appel, OhioLINK Electronic Theses, Dissertations Center, Ohio State University. Department of Electrical, and Computer Engineering. *Security Control Mechanism for Safety Critical Functions Operating on Automotive Controller Area Network*. Ohio State University, 2020.

[3] Rohit Bhatia, Vireshwar Kumar, Khaled Serag, Z. Berkay Celik, Mathias Payer, and Dongyan Xu. Evading Voltage-Based Intrusion Detection on Automotive CAN. In *Network and Distributed System Security Symposium (NDSS)*, pages 1–17, 2021.

[4] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. Network intrusion detection for iot security based on learning techniques. *IEEE Communications Surveys Tutorials*, 21(3):2671–2701, 2019.

[5] Pinkey Chauhan and M. Atulkar. Selection of tree based ensemble classifier for detecting network attacks in iot. In *2021 International Conference on Emerging Smart Computing and Informatics (ESCI)*, pages 770–775, 2021.

[6] Sajjad Dadkhah, Hassan Mahdikhani, Priscilla Kyei Danso, Alireza Zohourian, Kevin Anh Truong, and Ali A Ghorbani. Towards the development of a realistic multidimensional iot profiling dataset. In *2022 19th Annual International Conference on Privacy, Security & Trust (PST)*, pages 1–11. IEEE Computer Society, 2022.

[7] Statista Research Departmentn. Internet of things (iot) connected devices installed base worldwide from 2015 to 2025. 2016.

[8] Rohan Doshi, Noah Apthorpe, and Nick Feamster. Machine learning ddos detection for consumer internet of things devices. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 29–35, 2018.

[9] Antonio Farina. Chi-square test.

[10] Blesson George. A study of the effect of random projection and other dimensionality reduction techniques on different classification methods. *Baselius Researcher*, page 201769, 2017.

[11] Brij B Gupta and Amrita Dahiya. *Distributed Denial of Service (DDoS) Attacks: Classification, Attacks, Challenges and Countermeasures*. CRC press, 2021.

[12] Poulmanogo Illy, Georges Kaddoum, Christian Miranda Moreira, Kuljeet Kaur, and Sahil Garg. Securing fog-to-things environment using intrusion detection system based on ensemble learning. In *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1–7, 2019.

[13] Justin Johnson and Taghi Khoshgoftaar. Survey on deep learning with class imbalance. *Journal of Big Data*, 6:27, 03 2019.

[14] Robert M Lee, Michael J Assante, and Tim Conway. German steel mill cyber attack. *Industrial Control Systems*, 30(62), 2014.

[15] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, 4(5):1125–1142, 2017.

[16] Huan Liu and Rudy Setiono. Chi2: Feature selection and discretization of numeric attributes. In *Proceedings of 7th IEEE International Conference on Tools with Artificial Intelligence*, pages 388–391. IEEE, 1995.

[17] Ahmed Mahfouz, Abdullah Abuhussein, Deepak Venugopal, and Sajjan Shiva. Ensemble classifiers for network intrusion detection using a novel network attack dataset. *Future Internet*, 12(11), 2020.

[18] Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Ren Ping Liu, and Wei Ni. Anatomy of threats to the internet of things. *IEEE Communications Surveys Tutorials*, 21(2):1636–1675, 2019.

[19] J. Manyika, Michael Chui, Peter Bisson, Jonathan R. Woetzel, Richard Dobbs, Jacques Bughin, and Danor Aharon. The internet of things: mapping the value beyond the hype. 2015.

[20] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Dominik Breitenbacher, Asaf Shabtai, and Yuval Elovici. N-baiot: Network-based detection of iot botnet attacks using deep autoencoders. *CoRR*, abs/1805.03409, 2018.

[21] Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things. *IEEE Internet of Things Journal*, 6(3):4815–4830, 2019.

[22] S. Gopal Krishna Patro and Kishore Kumar Sahu. Normalization: A preprocessing stage, 2015.

[23] Nishkam Ravi, Nikhil Dandekar, Preetham Mysore, and Michael L Littman. Activity recognition from accelerometer data. In *Aaai*, volume 5, pages 1541–1546. Pittsburgh, PA, 2005.

[24] Karen Scarfone, Peter Mell, et al. Guide to intrusion detection and prevention systems (idps). *NIST special publication*, 800(2007):94, 2007.

[25] Iman Sharafaldin, Arash Habibi Lashkari, and Ali A. Ghorbani. Toward generating a new intrusion detection dataset and intrusion traffic characterization. In *ICISSP*, 2018.

[26] Bayu Adhi Tama, Marco Comuzzi, and Kyung-Hyune Rhee. Tse-ids: A two-stage classifier ensemble for intelligent anomaly-based intrusion detection system. *IEEE Access*, 7:94497–94507, 2019.

[27] Chuanlong Yin, Yuefei Zhu, Jinlong Fei, and Xinzheng He. A deep learning approach for intrusion detection using recurrent neural networks. *Ieee Access*, 5:21954–21961, 2017.

[28] Bernard Zenko, Ljupco Todorovski, and Sašo Dzeroski. A comparison of stacking with meta decision trees to other combining methods. In *ICDM Proceedings A of the Fourth International Multi-Conference Information Society IS*, pages 144–147, 2001.