Intrusion Detection System using Ensemble Learning Approaches: A Systematic Literature Review

https://doi.org/10.3991/ijoe.v18i13.33519

Aouatif Arqane(✉), Omar Boutkhoum, Hicham Boukhriss,
Abdelmajid EL Moutaouakkil
Chouaib Doukkali University, El Jadida, Morocco
aouatif.arqane@gmail.com

Abstract—Undoubtedly, the advancements in Machine Learning (ML) and especially ensemble learning models enable researchers to develop numerous fields in ways we had never imagined before. Intrusion Detection System (IDS) is one of these fields that benefits from the aforementioned techniques to identify and classify the security threats with more accuracy. In fact, IDS technology has become an essential component for any defense strategy, since it provides a healthy environment for businesses. Besides, it protects future network infrastructures from intruders and suspicious network activities. In this context, this paper presents a systematic literature review on ensemble learning-based IDS and the datasets used to evaluate the proposed methods. Furthermore, we illustrate the distribution of the reviewed papers by year of publication, datasets utilized and ensemble learning methods. Finally, we discuss the finding of this review and highlight some limitations of the aforementioned models. The overall purpose of this literature review is to provide a guideline on how to choose ensemble learning models to solve IDS issues based on the most efficient and recent trends.

Keywords—intrusion detection system, ensemble learning, cyber security

1 Introduction

Because of their ability to detect the security breaches that firewalls may not identify, Intrusion Detection Systems (IDSs) have become a critical ingredient in the security strategy of any organization. An IDS is a hardware appliance or software that detects and reports any security breach or violation of network policy. The principal goal of IDS is to continuously monitor network traffic and then alert security managers when suspicious activity or known threats are identified.

Nonetheless, due to the fast advances in the internet field and the variable network behavior, traditional IDS failed to detect and forestall new intrusions in an efficient way. Consequently, and because of the popularity and success of ensemble learning models in addressing numerous mind-boggling cases in many areas, researchers have investigated the prospects of its utilization to design more accurate IDS.

An ensemble model or ensemble classifier alludes to the aggregation of multiple Machine Learning (ML) algorithms to boost the performance of the model while reducing its variance and bias. Over the last decades, this approach acquired its place as a new trend as a result of its capacity to understand and tackle numerous intricate genuine issues. In some cases, ensemble methods are proposed as the best choice over single algorithms in several domains such as education [1], cyber security [2], and healthcare [3].

Since the security of networks and IT infrastructures are recently exposed to more cyberattacks, we decide to investigate the solutions and schemes proposed in the literature to improve the detection accuracy of the traditional IDS by using ensemble methods. For this purpose, this paper presents a systematic literature review of the various state of the art about ensemble-based IDS. It first introduces the basic background regarding IDS and ensemble learning methods. Then, it cites some literature reviews about this topic while highlighting their limitations. Moreover, a systematic review methodology is followed to select and analyze 49 papers from 226 papers collected through various well-rated academic databases and search engines.

The remainder of this survey is organized as follows: Section 2 presents the background about intrusion detection systems and ensemble learning. Section 3 describes the review methodology. Section 4 introduces and discusses the results found. Eventually, the conclusion is presented in Section 5.

2 Background

2.1 Intrusion detection system

IDS is a monitoring system that identifies suspicious activities and policy violations. IDSs can be divided into two categories depending on where they seek intrusive behavior: host-based (HIDS) and network-based (NIDS). HIDS is the IDS for hosts like servers or personal computers. It analyzes the log records, folders, and files. Periodically, it takes a snapshot of the existing system files to compare them with the previous ones. After that, an alert will be generated when the HIDS detects a modification in any critical system file or undesired configuration changes. On the other hand, NIDS is used to secure networks from suspicious threats and malicious intruders, that's why it is placed at network points such as routers and gateways. Thus, they are considered passive devices because they just listen to the network conversions without interfering with the traffic they monitor.

2.2 Ensemble learning

Ensemble learning model or ensemble classifier refers to one of the top trending and notable machine learning techniques. Its objective is to produce a robust and reliable model while reducing the variance, the bias, and over-fitting. The idea behind this approach is based on the "wisdom of the crowd" theory which assumes that the collective judgment of large crowds with average awareness of a topic is better than the opinion of one expert. In other words, the combination of multiple models called base learners offers more accurate results than a single model would.

The ensemble learning methods can be categorized into two broad approaches: parallel learning and sequential learning. In a sequential learning approach, the base learners are generated sequentially which leads to data dependency. Thus, each model trained in a specific step depends on the results of models trained at the prior steps. At the end of each training step, the weights of the formerly mislabeled data must be augmented to enhance the overall performance of the system. On the contrary, in the parallel learning approach, the base learners are fitted independently from each other and in parallel series.

3 Systematic literature review

3.1 Research methodology

By adopting the general guidelines of the systematic literature review provided in [4], we designed our research methodology that is composed of the following sequential steps:

1. Specify the pertinent research questions
2. Formulate the research keywords based on the predefined research questions
3. Select the databases and libraries
4. Define the preliminary selection and inclusion/exclusion criteria
5. Conduct the research based on preliminary selection criteria and keywords
6. Exclude duplicate and non-relevant papers by reading abstract and title
7. Apply inclusion/exclusion criteria
8. Determine a quality assessment while reading the whole selected papers
9. Extract important data and analyze the findings
10. Report the review results

3.2 Research questions

The goal of this systematic literature review is to present the trends of ensemble learning models for IDS and evaluate their effectiveness based on various datasets. In Table 1, we introduce four essential research questions to attend to the objectives of this survey.

Table 1. Research questions

	Questions	Motivation
RQ1	Which ensemble models are commonly employed to enhance IDS?	Identify the most popular ensemble learning based IDS models.
RQ2	What are the most used IDS datasets to evaluate the proposed approaches?	Illustrate the main datasets that researchers rely on to assess the abilities of their solutions.
RQ3	Which simulators and programming languages are utilized to build the models?	Discover the trendy simulators and programming languages used in intrusion detection field.
RQ4	What are the metrics employed to assess the approaches?	Identify the most known metrics in the IDS context.

3.3 Paper selection

Collecting as much as possible studies or papers concerning the research topic is one of the essential steps in the literature review. In this context, we performed a literature search on various digital libraries based on some preliminary criteria. To illuminate the most recent studies and future trends in ensemble learning-based IDS, we concentrated our research on papers published during the last five years: January 2017 to December 2021. Additionally, we used the aforementioned research questions and terms related to ensemble learning and intrusion detection to formulate the required keywords. Finally, ten keywords have been formulated including “intrusion detection system”, “IDS”, “signature detection”, “anomaly detection”, “ensemble learning”, “classifier ensemble”, “voting”, “bagging”, “stacking”, and “ boosting”.

Those terms and the period of publication along with the language of publication which must be English were the preliminary criteria to select the most appropriate studies published in journals and conference proceedings. To perform the present review, we used ten well-known digital databases that are exhibited in Table 2.

Table 2. Related digital databases

Index	Digital Database	URL
1	ACM	http://www.acm.org/
2	IEEE	http://ieeexplore.ieee.org/
3	ScienceDirect	http://www.sciencedirect.com/
5	SpringerLink	http://link.springer.com/
6	Google Scholar	https://scholar.google.com/
7	Taylor and Francis	http://taylorandfrancis.com/
8	MDPI	http://www.mdpi.com/
9	Wiley	http://onlinelibrary.wiley.com
10	AIS	https://aisel.aisnet.org/

3.4 Filtering criteria

This section presents all inclusion and exclusion criteria utilized to choose the pertinent studies. Table 3 exhibits in detail the aforementioned criteria.

Table 3. Inclusion & exclusion criteria

	Inclusion Criteria
IC1	peer- reviewed literature published in journals and proceedings,
IC2	paper focuses on ensemble learning models for IDS
IC3	paper presents clearly the implementation of the proposed approach
	Exclusion Criteria
EC1	paper that is presentations, technical reports, survey or review
EC2	paper not related to the RQ
EC3	paper published in other language then English
EC4	Paper published before January 2017

3.5 Quality assessment criteria

After excluding unrelated studies, we implemented the quality assessment criteria displayed in Table 3 to refine the selected studies, and finally, keep the relevant ones to be analyzed. The quality assessment questions are ranked yes and no, and the remained studies should have no less than two yes answers. Table 4 exhibits in detail the selection process.

Table 4. Quality assessment criteria

Quality Assessment Question	**Relevant to the RQ**
Is the study subject relevant to the research topic?	RQ1, RQ2, RQ3
Have the author(s) provided a clear explanation of the methodology utilized?	RQ1, RQ2, RQ3, RQ4
Does the author(s) clearly indicate the simulator used?	RQ3
Does the author(s) provided many technical details?	RQ1, RQ2, RQ3, RQ4

4 Results and discussion

The current review aims to interpret and analyze the chosen papers to give a clear idea about the most used ensemble learning algorithms for IDS and compare their effectiveness in different datasets.

4.1 Distribution of papers by year of publication

In Figure 1 the yearly distribution of the analyzed papers is presented. As shown in this Figure, the number of published papers discussing the reviewed topic is constantly increasing. Particularly, throughout the previous two years (2020 and 2021) where the numbers of analyzed papers are 13 and 15 respectively. Accordingly, we notice that the implementation of ensemble learning methods for IDS becomes an active research area.

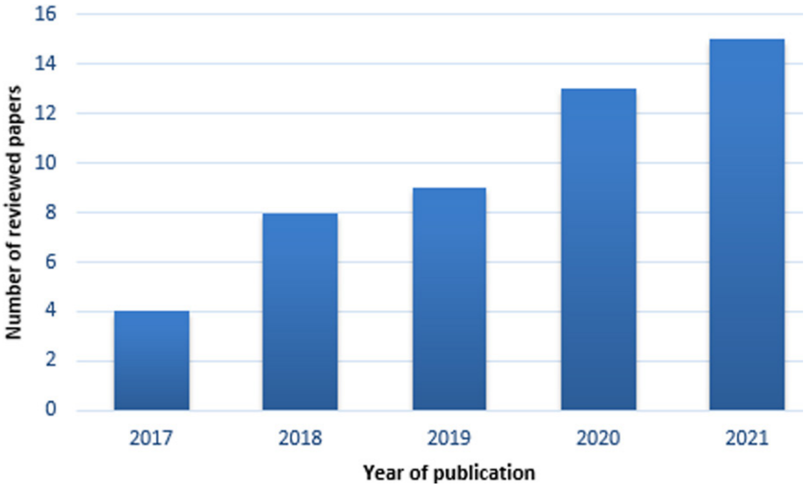

Fig. 1. Distribution of papers by year of publication

4.2 Distribution of papers by types of ensemble learning methods

In the current subsection, we shortly survey the selected papers that are grouped according to ensemble learning methods included in two categories: parallel learning and sequential learning. Following our systematic review, sequential ensemble methods especially majority voting is the most used by researches (47%), then stacking method (23%) come in second place, followed by boosting (16%) and bagging (10%).

Sequential learning. In paper [5], the authors explored the effect of consolidating information gain (IG) filter and ensemble learning classifiers on the detection performance of IDSs. They concluded that using majority voting of Partial Decision List and Random Forest (RF) outperformed the single classifiers C4.5, RF, and Partial Decision. The objective of Kumar Ahuja [6] was to provide a proficient NIDS by performing majority voting on multi-objective genetic algorithm and artificial neural networks (ANN). The assessments on ISCXIDS-2012 and NSL_KDD indicated that this approach diminished the false positive rate (FPR) by 2%. The same datasets were used by [9] to evaluate a model depending on an artificial bee colony (ABC) and AdaBoost algorithm. But the accuracy of this study (98.90) is better than the previous one (97.00). In [7], the FPR was minimized to 0.05 by deploying a shrewd IDS. This framework is composed of feature selection (FS) based on variable importance measure and Gini index (GI) alongside an ensemble of different classifiers: RF, kNN, DT, ANN and Support Vector Machine (SVM).

Fitni et al. [8] dissected the performance ameliorations in anomaly-based IDS by relying on the ensemble voting model and Spearman's rank correlation coefficient. This method helped in maximizing the accuracy. Also, by the use of the complete NSL-KDD dataset, the researchers in [10] tried the viability of a model based on NB and Random Tree combined by a sum rule scheme. In [11], the KDDcup99 dataset was utilized to assess the adequacy of an IDS based on Adaboost. After performing the ABC algorithm, the remained features were 16 out of 30 and the accomplished accuracy was close to 99%. The same dataset was employed to assess the detection accuracy of boosted trees based on IDS proposed by Bhati et al. [12] to detect Probing, Remote to User (R2L), and User to Root (U2R) attacks. The accuracy obtained was 98.9% while the overall error was 1.1%

[13] stated that implementing their novel method offered greater performance in regards to FPR, detection rate, and accuracy than many existing approaches. This method comprised of IG and principal component analysis (PCA) for dimensionally reduction (DR), and SVM, Instance-based Learning (IBL) algorithms along with Multilayered Perceptron (MLP) combined by voting as an ensemble classifier. Abbas et al. [14] reported that consolidating NB, DT, and Logistic Regression (LR) in a voting scheme could significantly improve the detection accuracy of IDS in the IoT domain. The authors of [15] also used the combination of NB and ADTree to boost the classification accuracy of an IDS. The work in [16] exploited the power of majority voting to construct a dependable IDS. The introduced ensemble classifier was made out of Sequential Minimal Optimization of SVM and MLP Neural Network.

Securing cloud computing against cyberattacks attracted the attention of authors of [17]. They decided to count on univariate ensemble FS and the DT, LR, NB, and SVM classifiers combined by majority voting to build a robust IDS. In the same context, Kunala and Duab [18] focused on reducing the computational expense and training time of an IDS by utilizing DR techniques and an ensemble of RF, RT, j48graft, REPTree, and k-NN classifiers combined by majority voting. The same scheme was used in [19] to build a framework to secure fog-to-things environment by gathering the classifiers DT, K-NN and RF. Likewise, the authors of [20] chose to uphold the protection of the cyber physical energy systems with a majority voting scheme. To do so, they aggregate the results of three individual classifiers: LightGBM, extreme learning machine (ELM), and XGBoost.

The approach presented in [21] endeavored to exploit a weighted voting scheme to design a strong IDS. The base classifiers were K-NN, SVM, NB, and DT. As per trial results, this approach had an advantage over other existing approaches in terms of maintainability and solidness. The contribution in [22] attempted to enhance the network IDS by gathering the three classifiers MLP, IBK, and J48. First, they tested the accuracy of six classifiers, then they picked the best three ones to build an effective model based on the majority voting method. Miller and Busby-Earle [23] tried to further improve the detection rate by separating features into well-defined groups. Notwithstanding, the empirical results showed that NB and Weighted Sum are better in identifying intrusions than Majority Voting*,* Bagging, Boosting, and Rotation Forest (RF). Mirza [24] performed a comparative analysis of the detection accuracy between three individual classifiers i.e. DT, LR, and neural networks, besides a weighted majority vote classifier. As a result, the author noticed that the accuracy of the ensemble learning classifier is better than the three other classifiers. In [25], the authors used the synthetic minority oversampling technique (SMOTE) and PCA with Adaboost to enhance anomaly detection. Also, Sundqvist et al. [26] demonstrated through several tests that the use of Adaboost can boost significantly the detection of anomalies in the 5G Radio Access Network.

In [27], an approach to identify intrusions in cloud computing was presented. To boost the detection performance, the authors consolidated the prediction of four classifiers i.e.: subspace discriminant, bagged tree, RUSBooted, and Boosted tree by a voting scheme. [28] stated that the mix of XGBoost, LR, and RF classifiers had emphatically a positive impact on reinforcing the security in the Internet of Softwarized Things field. The assessments on the UNSW-NB15 dataset certified that the accuracy can accomplish 99% with the use of the crow search algorithm for FS. Timčenko and Gajin [29] decided to utilize the UNSW-NB15 dataset to evaluate and compare the learning capacities of five boosting methods i.e.: LogitBoost, AdaBoost, GentleBoost, RUSBoost, and Bagged trees. By experiments, the authors mentioned that the highest performance was obtained by GentleBoost and Bagged trees, while RUSBoost was sorted as the less powerful classifier.

The dataset NSL-KDD 99 was used in [30] to evaluate the performance of five ML methods i.e.: Bagging, AdaBoost, Stacking, J48, and PART but this time with different FS techniques like correlation, Chi-square, Information Gain, Gain Ratio, Symmetrical Uncertainty, and One Rule. Exploratory outcomes showed that Adaboost with all FS techniques except correlation performed better than the other cited methods. [31] provided an alternate approach to enhance NIDS accuracy by utilizing Long Short-Term Memory (LSTM) and Auto-encoder consolidated by the weighted average scheme. The authors asserted that their approach is versatile in real-world situations and has a relearning of new models ability. The authors of [32] decided to take advantage of ensemble methods progress to preserve marine IoT sensors. They developed a methodology composed of label encoding for FS and an amended Light-GBM to handle the issue of distributed IoT assaults. In [33] an analytic comparison of different tree-based ensemble learning algorithms i.e.: Gradient Boost, Extra tree, RF, Light GBM, and XGBoost was conducted on the BoT-IoT dataset. The final results showed that Light GBM outperformed the other cited methods in terms of accuracy, precision, recall, F1, and detection time.

Parallel learning. Rajadurai and Gandhi [34] compared the general performance of an IDS-based stacking ensemble model against ten distinct models. The stacking model includes GB and RF as base learners and a meta-model. After the assessments, the authors reasoned that the proposed model can offer a better detection accuracy than the other ones especially bagging and boosting. A two-phase ensemble model based on RF and bagging was presented in [35] to build an anomaly-based IDS. Results of the experiments on NSL-KDD and UNSW-NB15 affirmed that this model had a good impact on the accuracy, detection rate, and sensitivity. Verma and al. [36] compared the viability of four tree ensemble classifiers named: Boosted Trees, Subspace Discriminant, Bagged Trees, and RUSBoosted Trees in identifying assaults against IPv6. The outcomes showed that Boosted Trees achieved the highest accuracy (94.4%) while the lowest accuracy was achieved by Subspace Discriminant (78.6%). A stacking learning model that includes SVM, RF, and auto-encoder was compared against the classical ML models: multiplayer perception, SVM, and RF in [37]. The authors confirmed that this approach was dependable in terms of accuracy, recall, and precision. Also, it was operable in various standalone networks.

In [38], experiments in KDDcup99 and NSL-KDD datasets affirmed that the mix of Recursive Feature Elimination and stacking model can enhance the detection rate of an IDS. Also, a stacking model was used in [39] to improve the performance of NIDS using heterogeneous Datasets. In [40], the authors tested the influence of using Optimum-Path Forest classifiers as a stacking ensemble on the performance of an IDS. The evaluations conducted on NSL-KDD and uneSPY (private dataset), demonstrated the ability of this approach to maintain its adequacy while dealing with big data. In [41], the authors performed many experiments on the AWID dataset to discover the best ensemble-based IDS for Wi-Fi networks among four different classifiers. They concluded that the detection accuracy of RF outperformed the other classifiers. Priyajit and Tuhina [42] focused on upgrading anomaly detection in wireless sensor networks by employing the ensemble model RF. The base learners of the ensemble were DT, K-NN, and NB. The results confirmed the advantage of utilizing the RF over the three mentioned classifiers separately.

The subject of distributed anomaly detection was discussed in [43] and an appropriate framework was proposed. The blending framework is composed of level 0 which contains LR and RF and SVM as level 1 learner. On a similar point, Khraisat and al. [44] argued that the stacking method composed of C5.0 DT as level 0 and SVM as level 1 can enhance the detection rate and reduce the FPR of IDSs. In [45], experiments conducted on the NSL-KDD dataset with a subset of 35 features affirmed that the bagging model with the base classifier J48 can give better accuracy and a lower FAR than boosting model with the same base classifier. Saba [46] investigated the opportunity of implementing ensemble learning models to protect Internet of Medical Things devices. To do so, the author tested the performance of six different ensemble learning algorithms on the KDDcup99 dataset with PCA. The results indicated that bagging with DT as a base learner is slightly better than Extra Trees, RF, Stochastic Gradient Boosting, and Adaboost. The authors of [47] performed a comparative analysis to discover the best ensemble model to detect intrusions in databases. After several tests, they presumed that the use of Ordering Points To Identify the Clustering Structure (OPTICS) alongside the stacking approach outperformed numerous classifiers such as rule induction and DT with different base learners.

Tama and Rhee [48] fulfilled a similar investigation of the viability of five ensemble methods i.e.: voting, boosting, bagging, RF, and stacking on NSL-KDD with eight picked features. In light of the assessment results, stacking and boosting with C4.5 base learner had the best performance in terms of accuracy, recall, precision. In [49], the topic of anomaly detection in IoT devices was tackled. The proposed approach was deployed on software-defined networks regulator and employed auto-encoder as FS along with stacking method as a classifier. The work in [50] focused on improving the learning capabilities of ensemble learning methods by employing the feature fusion technique to build various groups of extensive feature datasets. The tests conducted on NSL-KDD, KDDcup99, UNSW-NB15, and CIC-IDS2017 with the stacking method revealed that the proposed approach could significantly boost the detection rate of NIDS. The study in [51] applied a novel intrusion detection approach based on a CFS-BA technique for FS and an aggregation of RF, Forest Penalizing Attributes, and C4.5 for the training step. This approach was tested on AWID, NSL-KDD and CIC-IDS2017 datasets and the authors affirmed that the highest detection rate achieved was 99.9% by using the CIC-IDS2017 dataset with subset 13 features.

A combination of LightGBM, RF, DT, kNN, and XGBoost is used in [52] to build a framework that is robust enough to identify many kinds of attacks. The experimental results indicated that the performance of the proposed framework based on the voting approach is better than individual algorithms. In [53], the authors counted on the majority voting approach to construct an accurate IDS for SCADA-based power grids. The evaluation of the proposed method that includes nine heterogeneous classifiers showed improvements in accuracy, precision, F1 score, and recall.

4.3 Distribution of papers by datasets

According to our review NSL-KDD dataset is the most utilized one (32%). The CIC-IDS-2017 (25%) come in second place followed by KDDcup99 (10%), UNSW-NB15 (9%), and Kyoto 2006+ (6%). Other datasets like ISCX-2012 (4%), CSE-CIC-IDS2018 (3%), and BoT-IoT (3%) are less popular in the IDS field.

Table 5 illustrates information about reviewed papers achieving the best accuracy by using the five most used datasets.

Table 5. Best accuracy achieved in the five most used datasets

Dataset	Paper	Method	Accuracy	FS & DR
NSL-KDD	[9]	AdaBoost	99.86	ABC
CIC-IDS-2017	[51]	C4.5 + RF + PA	99.90	CFS-BA
KDD Cup 99	[11]	Adaboost	99.92	ABC
UNSW-NB15	[50]	DT + RF	99.95	Feature fusion
Kyoto 2006+	[13]	IBL + MLP + SVM	98.95	IG-PCA

4.4 Distribution of papers by simulators

Figure 2 exhibits the percentage of every simulator and programming language employed to assess the approaches in the reviewed papers. Depending on the results, Python is the first choice of researchers to build the ensemble learning-based IDS. The second choice is Weka which is open-source software for data mining tasks. While Matlab is less popular in the domain of ensemble learning.

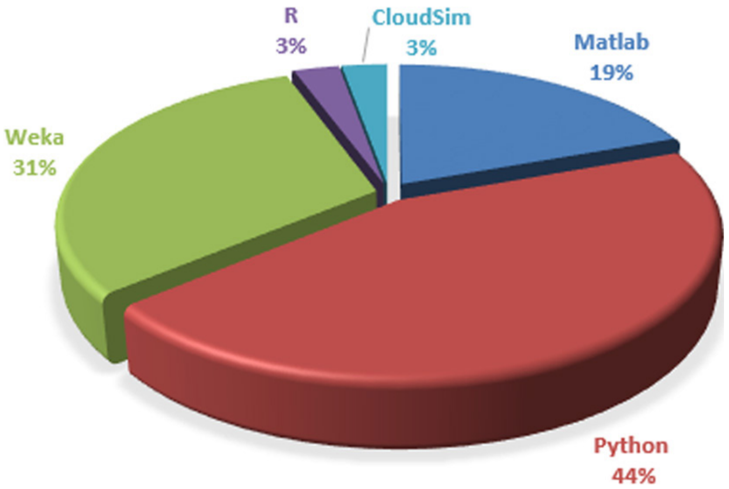

Fig. 2. Percentage of simulators used in reviewed papers

4.5 Distribution of papers by metrics

Figure 3 represents the metrics applied to assess the outlined approaches. As displayed, the most commonly used metrics are accuracy, precision, F1-score, and recall. Notwithstanding that these metrics show the general performance of an IDS, we confirm that other metrics such as detection rate and resource usage indicate a clearer idea about the optimal model to choose, especially in the Internet of Things field.

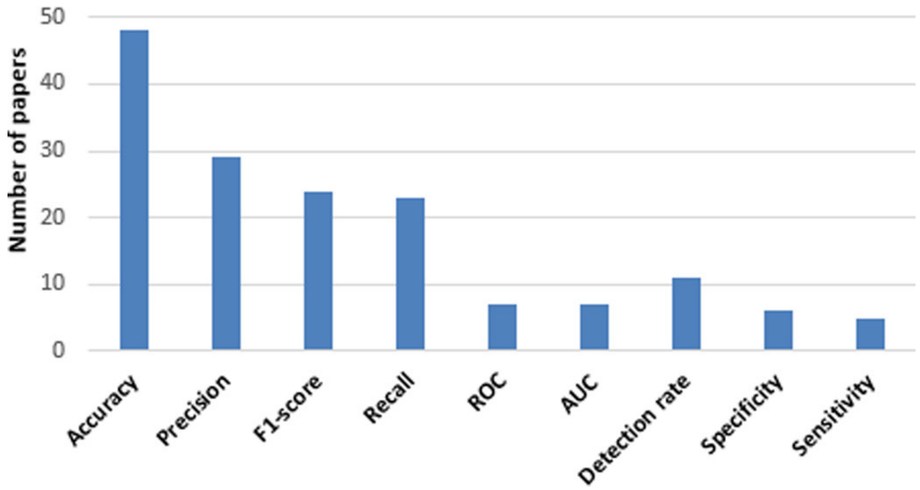

Fig. 3. Distribution of papers by metrics

5 Conclusion

Nowadays, the complexity and severity of cyberattacks increase the need for reliable security systems. Accordingly, the present systematic literature review aims to provide in-depth information about the datasets, models, programming language, FS and DR techniques commonly utilized to improve the performance of IDSs.

According to our review, we conclude that using ensemble learning models instead of single ones can improve the detection performance of an IDS, as shown in some studies like [5], [9], [13], [21], [23], [38], and [40]. Additionally, we are convinced that these models are very beneficial in some cases, like bootstrapping samples of small datasets and reducing the computational expense. On the other hand, the predominant of analyzed papers prefer utilizing NSL-KDD dataset and majority voting scheme to boost the performance of their IDS along with FS and DR techniques. For the programming language, python is the prevalent among security developers.

Finally, we would like to point out that the present work does not investigate in-depth the aspects of each ensemble learning category, which is an opportunity for other researchers to make a review and a comparative analysis in this field.

6 References

[1] Yu, J.: Academic Performance Prediction Method of Online Education using Random Forest Algorithm and Artificial Intelligence Methods. International Journal of Emerging Technologies in Learning (iJET). 16, 45–57 (2021). https://doi.org/10.3991/ijet.v16i05.20297

[2] Oladepo, A.G., Bajeh, A.O., Balogun, A.O., Mojeed, H.A., Salman, A.A., Bako, A.I.: Heterogeneous Ensemble with Combined Dimensionality Reduction for Social Spam Detection. International Journal of Interactive Mobile Technologies (iJIM). 15, 84–103 (2021). https://doi.org/10.3991/ijim.v15i17.19915

[3] Kumarasinghe, H., Kolonne, S., Fernando, C., Meedeniya, D.: U-Net Based Chest X-ray Segmentation with Ensemble Classification for Covid-19 and Pneumonia. International Journal of Online and Biomedical Engineering (iJOE). 18, 161–175 (2022). https://doi.org/10.3991/ijoe.v18i07.30807

[4] Brereton, P., Kitchenham, B.A., Budgen, D., Turner, M., Khalil, M.: Lessons From Applying The Systematic Literature Review Process Within The Software Engineering Domain. Journal of Systems and Software. 80, 571–583 (2007). https://doi.org/10.1016/j.jss.2006.07.009

[5] Abdullah, M., Balamash, A., Al-Shannaq, A., Almabdy, S.: Enhanced Intrusion Detection System using Feature Selection Method and Ensemble Learning Algorithms. International Journal of Computer Science and Information Security. 16, 48–55 (2018).

[6] Kumar Ahuja, Dr. G.: An Improved Ensemble Approach For Effective Intrusion Detection. The Journal of Supercomputing. 76 (2020). https://doi.org/10.1007/s11227-019-03035-w

[7] Rajadurai, H., Gandhi, U.D.: A Stacked Ensemble Learning Model For Intrusion Detection In Wireless Network. Neural Comput & Applic. (2020). https://doi.org/10.1007/s00521-020-04986-5

[8] Fitni, Q.R.S., Ramli, K.: Implementation of Ensemble Learning and Feature Selection for Performance Improvements in Anomaly-Based Intrusion Detection Systems. In: 2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT). 118–124 (2020). https://doi.org/10.1109/IAICT50021.2020.9172014

[9] Mazini, M., Shirazi, B., Mahdavi, I.: Anomaly Network-Based Intrusion Detection System Using A Reliable Hybrid Artificial Bee Colony And Adaboost Algorithms. Journal of King Saud University - Computer and Information Sciences. 31, 541–553 (2019). https://doi.org/10.1016/j.jksuci.2018.03.011

[10] Kevric, J., Jukic, S., Subasi, A.: An Effective Combining Classifier Approach Using Tree Algorithms For Network Intrusion Detection. Neural Comput. Appl. 28, 1051–1058 (2017). https://doi.org/10.1007/s00521-016-2418-1

[11] Mousavi, S., Majidnezhad, V., Naghipour, A.: A New Intelligent Intrusion Detector Based On Ensemble Of Decision Trees. Journal of Ambient Intelligence and Humanized Computing. (2019). https://doi.org/10.1007/s12652-019-01596-5

[12] Bhati, B.S., Rai, C.S., Balamurugan, B., Al-Turjman, F.: An Intrusion Detection Scheme Based On The Ensemble Of Discriminant Classifiers. Computers & Electrical Engineering. 86, 106742 (2020). https://doi.org/10.1016/j.compeleceng.2020.106742

[13] Salo, F., Nassif, A.B., Essex, A.: Dimensionality Reduction With Ig-Pca And Ensemble Classifier For Network Intrusion Detection. Comput. Networks. (2019). https://doi.org/10.1016/j.comnet.2018.11.010

[14] 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

[15] Akhil, J., Srinivas, K., Reddy, S.: A Novel Intelligent Ensemble Classifier for Network Intrusion Detection System. Presented at the December 1 (2018).

[16] Abdulrahaman, M., Alhassan, K.: Ensemble Learning Approach for the Enhancement of Performance of Intrusion Detection System. Presented at the September 5 (2018).

[17] Veni, K., Sivamohan, S., Subramanian, S., Prabakaran, S.: Efficient Feature Selection And Classification Through Ensemble Method For Network Intrusion Detection On Cloud Computing. Cluster Computing. 24, 1–19 (2021). https://doi.org/10.1007/s10586-020-03222-y

[18] Kunal, Dua, M.: Attribute Selection and Ensemble Classifier based Novel Approach to Intrusion Detection System. Procedia Computer Science. 167, 2191–2199 (2020). https://doi.org/10.1016/j.procs.2020.03.271

[19] Illy, P., Kaddoum, G., Moreira, C.M., Kaur, K., Garg, S.: Securing Fog-to-Things Environment Using Intrusion Detection System Based On Ensemble Learning. In: 2019 IEEE Wireless Communications and Networking Conference (WCNC). 1–7. IEEE Press, Marrakesh, Morocco (2019). https://doi.org/10.1109/WCNC.2019.8885534

[20] Li, Y., Xue, W., Wu, T., Wang, H., Zhou, B., Aziz, S., He, Y.: Intrusion Detection Of Cyber Physical Energy System Based On Multivariate Ensemble Classification. Energy. 218, 119505 (2021). https://doi.org/10.1016/j.energy.2020.119505

[21] Li, X., Zhu, M., Yang, L.T., Xu, M., Ma, Z., Zhong, C., Li, H., Xiang, Y.: Sustainable Ensemble Learning Driving Intrusion Detection Model. IEEE Transactions on Dependable and Secure Computing. 18, 1591–1604 (2021). https://doi.org/10.1109/TDSC.2021.3066202

[22] Mahfouz, A., Abuhussein, A., Venugopal, D., Shiva, S.: Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset. Future Internet. 12, 180 (2020). https://doi.org/10.3390/fi12110180

[23] Miller, S.T., Busby-Earle, C.: Multi-Perspective Machine Learning a Classifier Ensemble Method for Intrusion Detection. In: Proceedings of the 2017 International Conference on Machine Learning and Soft Computing. 7–12. Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3036290.3036303

[24] Mirza, A.H.: Computer Network Intrusion Detection Using Various Classifiers And Ensemble Learning. In: 2018 26th Signal Processing and Communications Applications Conference (SIU). 1–4 (2018). https://doi.org/10.1109/SIU.2018.8404704

[25] Qu, Z., Liu, H., Wang, Z., Xu, J., Zhang, P., Zeng, H.: A Combined Genetic Optimization With Adaboost Ensemble Model For Anomaly Detection In Buildings Electricity Consumption. Energy and Buildings. 248, 111193 (2021). https://doi.org/10.1016/j.enbuild.2021.111193

[26] Sundqvist, T., Bhuyan, M.H., Forsman, J., Elmroth, E.: Boosted Ensemble Learning for Anomaly Detection in 5G RAN. In: Maglogiannis, I., Iliadis, L., and Pimenidis, E. (eds.) Artificial Intelligence Applications and Innovations. 15–30. Springer International Publishing, Cham (2020). https://doi.org/10.1007/978-3-030-49161-1_2

[27] Singh, P., Ranga, V.: Attack And Intrusion Detection In Cloud Computing Using An Ensemble Learning Approach. Int. J. Inf. Tecnol. 13, 565–571 (2021). https://doi.org/10.1007/s41870-020-00583-w

[28] Srivastava, G., Deepa, N., Prabadevi, B., Praveen Kumar Reddy M.: An Ensemble Model For Intrusion Detection In The Internet of Softwarized Things. In: Adjunct Proceedings of the 2021 International Conference on Distributed Computing and Networking. 25–30. Association for Computing Machinery, New York, NY, USA (2021). https://doi.org/10.1145/3427477.3429987

[29] Timčenko, V., Gajin, S.: Ensemble Classifiers For Supervised Anomaly Based Network Intrusion Detection. In: 2017 13th IEEE International Conference on Intelligent Computer Communication and Processing (ICCP). 13–19 (2017). https://doi.org/10.1109/ICCP.2017.8116977

[30] Vinutha, H.P., Poornima, B.: An Ensemble Classifier Approach on Different Feature Selection Methods for Intrusion Detection. Presented at the January 1 (2018).

[31] Zhong, Y., Chen, W., Wang, Z., Chen, Y., Wang, K., Li, Y., Yin, X., Shi, X., Yang, J., Li, K.: HELAD: A Novel Network Anomaly Detection Model Based On Heterogeneous Ensemble Learning. Computer Networks. 169, 107049 (2020). https://doi.org/10.1016/j.comnet.2019.107049

[32] Tiwari, D., Bhati, B.S., Nagpal, B., Sankhwar, S., Al-Turjman, F.: An Enhanced Intelligent Model: To Protect Marine Iot Sensor Environment Using Ensemble Machine Learning Approach. Ocean Engineering. 242, 110180 (2021). https://doi.org/10.1016/j.oceaneng.2021.110180

[33] Chauhan, P., Atulkar, M.: Selection of Tree Based Ensemble Classifier for Detecting Network Attacks in IoT. In: 2021 International Conference on Emerging Smart Computing and Informatics (ESCI). 770–775 (2021). https://doi.org/10.1109/ESCI50559.2021.9397033

[34] Khonde, S. R., Ulagamuthalvi, V.: Ensemble-Based Semi-Supervised Learning Approach For A Distributed Intrusion Detection System. Journal of Cyber Security Technology. 3, 163–188 (2019). https://doi.org/10.1080/23742917.2019.1623475

[35] Tama, B.A., Comuzzi, M., Rhee, K.-H.: TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. IEEE Access. 7, 94497–94507 (2019). https://doi.org/10.1109/ACCESS.2019.2928048

[36] Verma, A., Ranga, V.: ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things. In: 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). 1–6 (2019). https://doi.org/10.1109/IoT-SIU.2019.8777504

[37] Hsu, Y.-F., He, Z., Tarutani, Y., Matsuoka, M.: Toward an Online Network Intrusion Detection System Based on Ensemble Learning. In: 2019 IEEE 12th International Conference on Cloud Computing (CLOUD). 174–178 (2019). https://doi.org/10.1109/CLOUD.2019.00037

[38] Lian, W., Nie, G., Jia, B., Shi, D., Fan, Q., Liang, Y.: An Intrusion Detection Method Based on Decision Tree-Recursive Feature Elimination in Ensemble Learning. Mathematical Problems in Engineering. 2020, e2835023 (2020). https://doi.org/10.1155/2020/2835023

[39] Rajagopal, S., Kundapur, P.P., Hareesha, K.S.: A Stacking Ensemble for Network Intrusion Detection Using Heterogeneous Datasets. Security and Communication Networks. 2020, e4586875 (2020). https://doi.org/10.1155/2020/4586875

[40] Bertoni, M.A., Rosa, G. de, Brega, J.R.: Optimum-Path Forest Stacking-Based Ensemble For Intrusion Detection. (2021). https://doi.org/10.1007/s12065-021-00609-7

[41] Vaca, F.D., Niyaz, Q.: An Ensemble Learning Based Wi-Fi Network Intrusion Detection System (WNIDS). In: 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA). 1–5 (2018) https://doi.org/10.1109/NCA.2018.8548315

[42] Biswas, P., Samanta, T.: Anomaly Detection Using Ensemble Random Forest In Wireless Sensor Network. Int. J. Inf. Tecnol. 13, 2043–2052 (2021). https://doi.org/10.1007/s41870-021-00717-8

[43] Jain, M., Kaur, G.: Distributed Anomaly Detection Using Concept Drift Detection Based Hybrid Ensemble Techniques In Streamed Network Data. Cluster Computing. 24, 1–16 (2021). https://doi.org/10.1007/s10586-021-03249-9

[44] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J., Alazab, A.: Hybrid Intrusion Detection System Based on the Stacking Ensemble of C5 Decision Tree Classifier and One Class Support Vector Machine. Electronics. 9, 173 (2020). https://doi.org/10.3390/electronics9010173

[45] Pham, N.T., Foo, E., Suriadi, S., Jeffrey, H., Lahza, H.F.M.: Improving performance of intrusion detection system using ensemble methods and feature selection. In: Proceedings of the Australasian Computer Science Week Multiconference. 1–6. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3167918.3167951

[46] Saba, T.: Intrusion Detection in Smart City Hospitals using Ensemble Classifiers. In: 2020 13th International Conference on Developments in eSystems Engineering (DeSE). 418–422 (2020). https://doi.org/10.1109/DeSE51703.2020.9450247

[47] Subudhi, S., Panigrahi, S.: Application of OPTICS and Ensemble Learning for Database Intrusion Detection. Journal of King Saud University - Computer and Information Sciences. (2019). https://doi.org/10.1016/j.jksuci.2019.05.001

[48] Adhi Tama, B., Rhee, K.H.: Performance Evaluation Of Intrusion Detection System Using Classifier Ensembles. International Journal of Internet Protocol Technology. 10, 22 (2017). https://doi.org/10.1504/IJIPT.2017.083033

[49] Tsogbaatar, E., Bhuyan, M., Taenaka, Y., Fall, D., Gonchigsumlaa, K., Elmroth, E., Kadobayashi, Y.: SDN-Enabled IoT Anomaly Detection Using Ensemble Learning. Presented at the May 29 (2020). https://doi.org/10.1007/978-3-030-49186-4_23

[50] Zhang, H., Li, J.-L., Liu, X.-M., Dong, C.: Multi-Dimensional Feature Fusion And Stacking Ensemble Mechanism For Network Intrusion Detection. Future Generation Computer Systems. 122, 130–143 (2021). https://doi.org/10.1016/j.future.2021.03.024

[51] Zhou, Y., Cheng, G., Jiang, S., Dai, M.: Building An Efficient Intrusion Detection System Based On Feature Selection And Ensemble Classifier. Computer Networks. 174, 107247 (2020). https://doi.org/10.1016/j.comnet.2020.107247

[52] Seth, S., Chahal, K.K., Singh, G.: A Novel Ensemble Framework for an Intelligent Intrusion Detection System. IEEE Access. 9, 138451–138467 (2021). https://doi.org/10.1109/ACCESS.2021.3116219

[53] Upadhyay, D., Manero, J., Zaman, M., Sampalli, S.: Intrusion Detection in SCADA Based Power Grids: Recursive Feature Elimination Model With Majority Vote Ensemble Algorithm. IEEE Transactions on Network Science and Engineering. 8, 2559–2574 (2021). https://doi.org/10.1109/TNSE.2021.3099371

7 Authors

Aouatif Arqane is a PhD student at LAROSERI Laboratory, Department of Computer Science, Chouaib Doukkali University,El Jadida, Morocco. Here research interests are in the application of Machine Learning models in intrusion detection field.

Omar Boutkhoum is an Associate Professor at computer Science department in the Faculty of Sciences of Chouaib Doukkali University, EL Jadida, Morocco. His research interests are in the application of decision support systems and Blockchain technology to sustainable supply chain management.

Hicham Boukhriss is a PhD student at LAROSERI Laboratory, Department of Computer Science, Chouaib Doukkali University,El Jadida, Morocco. His research interests are in the application of Blockchain in intrusion detection field.

Abdelmajid EL Moutaouakkil is an Associate Professor at computer Science department in the Faculty of Sciences of Chouaib Doukkali University, EL Jadida, Morocco. His research interests are in medical image processing.

Article submitted 2022-06-21. Resubmitted 2022-09-06. Final acceptance 2022-09-08. Final version published as submitted by the authors.