

Anomaly-based intrusion detection system based on feature selection and majority voting

Mina Eshak Magdy¹, Ahmed M. Matter², Saleh Hussin¹, Doaa Hassan³, Shaimaa Ahmed Elsaid¹

¹Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, Egypt

²Department of Computer Engineering and Artificial Intelligence, Military Technical College, Cairo, Egypt

³Department of Computers and Systems, National Telecommunication Institute, Cairo, Egypt

Article Info

Article history:

Received Jun 4, 2022

Revised Feb 8, 2023

Accepted Feb 23, 2022

Keywords:

Adaptive voting

Cyber-security

Deep learning

Intrusion detection system

Machine learning

ABSTRACT

Recently, cyberattacks have been more complex than in the past, as a new cyber-attack is initiated almost every day. Therefore, researchers should develop efficient intrusion detection systems (IDS) to detect cyber-attacks. In order to improve the detection and prevention of the aforementioned cyber-attacks, several articles developed IDSs exploiting machine learning and deep learning. In this paper, a way to find network intrusions using a combination of feature selection and adoptive voting is investigated. NSL-KDD dataset, a high-dimensional dataset that has been widely used for network intrusion detection, is applied in this approach. Feature selection plays an important role for improving accuracy and testing time as it eliminates the less significant attributes from the data set, thus saving computational power and effort. The experimental results show that the proposed approach achieves an accuracy of 86.5% on the NSL-KDD test dataset using an adoptive voting algorithm trained with the selected features. In addition, the time to process each record is 97.5 microseconds, which reflects the proposed model's superior performance. Comparing the proposed model with the existing models in the literature shows that the proposed adaptive voting approach significantly improves intrusion detection accuracy, enhances computational efficiency, and reduces false positives.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Mina Eshak Magdy

Department of Electronics and Communications, Faculty of Engineering, Zagazig University

Zagazig University, Zagazig, Egypt

Email: memw22@gmail.com

1. INTRODUCTION

The communication systems make the world smaller by connecting people via many ways starting from simple way like old telephones, then developing computer systems, followed by smart phones with all of internet applications like social media, trading and financial platforms. Finally, internet of things (IoT) [1] where everything is connected to internet where communication is not limited to humans but also the newly invented devices. All this communication systems mostly designed to provide all means of linking between entities, but it does not design to provide security measures. Therefore, these systems are prone to cyber-attacks which is considered the main threat to existing communication systems. Many research attempts had been conducted focusing on cyber-attacks to minimize their risks as much as possible. One of the important technologies to achieve systems security is the intrusion detection system (IDS). IDSs are divided in two categories: signature-based IDSs, where attacks can be eliminated based on their signatures and anomaly IDSs, While the attacks can be detected based on their behavior. A lot of researchers have been seeking to enhance the detection performance of IDSs; most of them employed approaches based on machine learning (ML). The importance of picking

significant or deleting less features from a dataset was implied with feature selection [2]. Feature selection is considered a crucial process to improve the performance of IDSs.

Internet of things is connecting users globally without human intervention. It utilizes smart devices to connect everything to the Internet. IoT applications are susceptible to security vulnerabilities that must be mitigated. Users' safety and privacy have been compromised because of the fast increase of network intrusions. The following are the main contributions of this paper:

- A novel approach is proposed which consolidates the advantages of majority voting machine learning classifier alongside feature selection. The main goal of the proposed approach is providing an effective and precise intrusion detection system.
- With regards to feature selection, wrapper-Based approach for assessing the relationship between the selected features and maximizing training/testing phase efficiencies is presented.

The remainder of the paper is structured as follows: literature review is covered in section 2. Section 3 describes the proposed system briefly. Performance analysis of the proposed system and a comparison to existing systems are analyzed in section 4. Section 5 presents the conclusion.

2. LITERATURE REVIEW

Recently, several IDSs utilize ML or deep neural network (DNN) techniques to increase its attack-detection efficiency. Machine learning based IDSs were presented, analyzed, and compared to others in [3]. The importance of feature extraction in the classifying and training phases of ML IDS is illustrating feature selection affects the performance of ML based IDS in [4], authors highlight the challenges and present unsupervised feature learning called the nonsymmetric deep autoencoder (NDAE). SCDNN approach conjugates deep neural network (DNN) and spectral clustering (SC) algorithms was proposed in [5]. Based on self-taught learning (STL) framework [6], a successful deep learning technique called self-taught learning (STL)-IDS which is used to learn features and reduce dimensionality. It significantly saves training and testing time while significantly improving support vector machine (SVM) attack prediction accuracy. In terms of enhancing accuracy of the system, a 5-level hybrid categorization approach based on flow statistics was presented in [7]. They use the k-nearest neighbor method (KNN) for the first level, and the extreme learning machine (ELM) for the second level. A framework named DFEL was introduced in [8] to identify internet infiltration in the IoT paradigm in order to avert irreparable cyberattack damage. The authors demonstrated that DFEL also improves classifiers' accuracy in predicting cyber-attacks, and also considerably reduces detection time. Using MultiTree algorithm with adaptive voting algorithm leading to an improve in binary classification as shown in [9]. A comparison is conducted to evaluate the most significant approach was summarized in Table 1.

Table 1. Literature review

Ref.	Approach	Accuracy	Precision	Recall	F1-score	False positive rate	training time(s)	testing time(s)	specificity
[10]	Deep neural network (DNN)	75.75	83	76	75	-	-	-	-
[11]	Convolutional neural network (CNN)	79.48	23.4	68.66	-	27.90	-	-	-
[12]	self-taught learning (STL) + SVM	84.96	96.23	76.57	85.28	-	673.031	4.648	-
[13]	Adaptive ensemble learning	85.2	86.5	85.2	84.9	-	-	-	-
[14]	Deep neural network (DNN), Hybrid intrusion detection framework called SHIA	80.1	69.2	96.9	80.7	-	-	-	-
[15]	Improved conditional variational autoencoder (ICVAE-DNN)	85.97	97.39	77.43	86.27	2.74	-	-	-
[16]	Self-taught learning alongside with MAPE-K (self-adaptive system)	77.99	-	60.34	-	0.4	-	-	-
[17]	Autoencoder (AE)	84.24	87	80.37	81.98	0.4	-	-	-
[18]	Deep learning spark intrusion detection system (DLS-IDS)	83.57	96.46	78.12	86.32	3.57	-	-	96.43
[19]	Difficult set sampling technique (DSSTE)+alexnet	82.84	83.94	82.78	81.66	-	-	-	-

3. THE PROPOSED SYSTEM

Figure 1 shows the framework of the proposed IDS system. It is a hybrid approach based on feature selection and adaptive voting and it is applied for network intrusion detection. It utilizes wrapper method that utilizes j48 tree to select optimal features which can be employed to improve the accuracy and lessen the testing time. Although wrapper method takes much time, it is very effective in terms of finding optimal features which results in 13 optimum features shown in Table 2. After applying the features selection algorithm, the classifiers (J48, REPTREE, LMT, and ConjunctiveRule) are trained using the optimal features of the KDDtrain+ dataset. Then, the voting algorithm is developed, it uses several classifiers to execute the decision process [20] by using the combination rule for its decision. KDDtrain+ dataset is partitioned into many sub-sets through majority voting, and several classifiers are employed to train them and complete the learning process. Based on the number of votes collected in favour of a given class gathered from several classifiers, the final outcome of giving a label to the record is determined. After model building, its performance was evaluated using the same 13 selected features on the KDDTest+ dataset. The proposed approach is described as follows and its framework is shown in Figure 1.

- Apply the feature selection wrapper technique which utilize J48 algorithm to the training dataset to select the 13 optimal features.
- Train the machine learning classifiers whether tree or rule technique-based algorithm using the training dataset.
- Combine J48, REPTREE, LMT trees, and conjunctive rule; the combination method applied is majority voting.
- Building and evaluating the model on the testing dataset after applying the feature selection technique.

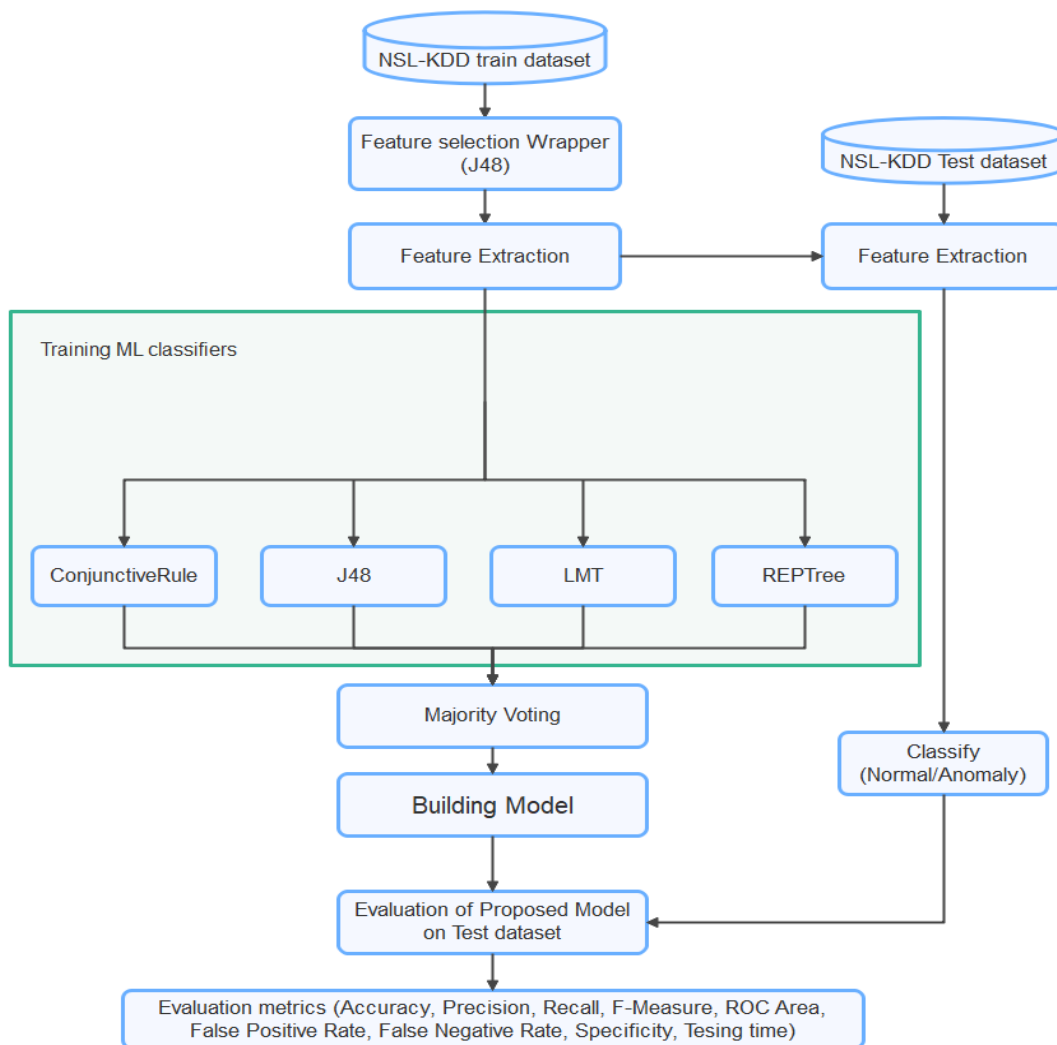


Figure 1. Proposed system framework

3.1. Dataset and pre-processing

KDD99 [8] is one of the most commonly used cyber security research datasets that was developed in 1999. Experiments revealed some disadvantages of KDD99 that should be fixed, for example, overt repetitiveness and the irrational number of records in train and test dataset making it hard to deal with. To defeat the previously mentioned drawbacks, a more uptodate adaptation was proposed in NSL-KDD [21]. NSLKDD has been regarded as the new standard dataset for cyber security research since 2009. Figure 2 presents the whole NSL-KDD Records. This benchmark dataset consists of KDDTrain+ (125,973) records for training as shown in Figure 2(a) and KDDTest+ 22,544 records for testing as shown in Figure 2(b). Each record has 41 features that fall into four main feature categories, including [22]: time-based traffic features, content features, basic features, and connection-based traffic features.

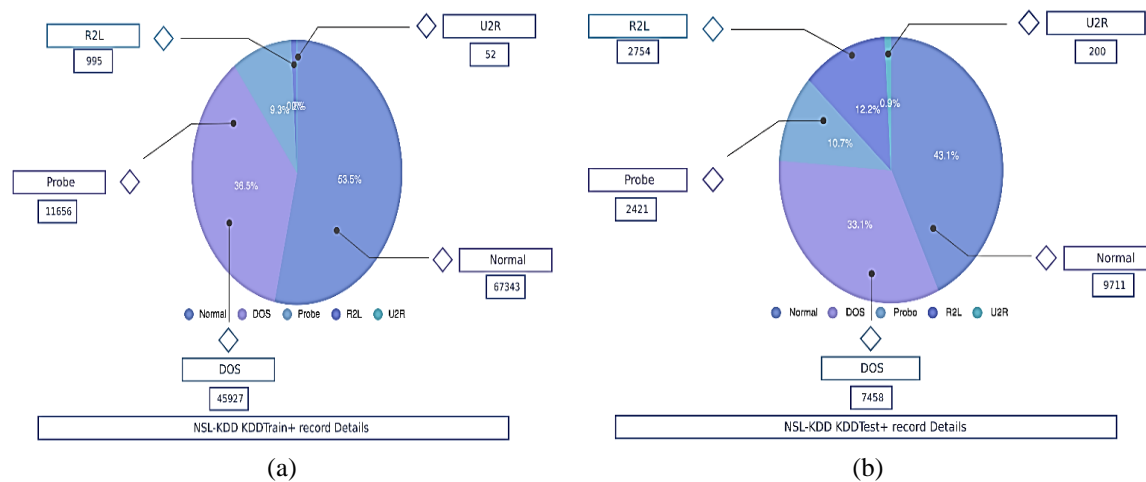


Figure 2. NSL-KDD records (a) train dataset and (b) test dataset

3.2. Classifiers

A vast amount of structured and unstructured data is one resource that we have in abundance in this era of modern technological advancements. The discipline of computer programming that derives knowledge from experience is called machine learning (ML). Algorithms for self-learning that generate knowledge from data and make predictions are involved. A typical machine learning (ML) model learns in three stages: it generates a pattern based on input data for decision-making, uses an error function to compare the model to known instances, and then updates its weight values to reduce the error between known examples and model estimation for optimization. The ML model data is divided into two sets during the learning process: training and testing. Following is a brief description of ML classifiers considered in this research.

3.2.1. J48

J48 is one of the most common classification algorithms, passing via decision tree evaluates every node in order to select best split depending on the value of maximum gain ratio. This algorithm builds decision trees based on a set of training data in the same way the ID3 algorithm does. It also use the concept of information entropy.

3.2.2. Random forest

Random forest is also characterized as a decision tree algorithm since it works by building several decision trees. It classifies numerous of input variables based on its importance without removing any variables, it also known with its ability to decrease bias [23]. Random forests are frequently used as black box models in businesses, as they generate reasonable predictions across a wide range of data while requiring little configuration.

3.2.3. LMT

Logistic model tree (LMT) is a machine learning technique that combines the decision tree (DT) and logistic regression algorithms (LR) [24]. Rather than only basic classification, logistic regression functions evaluate probability for each class in the LMT structure. The basic LMT induction algorithm uses cross-validation to find a number of LogitBoost iterations that does not overfit the training data.

3.2.4. REPTREE

Reduced error pruning tree (REPTREE) is a data mining technique that downsizing decision trees by deleting parts of the tree that have less importance to classify samples [25]. Pruning has two goals: it reduces the final classifier's complexity. It can also improve prediction accuracy by reducing overfitting and removing portions of a classifier which may be reliant on noisy or misleading data.

3.2.5. Classification via regression

Classification via regression is a classification technique which converts various problems to regression functions. On multiple sub-trees (leaves) [26], this technique implies the idea of the decision tree algorithm and linear regression. It can combine the principles of the decision tree algorithm and linear regression on several sub-trees (leaves).

3.2.6. Conjunctive rule

Conjunctive rule can not deal with numeric class labels only but also with nominal class labels, a rule is made up of "AND"ed predecessors and the result here is class label for classification/regression. From the affordmintoned conjunctive rule can be utilized with classification and regression based on the entropies weighted average to classification or mean-squared errors weighted average for regression [27]. Single conjunctive rule learner is one of the machine learning algorithms and is normally known as inductive Learning.

3.2.7. Vote

Its estimator technique which trains many base models then combine decision for the voted classifiers [28]. The main advantage of voting is to reduce false positives and improve detection accuracy. Vote has two main types hard and soft vote.

4. RESULTS AND DISCUSSION

Wrapper feature selection method that utilizes j48 tree to select optimal features was applied to improve the accuracy and lessen the testing time. Although wrapper method takes much time, it's very effective in terms of finding optimal features which results in 13 optimum features as shown in Table 2. The classifiers (J48, REPTREE, LMT, and ConjunctiveRule) were trained with those features on the KDDtrain+ dataset. The voting algorithm which uses several classifiers to execute the decision process [20] using the combination rule for its decision is developed. KDDtrain+ dataset is partitioned into many sub-sets through majority voting, and several classifiers are employed to train them and complete the learning process. Based on the number of votes collected in favour of a given class gathered from several classifiers, the final outcome of giving a label to the record is determined. After model building, it is evaluated using the same 13 selected features on the KDDTest+ dataset. By performing many combinations of classifiers with/without voting in Table 3, we found that the optimal performance can be achieved using majority voting utilizing (J48, REPTREE, LMT, ConjunctiveRule) algorithms that results in an accuracy of 86.502% as shown Table 3, testing time of 97.5 μsec for each record, precision of 96.41%, false positive rate of 3.90%, F1 Score of 86.99%, sensitivity of 86.5%, false negative rate of 20.76%, specificity of 96.10, Roc Area of 87.67. Figure 3 presents performance comparison results among the proposed models and other IDSs; Figure 3(a) presents testing accuracy, Figure 3(b) demonstrates sensitivity, Figure 3(c) provides specificity results, and Figure 3(d) presents False positive rate. Also Figure 4 shows the confusion matrix. All experiments are performed using PC with Intel(R) Core (TM) i7-1065G7 CPU @ 1.50 GHz and 16 GB RAM.

Table 2. Selected features

#	Feature name	Type	Value type
1	Duration	Continuous	Integral
2	Service	Categorical	Strings
3	Src Bytes	Continuous	Integral
4	Dst Bytes	Continuous	Integral
5	Logged In	Binary	Integral
6	Num File Creations	Continuous	Integral
7	Count	Discrete	Integral
8	Srv Count	Discrete	Integral
9	Serror Rate	Discrete	Floats
10	Srv Serror Rate	Discrete	Floats
11	Dst Host Count	Discrete	Integral
12	Dst Host Same Srv Rate	Discrete	Floats
13	Dst Host Diff Srv Rate	Discrete	Floats

Table 3. Performance comparison

Algorithm	Training accuracy (%)	Testing time (sec)	Testing accuracy (%)	Sensitivity	Specificity	Precision	F-Measure	FNR	FPR
Classification Via Regression	99.87	0.17	83.463	77.20	91.74	92.51	84.16	22.80	8.26
J48	99.94	0.07	85.309	77.17	96.07	96.29	85.67	22.83	3.93
LMT	99.95	0.54	85.633	77.67	96.16	96.39	86.02	22.33	3.84
Random Forest	99.99	2.68	80.500	71.97	91.77	92.04	80.78	28.03	8.23
REPTree	99.88	0.08	84.683	79.49	91.55	92.55	85.53	20.51	8.45
Proposed Vote1	99.94	0.21	86.498	79.24	96.09	96.40	86.98	20.76	3.91
Proposed Vote2	99.94	0.22	86.502	79.24	96.10	96.41	86.99	20.76	3.90
Proposed Vote3	99.94	0.45	86.183	78.61	96.19	96.46	86.63	21.39	3.81

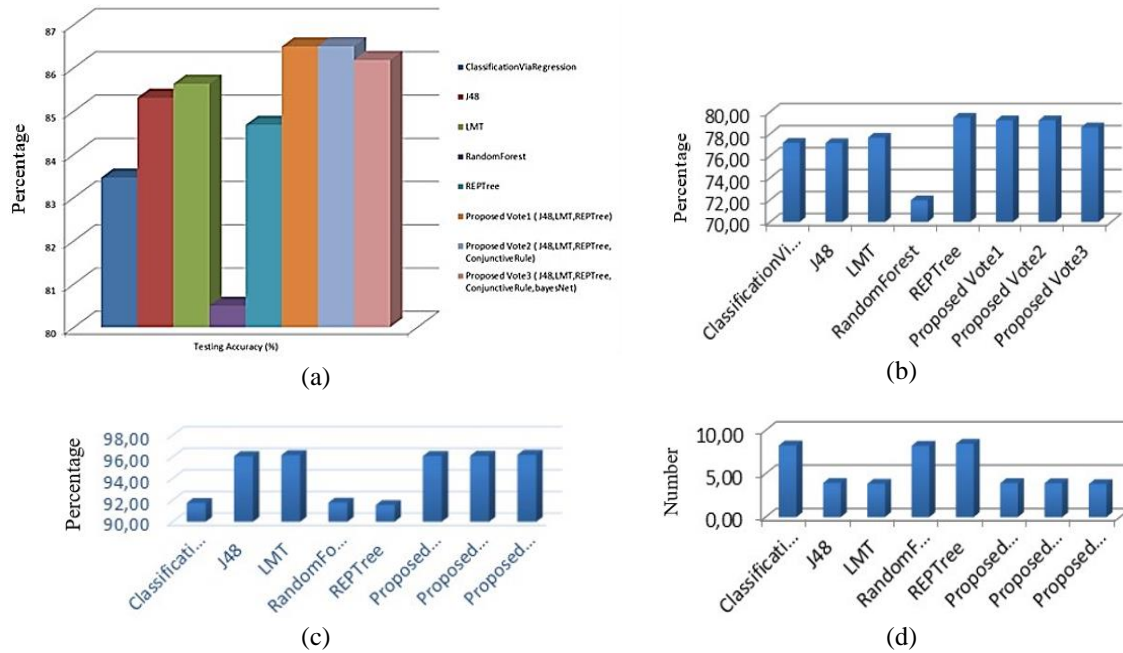


Figure 3. Performance comparison results; (a) testing accuracy, (b) sensitivity, (c) specificity, and (d) false positive rate



Figure 4. Confusion matrix

5. CONCLUSION

The proposed model is based on adaptive voting, the main idea is to employ majority vote learning to combine the benefits of multiple machine learning techniques, after using wrapper feature selection technique for feature selection that results in 13 optimum features proven to minimize training time, enhance detection accuracy,




and improve computational efficiency. The results demonstrate that the proposed model effectively enhances the detection accuracy compared to other research articles achieving an accuracy of 86.502% and testing time of 97.5 μ sec per processed record, which reflects the superiority of the performance of the proposed model. Moreover, the impact of use the majority voting shows that it's worthy to be used in research field of cybersecurity.

REFERENCES




- [1] A. F. Alshudukhi, S. A. Jabbar, and B. Alshaihdeeb, "A feature selection method based on auto-encoder for internet of things intrusion detection," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 3, pp. 3265–3275, 2022, doi: 10.11591/ijece.v12i3.pp3265-3275.
- [2] C. D. Xuan, H. Thanh, and N. T. Lam, "Optimization of network traffic anomaly detection using machine learning," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 3, pp. 2360–2370, 2021, doi: 10.11591/ijece.v11i3.pp2360-2370.
- [3] E. Hodo, X. Bellekens, A. Hamilton, C. Tachtatzis, and R. Atkinson, "Shallow and deep networks intrusion detection system: a taxonomy and survey," *arXiv preprint arXiv:1701.02145*, Jan. 2017.
- [4] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2018, doi: 10.1109/TETCI.2017.2772792.
- [5] T. Ma, F. Wang, J. Cheng, Y. Yu, and X. Chen, "A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks," *Sensors*, vol. 16, p. 1701, Oct. 2016, doi: 10.3390/s16101701.
- [6] M. Alqatf, L. Yu, M. Alhabib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, p. 1, Sep. 2018, doi: 10.1109/ACCESS.2018.2869577.
- [7] M. Latah and L. Toker, "An efficient flow-based multi-level hybrid intrusion detection system for software-defined networks," *CCF Transactions on Networking*, vol. 3, pp. 1–11, Oct. 2020, doi: 10.1007/s42045-020-00040-z.
- [8] Y. Zhou, M. Han, L. Liu, J. He, and Y. Wang, "Deep learning approach for cyberattack detection," *In IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, 2018, pp. 262–267. IEEE, doi: 10.1109/INFOCOMW.2018.8407032.
- [9] X. Gao, C. Shan, C. Hu, Z. Niu, and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, p. 1, Jun. 2019, doi: 10.1109/ACCESS.2019.2923640.
- [10] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep learning approach for network intrusion detection in software defined networking," *International Conference on Wireless Networks and Mobile Communications (WINCOM)*, 2016, pp. 258–263, doi: 10.1109/WINCOM.2016.7777224.
- [11] K. Wu, Z. Chen, and W. Li, "A novel intrusion detection model for a massive network using convolutional neural networks," *IEEE Access*, vol. 6, pp. 50850–50859, 2018, doi: 10.1109/ACCESS.2018.2868993.
- [12] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.
- [13] X. Gao, C. Shan, C. Hu, and Z. Liu, "An adaptive ensemble machine learning model for intrusion detection," *IEEE Access*, vol. 7, pp. 82512–82521, 2019, doi: 10.1109/ACCESS.2019.2923640.
- [14] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE Access*, vol. 7, pp. 41525–41550, 2019, doi: 10.1109/ACCESS.2019.2895334.
- [15] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network," *Sensors*, vol. 19, no. 11, 2019, doi: 10.3390/s19112528.
- [16] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019, doi: 10.1109/ACCESS.2019.2893871.
- [17] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, 2020, doi: 10.1016/j.neucom.2019.11.016.
- [18] M. Haggag, M. M. Tantawy, and M. M. S. El-Soudani, "Implementing a deep learning model for intrusion detection on apache spark platform," *IEEE Access*, vol. 8, pp. 163660–163672, 2020, doi: 10.1109/ACCESS.2020.3019931.
- [19] L. Liu, P. Wang, J. Lin, and L. Liu, "Intrusion detection of imbalanced network traffic based on machine learning and deep learning," *IEEE Access*, vol. 9, pp. 7550–7563, 2021, doi: 10.1109/ACCESS.2020.3048198.
- [20] Y. Zhou, G. Cheng, S. Jiang, and M. Dai, "Building an efficient intrusion detection system based on feature selection and ensemble classifier," *Computer Networks*, vol. 174, Jun. 2020, doi: 10.1016/j.comnet.2020.107247.
- [21] M. Tavallae, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symposium on Computational Intelligence for Security and Defense Applications*, pp. 1–6, 2009, doi: 10.1109/CISDA.2009.5356528.
- [22] F. Amiri, M. R. Yousefi, C. Lucas, A. Shakery, and N. Yazdani, "Mutual information-based feature selection for intrusion detection systems," *Journal Network and Computer Applications*, vol. 34, pp. 1184–1199, Jul. 2011, doi: 10.1016/j.jnca.2011.01.002.
- [23] S. Rajagopal, P. P. Kundapur, and K. S. Hareesha, "A predictive model for network intrusion detection using stacking approach," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 2734–2741, 2020, doi: 10.11591/ijece.v10i3.pp2734-2741.
- [24] N. Landwehr, M. Hall, and E. Frank, "Logistic model trees," *Machine Learning*, vol. 59, pp. 161–205, Feb. 2005, doi: 10.1007/s10994-005-0466-3.
- [25] A. Galathiya, A. Ganatra, and C. Bhensdadia, "Improved decision tree induction algorithm with feature selection, cross validation, model complexity and reduced error pruning," *International Journal of Computer Science and Information Technologies*, vol. 3, no. 2, pp. 3427–3431, May 2012.
- [26] I. Nurma, M. I. Fanany, and A. Arymurthy, "Comparing classification via regression and random committee for automatic sleep stage classification in autism patients," *Journal of Physics: Conference Series*, vol. 1230, p. 12010, Jul. 2019, doi: 10.1088/1742-6596/1230/1/012010.
- [27] R. Rabi, M. Joannis, T. Zhu, and J. Minda, "Cognitive changes in conjunctive rule-based category learning: An ERP approach," *Cognitive, Affective, and Behavioral Neuroscience*, vol. 18, Jun. 2018, doi: 10.3758/s13415-018-0620-6.
- [28] A. Bamhdi, I. Abrar, and F. Masoodi, "An ensemble based approach for effective intrusion detection using majority voting," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 19, pp. 664–671, Apr. 2021, doi: 10.12928/TELKOMNIKA.v19i2.18325.

BIOGRAPHIES OF AUTHORS






Mina Eshak Magdy    is M.Sc. student at Electronics and Communications Department, Faculty of Engineering, Zagazig University, Zagazig, Egypt. He has received the bachelor of science (BSc) in 2008. He can be contacted at email: m.tawfeek22@eng.zu.edu.eg.






Prof. Dr. Ahmed M. Matter    is Associate Professor at Department of computer engineering and artificial intelligence, military technical college, Cairo, Egypt. He has received the M.Sc degree and Ph.D. degree in the field of networks security. He can be contacted at email: a.mattar@ieee.org.






Dr. Saleh Hussin    received the B.S. in electronics and communication engineering from Zagazig University, Zagazig, Egypt, in 2002, and received the M.Sc. in information engineering from Ilmenau University of Technology, Ilmenau, Germany, 2010. He received the Ph.D. degree in electrical engineering from Paderborn University, Paderborn, Germany, in 2015. Since 2015, he is an assistant professor with electronics and communication engineering department at Zagazig University, Zagazig, Egypt. His current research interests are in wireless and optical communication system, signal processing, cognitive radio networks, long term evolution advanced (LTE-A) networks and 5G mobile communication. He can be contacted at email: saleh.hussin@campus.tu-berlin.de.



Dr. Doaa Hassan    is Associate is an associate professor at Computers and Systems Department, National Telecommunication Institute, Cairo, Egypt, and a research scholar at Indiana University–Purdue University Indianapolis (IUPUI) in U.S. She earned her PhD in Computer and Control Engineering from Faculty of Engineering at Zagazig University in Egypt in 2012, in a Data Collection program with Eindhoven University of Technology (TU/e) in Netherlands. Her current research interests focus on the new directions for application of data mining and machine learning techniques, particularly in cyber security, social networks, and computational biology. She can be contacted at email: hsdoaa@gmail.com.



Dr. Shaimaa Ahmed Elsaid    is an Associate Prof. at Electronics and Communications Dep., Faculty of Engineering, Zagazig University, Egypt. She has received the M.Sc degree (2006) in Networks Security and Ph.D. degree (2011) in Multimedia Security from Faculty of Engineering, Zagazig University (Egypt). Her current research interests include cyber security, internet of things (IoT), artificial intelligence, and digital image processing. She is the author of 2 books and many research papers published at international journals, and conference proceedings. Also, she has supervised many graduation projects, M.Sc. and Ph.D. theses. She can be contacted at email: saelsaid29@gmail.com.