Improving firewall performance using hybrid of optimization algorithms and decision trees classifier

Mosleh M. Abualhaj[1], Ahmad Adel Abu-Shareha[2], Sumaya Nabil Al-Khatib[1], Adeeb M. Alsaaidah[1], Mohammed Anbar[3]

[1]Department of Networks and Cybersecurity, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
[2]Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan
[3]Cybersecurity Research Center, Universiti Sains Malaysia, Penang, Malaysia

Article Info

Article history:

Received Sep 24, 2024
Revised Mar 16, 2025
Accepted Jun 8, 2025

Keywords:

Decision trees
Feature selection
Firewall
Harris hawks algorithm
Whale optimization algorithm

ABSTRACT

One of the primary concerns of governments, corporations, and even individual users is their level of online protection. This is because a large number of attacks target their primary assets. A firewall is a critical tool that almost every organization uses to protect its assets. However, firewalls become less reliable when they deal with large amounts of data. One method for reducing the amount of data and enhancing firewall performance is feature selection. The main aim of this study is to enhance the firewall's performance by proposing a new feature selection method. The proposed feature selection method combines the strengths of Harris Hawks optimization (HHO) and whale optimization algorithm (WOA). Experiments were performed utilizing the NSL-KDD dataset to measure the effectiveness of the proposed method. The experiments employed the decision trees (DTs) as a machine classifier. The experimental results show that the achieved accuracy is 98.46% when using HHO/WOA for feature selection and DT for classification, outperforming the HHO and WOA when used separately for feature selection. The study's findings offer insightful information for researchers and practitioners looking to improve firewall effectiveness and efficiency in defending internet connections against changing threats.

Corresponding Author:

Mosleh M. Abualhaj
Department of Networks and Cybersecurity, Faculty of Information Technology
Al-Ahliyya Amman University
Amman 19111, Jordan
Email: m.abualhaj@ammanu.edu.jo

1. INTRODUCTION

Cyberattacks are deliberate attempts to hack or take advantage of computer systems, networks, or other technology. The number of cyberattacks is a problem that is continually changing and expanding as more companies, organizations, and people rely on digital technologies to store and send sensitive information. Cyberattacks spread from one network or system to another [1]–[3]. Several reports indicate that, during the past few years, the number of cyberattacks has been continuously rising. For instance, the number of phishing websites increased by 350% in 2020 [4], and the number of ransomware attacks increased by 400% [5].

A firewall is a tool widely used by organizations to protect their assets. Firewalls analyze network data in real-time, contrasting it with known patterns of malicious activity and applying algorithms to find potential threats. Figure 1 clarifies the role of firewalls. It is crucial to remember that they are not foolproof and can be defeated by cunning attackers [6]–[8]. Therefore, building systems with advanced algorithms is crucial to providing comprehensive protection against cyberattacks.

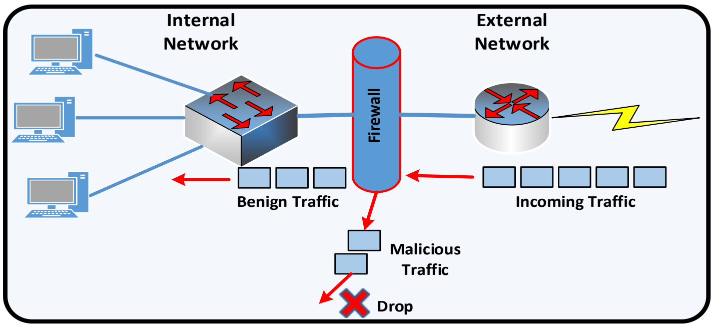

Figure 1. Firewall function

Modern firewalls use machine learning (ML) techniques to stop the new types of cyberattacks. By incorporating ML into firewalls, security issues can be discovered and avoided with incredible speed and accuracy. However, inaccurate data classification is a common problem that firewall-based ML frequently faces. Inaccurate data classification happens when a firewall incorrectly labels a regular network activity as malicious, wasting resources and causing unwanted alarms [9]–[11].

Feature selection is a widely utilized technique in firewall-based ML to reduce the inaccuracy of data classification. Selecting the features or variables most likely to distinguish between malicious and legitimate data is essential. The ML algorithms can identify network data more accurately by emphasizing the most valuable features [12], [13]. Feature selection can be implemented using filter-based and wrapper-based techniques. The filter-based techniques select features feature-by-feature, which enforces independencies between features. Wrapper-based techniques select features collaboratively, yet they require vast amounts of time and resources, as all possible feature combinations should be tested to produce the output set [14]–[16]. Accordingly, metaheuristic algorithms ease the computational requirements of wrapper-based feature selection. This paper will use the Harris Hawks optimization (HHO) and whale optimization algorithm (WOA) metaheuristic algorithms to select features for firewall-based ML.

Numerous works have been proposed to mitigate emerging cyberattacks. The authors in [17] suggested the double-layered hybrid approach (DLHA) to handle the issue of the large difference in the patterns of attacks when using network intrusion detection system (NIDS). The first layer of DLHA uses a naive Bayes (NB) classifier to detect denial of service (DoS) and probe attacks. The second layer of DLHA uses a support vector machine (SVM) classifier to detect remote to local (R2L) and user to root (U2R) attacks. The DLHA approach combines the outputs of both layers (NB and SVM layers) to categorize the network traffic as normal or anomalous, which enhances accuracy and lessens the false-positive rate. The suggested approach achieves an accuracy of 88.97% and a false-positive rate of 0.12% on the widely used NSL-KDD dataset.

According to Mughaid *et al.* [18], the detection model using ML techniques has been proposed by splitting the dataset for the detection model training and results validation. Also, this work aims to capture inherent characteristics from email text along with other features. These features are classified as phishing or non-phishing involving three different datasets. The evaluation had been conducted based on three supervised datasets, then made a comparison between these classifiers. The main finding of this work is the high level of accuracy when using phishing email detection. The noticeable results collected from the comparison between algorithms are based on the multi-feature of (50), which in turn obtains the highest accuracy. However, while using fewer features than 20, the accuracy registered an acceptable value, but this status is not effective enough to detect phishing emails. The overall finding of this work is that the best ML algorithm accuracies are 0.88%, 0.97%, and 100% consecutively for strengthening the decision tree (DT) on the applied datasets.

Liu *et al.* [19] propose a novel approach for detecting network intrusions in imbalanced network traffic data, where the number of normal network traffic instances significantly outweighs the number of intrusion instances. The suggested difficult set sampling technique (DSSTE) approach uses both ML and deep learning to handle this issue. The DSSTE technique lessens the imbalance of the original training set and provides targeted data augmentation for the underrepresented class that needs to learn. Therefore, the DSSTE technique enables the classifier to perform better during classification and better learn the distinctions during the training stage. The test findings show that the suggested DSSTE technique achieves an accuracy of 82.84%, precision 84.64%, and recall 82.78%, in multiclass classification.

2. METHOD

2.1. NSL-KDD dataset

NSL-KDD is considered a sufficient dataset that helps security researchers in investigating numerous firewalls. It is possible to successfully conduct the experiments and analyze the outcomes using the NSL-KDD dataset since it has a sufficient number of records [20]. The NSL-KDD dataset contains 148,517 samples and 41 features including the label column. There are 38 types of attacks in the NSL-KDD dataset groped into four main types:

- DoS attack: The DoS attack aims to make a network or system unavailable by overwhelming it with traffic or requests.
- Probe attack: The probe attack involves the attacker attempting to gather information about the target network or system.
- Root U2R attack: the U2R attack involves an unauthorized user gaining elevated privileges on a target system.
- R2L attacks: The R2L attacks involves an attacker gaining access to a system through a remote connection, such as exploiting a vulnerability in a service or application.

Besides, the NSL-KDD dataset contains a "normal,” type which represents regular network traffic [20]. The number of records in the NSL-KDD dataset is broken down by attack type in Table 1.

Table 1. Number of records for each attack

Attack type	Number of records
DoS	53,387
Probe	14,077
U2R	119
R2L	3,880
Normal	77,055

2.2. Feature selection using Harris Hawks optimization and whale optimization algorithm

Selecting the most pertinent features or variables from a dataset to include in a model is known as feature selection and is a critical step in an ML model. Due to their capacity to scan the whole feature space and identify the ideal subset of features, optimization algorithms are frequently utilized in feature selection. As mentioned earlier, the HHO and WOA optimization algorithms will be used to select the attack features that the firewall can use to detect the attacks. The HHO and WOA have been widely tested in cybersecurity and proven robust and efficient. In addition, combining these two algorithms can potentially leverage their respective strengths, providing a more robust and effective optimization strategy to select the most relevant features to detect the attacks. Furthermore, WOA is renowned for its robust global exploration skills, enabling it to quickly navigate the search space and avoid being trapped in local optima. HHO demonstrates effective exploration by utilizing many stages of hunting behavior, including exploration, interception, and attack [21], [22]. The proposed feature selection in this work proposes combining the features selected by the HHO and WOA optimization algorithms into one subset of features. The HHO algorithm identified a subset of 13 features, while the WOA algorithm identified a subset of 16 features. The union of these two subsets creates a final subset of 25 features. Figure 2 shows the proposed feature selection steps. Table 2 shows the created subset of features by each method.

2.3. Decision tree classifier

In this work, the DT classifier categorizes network traffic as benign or attack traffic. Based on the features of the input data, DT classifier constructs a model of decisions and potential outcomes that resembles a tree. Each internal node of the tree represents a decision based on a specific feature, and each leaf node represents a class label or a decision outcome. The construction of a DT starts with the entire dataset, and at each step, the algorithm selects the feature that provides the most information about the class labels. The algorithm splits the dataset based on the selected feature and its possible values and creates a new node for each split. The process is repeated recursively until a stopping criterion is met, such as a maximum depth of the tree or a minimum number of instances per leaf. Figure 3 clarifies the DT technique. The function that will be used with DT in the proposed system to measure the quality of a split is "Gini impurity". The Gini impurity is defined as the probability of misclassifying a randomly chosen element in the set if it were randomly labeled according to the distribution of labels in the subset [23], [24]. As in (1) is used for calculating Gini impurity. Where J is the number of classes, and p(i) is the proportion of the samples that belong to class i.

$$\text{Gini Impurity} = 1 - (\sum(i = 1 \text{ to } J)p(i)^2) \quad (1)$$

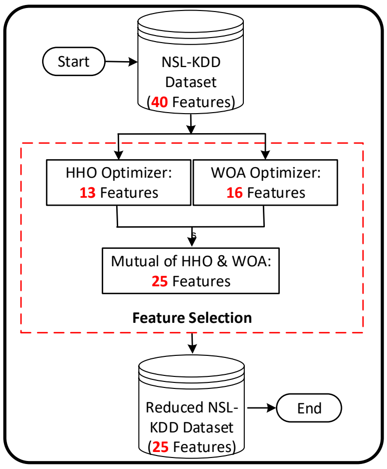
Start
NSL-KDD Dataset (40 Features)
HHO Optimizer: 13 Features
WOA Optimizer: 16 Features
Mutual of HHO & WOA: 25 Features
Feature Selection
Reduced NSL-KDD Dataset (25 Features)
End

Figure 2. Feature selection process

Table 2. Selected feature by different methods

Optimizer	Selected features (feature#)
WOA	Service, Flag, src_bytes, num_failed_logins, num_root, num_access_files, num_outbound_cmds, is_host_login, is_guest_login, srv_count, serror_rate, srv_serror_rate, same_srv_rate
HHO	protocol_type, Flag, src_bytes, dst_bytes, urgent, hot, num_access_files, Count, diff_srv_rate
HHO & WOA	protocol_type, service, Fla, src_bytes, dst_bytes, urgent, hot, num_failed_logins, num_root, num_access_files, num_outbound_cmds, is_host_login, is_guest_login, Count, srv_count, serror_rate, srv_serror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, dst_host_count, dst_host_srv_count, dst_host_diff_srv_rate, dst_host_same_src_port_rate, dst_host_rerror_rate

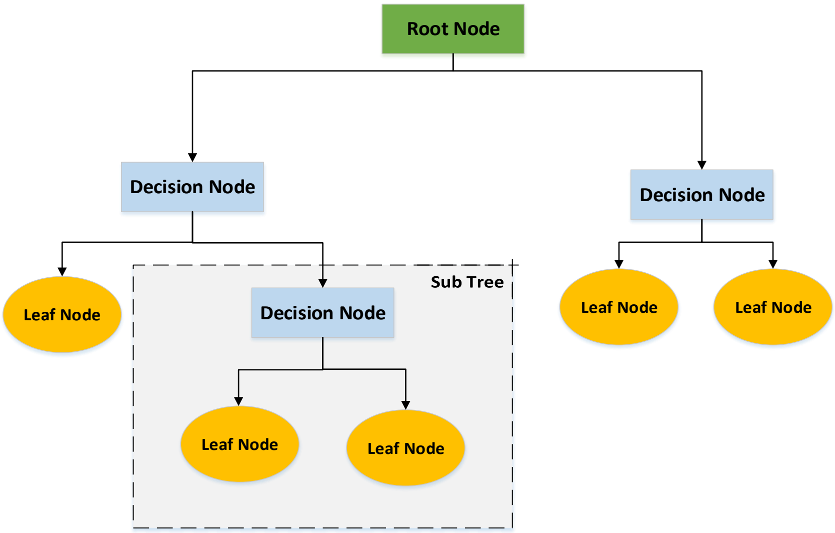

Figure 3. DT technique scheme

2.4. Attack detection

This section discusses the steps involved in firewall-based ML detection. Figure 4 shows the attack detection steps. First, all the non-numeric data in the NSL-KDD dataset has been transformed into numbers, using the label-encoding method, to ensure that implementing the DT classifier will be error-free [20], [25]. Next, the entire NSL-KDD dataset was normalized using the min-max scaler method to ensure all data points fall within the same range. Normalization prevents data with larger values from dominating the data with small values during the DT classifier implementation [20], [25]. The final step in preparing the data is to select the features with the highest impact on detecting attacks. Therefore, only the critical features that provide useful information are used for attack detection, improving the DT classifier's accuracy. The proposed features selection method is discussed in section 2.2. After preparing the data, the classification process starts using the DT classifier. The DT classifier has been trained and tested to measure its performance in attack detection.

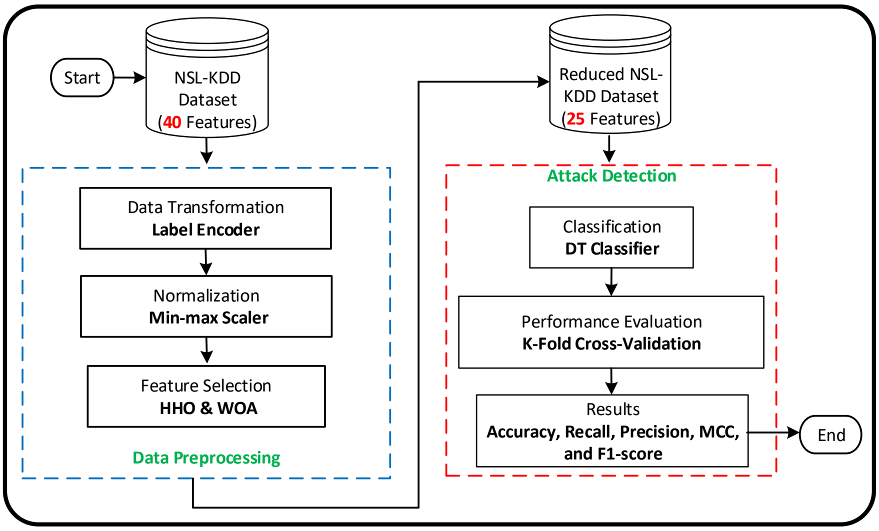

Figure 4. Attack detection model

The DT classifier was implemented using the K-fold cross-validation method. The K-fold method divides the available data into K equal-sized folds or subsets, uses K-1 folds for model training, and uses the last fold for model testing. Each of the K folds is utilized as validation data exactly once during the K times this process is conducted. In order to provide an overall estimate of the model's performance, the results are averaged over the K iterations. K-fold cross-validation has the benefit of allowing for a more precise estimation of the model's performance and can aid in avoiding overfitting [20], [25]. The performance of the DT classifiers has been evaluated using accuracy, recall, precision, and F1-score.

3. RESULTS AND DISCUSSION

The results of the proposed firewall model are computed based on the elements of the confusion matrix: true positive (TPo), true negative (TNe), false positive (FPo), and false negative (FNe). Several metrics are calculated based on these elements, including accuracy, precision, recall, and F1-score. Accuracy evaluates overall correctness but may be misleading with imbalanced data. The accuracy of the proposed firewall model is calculated using (2). Precision minimizes false positives, making it ideal for applications where false alarms are costly. The precision of the proposed firewall model is calculated using (3). Recall reduces false negatives, ensuring important instances are not missed. The recall of the proposed firewall model is calculated using (4). F1-score balances precision and recall, making it suitable for imbalanced datasets. The F1-score of the proposed firewall model is calculated using (5) [20], [25]. These four metrics have been calculated for DT with HHO (DT-HHO) method, DT with WOA (DT-WOA) method, and DT with HHO/WOA (DT-HHO/WOA) method that is used with the proposed firewall model.

$$Accuracy = \frac{(TPo+TNe)}{(TPo+TNe+FPo+FNe)} \quad (2)$$

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

$$Precision = \frac{TPo}{(TPo+FPo)} \tag{4}$$

$$F1 - score = \frac{Precision\ X\ Recall}{Precision + Recall} \tag{5}$$

Figure 5 presents the accuracy achieved by the proposed firewall model. The DT-HHO method has an accuracy of 97.59%, the DT-WOA method has an accuracy of 97.5%, and the DT-HHO/WOA method has an accuracy of 98.46%. The accuracy achieved by the DT-HHO/WOA method outperformed the accuracy achieved by the DT-HHO method and by the DT-WOA method by 0.87% and 0.96%, respectively. Therefore, the proposed DT-HHO/WOA method improves the firewall's detection attack accuracy.

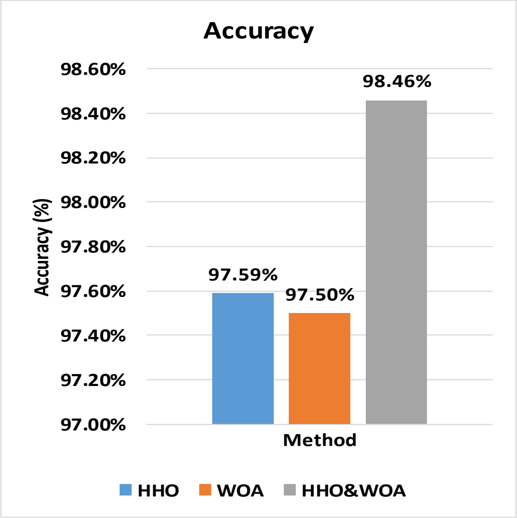

Figure 5. Accuracy of the proposed firewall model

Figure 6 presents the recall achieved by the proposed firewall model. The DT-HHO method has a recall of 97.59%, the DT-WOA method has a recall of 97.5%, and the DT-HHO/WOA method has a recall of 98.46%. The recall achieved by the DT-HHO/WOA method outperformed the recall achieved by the DT-HHO method and by the DT-WOA method by 0.87% and 0.96%, respectively. Therefore, the proposed DT-HHO/WOA method improves the firewall's detection attack recall.

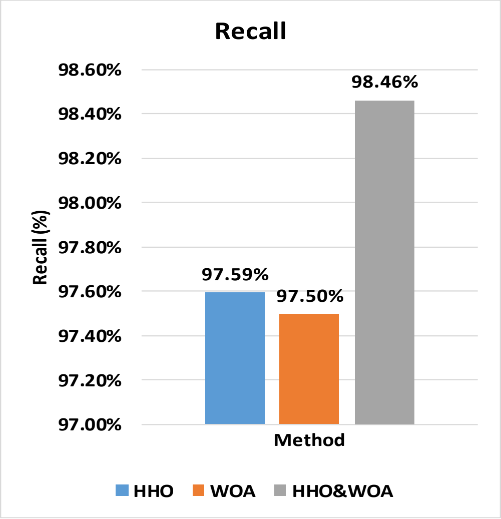

Figure 6. Recall of the proposed firewall model

Figure 7 presents the precision achieved by the proposed firewall model. The DT-HHO method has a precision of 97.59%, the DT-WOA method has a precision of 97.5%, and the DT-HHO/WOA method has a precision of 98.46%. The precision achieved by the DT-HHO/WOA method outperformed the precision achieved by the DT-HHO method and by the DT-WOA method by 0.87% and 0.96%, respectively. Therefore, the proposed DT-HHO/WOA method improves the firewall's detection attack precision.

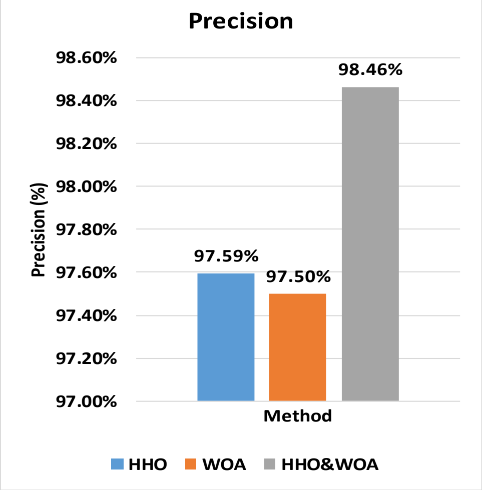

Figure 7. Precision of the proposed firewall model

Figure 8 presents the F1-score achieved by the proposed firewall model. The DT-HHO method has an F1-score of 97.59%, the DT-WOA method has an F1-score of 97.5%, and the DT-HHO/WOA method has an F1-score of 98.46%. The F1-score achieved by the DT-HHO/WOA method outperformed the F1-score achieved by the DT-HHO method and by the DT-WOA method by 0.87% and 0.96%, respectively. Therefore, the proposed DT-HHO/WOA method improves the firewall's detection attack an F1-score.

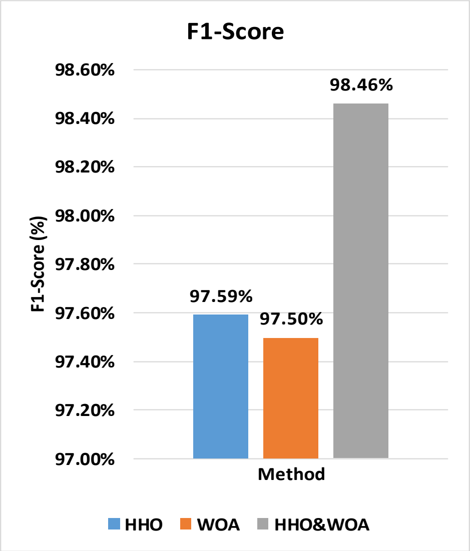

Figure 8. F1-score of the proposed firewall model

In summary, the superior performance of the proposed model stems from the combined strengths of HHO and WOA in feature selection. HHO enhances exploration, while WOA refines local exploitation, resulting in an optimized feature subset. This improves the DT classifier’s accuracy, reducing irrelevant features and enhancing attack detection. The achieved 98.46% accuracy confirms the effectiveness of this approach over using HHO or WOA separately. Additionally, the method reduces computational complexity, enabling faster processing while maintaining high detection accuracy. These results demonstrate the practical benefits of the proposed approach in improving firewall efficiency against evolving cyber threats.

4. CONCLUSION

A firewall is one of the key components that protects the internal network from internet attacks. Traditional firewalls do not cope with recent attacks that use sophisticated techniques. In this paper, we have proposed a firewall that uses ML methods to stop these sophisticated attack techniques. The proposed firewall employs the HHO and WOA algorithms for feature selection. The main purpose of HHO and WOA is to select only the key features of the traffic that can identify the attacks. The HHO has selected 13 features, while the WOA has selected 16 features from 40 features. The common features between the two algorithms are 25. Combining the features from the two algorithms has enhanced the firewall performance. For example, the accuracy achieved when using HHO is 97.59%, and WOA is 97.5%, while when using the common features of the two algorithms, the accuracy reached 98.46%. The archived result proved that the proposed ML-based firewall is a promising solution to mitigate the attacks on the internal network.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Mosleh M. Abualhaj	✓	✓			✓				✓	✓		✓		
Ahmad Adel Abu-Shareha		✓		✓		✓				✓				
Sumaya Nabil Al-Khatib		✓	✓			✓	✓	✓		✓	✓			
Adeeb M. Alsaaidah	✓			✓	✓			✓	✓		✓			
Mohammed Anbar	✓				✓	✓			✓		✓			

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are openly available in [Canadian Institute for Cybersecurity] at https://www.unb.ca/cic/datasets/ids.html [doi: 10.1016/j.cose.2011.12.012], reference [20].

REFERENCES

[1] M. Cui, J. Wang, and B. Chen, "Flexible machine learning-based cyberattack detection using spatiotemporal patterns for distribution systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 2, pp. 1805–1808, 2020, doi: 10.1109/TSG.2020.2965797.

[2] M. M. Abualhaj, A. A. Abu-Shareha, Q. Y. Shambour, A. Alsaaidah, S. N. Al-Khatib, and M. Anbar, "Customized K-nearest neighbors' algorithm for malware detection," *International Journal of Data and Network Science*, vol. 8, no. 1, pp. 431–438, 2024, doi: 10.5267/j.ijdns.2023.9.012.

[3] A. O. Aluko, R. Musumpuka, and D. G. Dorrell, "Cyberattack-resilient secondary frequency control scheme for stand-alone microgrids," *IEEE Transactions on Industrial Electronics*, vol. 70, no. 2, pp. 1622–1634, Feb. 2023, doi: 10.1109/TIE.2022.3159965.

[4] D. -J. Liu, G. -G. Geng, X. -B. Jin, and W. Wang, "An efficient multistage phishing website detection model based on the CASE feature framework: Aiming at the real web environment," *Computers & Security*. vol. 110, pp. 1-11, Nov. 2021, doi: 10.1016/j.cose.2021.102421

[5] D. H. Kass, “FBI: covid-19 cyberattacks spike 400% in pandemic,” *MSSP Alert*. Accessed: Sep. 14, 2024. [Online]. Available: https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/

[6] H. Gu *et al.*, “DIAVA: a traffic-based framework for detection of SQL injection attacks and vulnerability analysis of leaked data,” *IEEE Transactions on Reliability*, vol. 69, no. 1, pp. 188–202, Mar. 2020, doi: 10.1109/TR.2019.2925415.

[7] H. Jmal, F. Ben Hmida, N. Basta, M. Ikram, M. A. Kaafar, and A. Walker, “SPGNN-API: a transferable graph neural network for attack paths identification and autonomous mitigation,” *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1601–1613, 2024, doi: 10.1109/TIFS.2023.3338965.

[8] F. Chen, B. Bruhadeshwar, and A. X. Liu, “Cross-domain privacy-preserving cooperative firewall optimization,” *IEEE/ACM Transactions on Networking*, vol. 21, no. 3, pp. 857–868, Jun. 2013, doi: 10.1109/TNET.2012.2217985.

[9] P. Zhou, H. Zhang, and W. Liang, “Research on hybrid intrusion detection based on improved harris hawk optimization algorithm,” *Connection Science*, vol. 35, no. 1, Dec. 2023, doi: 10.1080/09540091.2023.2195595.

[10] G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh, and A. SaiTeja, “Intrusion detection system framework using machine learning,” in *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, Sep. 2021, pp. 1224–1230, doi: 10.1109/ICIRCA51532.2021.9544717.

[11] J. A. Abraham and V. R. Bindu, “Intrusion detection and prevention in networks using machine learning and deep learning approaches: a review,” in *2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, Oct. 2021, pp. 1–4, doi: 10.1109/ICAECA52838.2021.9675595.

[12] A. Gupta *et al.*, “On the utility of power spectral techniques with feature selection techniques for effective mental task classification in noninvasive BCI,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 5, pp. 3080–3092, May 2021, doi: 10.1109/TSMC.2019.2917599.

[13] D. Palacios, I. De-la-Bandera, A. Gomez-Andrades, L. Flores, and R. Barco, “Automatic feature selection technique for next generation self-organizing networks,” *IEEE Communications Letters*, vol. 22, no. 6, pp. 1272–1275, Jun. 2018, doi: 10.1109/LCOMM.2018.2825392.

[14] M. Banerjee and N. R. Pal, “Unsupervised feature selection with controlled redundancy (UFeSCoR),” *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 12, pp. 3390–3403, Dec. 2015, doi: 10.1109/TKDE.2015.2455509.

[15] M. M. Sakr, M. A. Tawfeeq, and A. B. El-Sisi, “Filter versus wrapper feature selection for network intrusion detection system,” in *2019 Ninth International Conference on Intelligent Computing and Information Systems (ICICIS)*, Dec. 2019, pp. 209–214, doi: 10.1109/ICICIS46948.2019.9014797.

[16] S. M. Kasongo and Y. Sun, “Performance analysis of intrusion detection systems using a feature selection method on the UNSW-NB15 dataset,” *Journal of Big Data*, vol. 7, no. 1, Dec. 2020, doi: 10.1186/s40537-020-00379-6.

[17] T. Wisanwanichthan and M. Thammawichai, “A double-layered hybrid approach for network intrusion detection system using combined naive Bayes and SVM,” *IEEE Access*, vol. 9, pp. 138432–138450, 2021, doi: 10.1109/ACCESS.2021.3118573.

[18] A. Mughaid, S. AlZu’bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, “An intelligent cyber security phishing detection system using deep learning techniques,” *Cluster Computing*, vol. 25, no. 6, pp. 3819–3828, 2022, doi: 10.1007/s10586-022-03604-4.

[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] A. Shiravani, M. H. Sadreddini, and H. N. Nahook, “Network intrusion detection using data dimensions reduction techniques,” *Journal of Big Data*, vol. 10, no. 1, Mar. 2023, doi: 10.1186/s40537-023-00697-5.

[21] M. M. Abualhaj, S. N. Al-Khatib, A. Al-Allawee, A. Munther, and M. Anbar, “Enhancing network intrusion detection systems through dimensionality reduction,” *Recent Advances on Soft Computing and Data Mining*, pp. 244–253, 2024, doi: 10.1007/978-3-031-66965-1_24.

[22] M. M. Abualhaj, A. A. Abu-Shareha, A. Al-Allawee, A. Munther, and M. Anbar, “Performance evaluation of whale and harris hawks optimization algorithms with intrusion prevention systems,” *Recent Advances on Soft Computing and Data Mining*, pp. 254–265, 2024, doi: 10.1007/978-3-031-66965-1_25.

[23] M. M. Abualhaj, A. S. Al-Shamayleh, A. Munther, S. N. Alkhatib, M. O. Hiari, and M. Anbar, “Enhancing spyware detection by utilizing decision trees with hyperparameter optimization,” *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 5, pp. 3653–3662, 2024, doi: 10.11591/eei.v13i5.7939.

[24] X.-Y. Shih, Y. Chiu, and H.-E. Wu, “Design and implementation of decision-tree (DT) online training hardware using divider-free GI calculation and speeding-up double-root classifier,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 70, no. 2, pp. 759–771, Feb. 2023, doi: 10.1109/TCSI.2022.3222515.

[25] M. M. Abualhaj, A. A. Abu-Shareha, M. O. Hiari, Y. Alrabanah, M. Al-Zyoud, and M. A. Alsharaiah, “A paradigm for DoS attack disclosure using machine learning techniques,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 3, 2022, doi: 10.14569/IJACSA.2022.0130325.

BIOGRAPHIES OF AUTHORS

Mosleh M. Abualhaj is a senior lecturer at Al-Ahliyya Amman University. He received his first degree in Computer Science from Philadelphia University, Jordan, in 2004, master degree in Computer Information System from the Arab Academy for Banking and Financial Sciences, Jordan in 2007, and Ph.D. in Multimedia Networks Protocols from Universiti Sains Malaysia in 2011. His research area of interest includes VoIP, congestion control, and cybersecurity data mining and optimization. He can be contacted at email: m.abualhaj@ammanu.edu.jo.

Ahmad Adel Abu-Shareha received his first degree in Computer Science from Al Al-Bayt University, Jordan, 2004, master degree from Universiti Sains Malaysia (USM), Malaysia, in 2006, and Ph.D. degree from USM, Malaysia, in 2012. His research focuses on data mining, artificial intelligent, and multimedia security. He investigated many machine learning algorithms and employed artificial intelligence in variety of fields, such as network, medical information process, knowledge construction and extraction. He can be contacted at email: a.abushareha@ammanu.edu.jo.

Sumaya Nabil Al-Khatib is a senior lecturer in Al-Ahliyya Amman University. She received his first degree in Computer Science from Baghdad University, Iraq, in June 1994 and master degree in Computer Information System from the Arab Academy for Banking and Financial Sciences, Jordan in February. Her research area of interest includes VoIP, multimedia networking, and congestion control. She can be contacted at email: sumayakh@ammanu.edu.jo.

Adeeb M. Alsaaidah received the bachelor’s degree in Computer Engineering from the Faculty of Engineering, Al-Balqa Applied University, the master’s degree in Networking and Computer Security from NYIT University, and the Ph.D. degree in Computer Network from Universiti Sains Islam Malaysia, Malaysia. He is currently an Assistant Professor in Network and Cybersecurity department at Al-Ahliyya Amman University. His research interests include network performance, multimedia networks, network quality of service (QoS), the IoT, network modeling and simulation, network security, and cloud security. He can be contacted at email: a.alsaaidah@ammanu.edu.jo.

Mohammed Anbar received the B.Sc. degree in Software Engineering from Al-Azhar University, Palestine, in 2008, the M.Sc. degree in Information Technology from Universiti Utara Malaysia, in 2009, and the Ph.D. degree in Advanced Internet Security and Monitoring from Universiti Sains Malaysia, in 2013. He is currently a senior lecturer with the National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia. His current research interests include malware detection, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), network monitoring, the internet of things (IoT), software-defined networking (SDN) security, cloud computing security, and IPv6 security. He can be contacted at email: anbar@usm.my.