

Harris Hawks Feature Selection in Distributed Machine Learning for Secure IoT Environments

Neveen Hijazi¹, Moayad Aloqaily¹, Bassem Ouni², Fakhri Karray¹, Merouane Debbah²

¹Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE

²Technology Innovation Institute (TII), Abu Dhabi, UAE

E-mails: ¹{neveen.hijazi; moayad.aloqaily; fakhri.karray}@mbzuai.ac.ae

²{bassem.ouni; merouane.debbah}@tii.ae

Abstract—The development of the Internet of Things (IoT) has dramatically expanded our daily lives, playing a pivotal role in the enablement of smart cities, healthcare, and buildings. Emerging technologies, such as IoT, seek to improve the quality of service in cognitive cities. Although IoT applications are helpful in smart building applications, they present a real risk as the large number of interconnected devices in those buildings, using heterogeneous networks, increases the number of potential IoT attacks. IoT applications can collect and transfer sensitive data. Therefore, it is necessary to develop new methods to detect hacked IoT devices. This paper proposes a Feature Selection (FS) model based on Harris Hawks Optimization (HHO) and Random Weight Network (RWN) to detect IoT botnet attacks launched from compromised IoT devices. Distributed Machine Learning (DML) aims to train models locally on edge devices without sharing data to a central server. Therefore, we apply the proposed approach using centralized and distributed ML models. Both learning models are evaluated under two benchmark datasets for IoT botnet attacks and compared with other well-known classification techniques using different evaluation indicators. The experimental results show an improvement in terms of accuracy, precision, recall, and F-measure in most cases. The proposed method achieves an average F-measure up to 99.9%. The results show that the DML model achieves competitive performance against centralized ML while maintaining the data locally.

Index Terms—IoT, Harris Hawks Optimization, Cognitive Cities, Smart Buildings, Distributed Machine Learning.

I. INTRODUCTION

Internet of Things (IoT) is one of the most significant revolutions of the 21st century and can be simply described as a set of connected smart edge devices. These devices can be found in many applications we encounter across our daily lives including healthcare, smart cities, transportation systems, and smart grids [1]. IoT environments typically consist of collections of distributed heterogeneous devices with low computational memory, and they have the ability to expand with other interconnected networks, which results in many security concerns [2]. The enormous increase in IoT devices and their lack of security guarantees has motivated attackers to launch attacks by setting up large-scale IoT botnet attacks. A botnet is a network of devices connected to IoT devices that are infected by malware. In addition, compromised devices have a simple infection process, which makes every vulnerable device a bot candidate. Some of the most popular examples of IoT botnet attacks are Mirai, BASHLITE, and Phishing [3]. Consequently, this highlights the importance of increasing

security measures to identify the most critical cyberattacks in a smart IoT environment.

Intrusion Detection Systems (IDSs) are security systems that detect attacks and malicious activities in networks, such as botnet attacks. ML techniques can play an essential role in IDS structures to classify and predict attacks. Different ML techniques are used to detect anomalies and attacks in cybersecurity, such as K-Nearest Neighbor (KNN), Support Vector Machines (SVM), and Decision Trees (DT) [4], [5]. However, IoT devices continuously produce vast amounts of data that is challenging to deal with using traditional ML techniques and requires complex models to process such as deep learning technique [1]. Therefore, there is a need for more efficient searching and learning algorithms, which has led to the emergence of metaheuristic algorithms.

Metaheuristics algorithms are a well-regarded choice to solve high-dimensional problem through the utilization of the feature selection technique [6]. The objective of this technique is to generate a highly accurate general model while minimizing the number of selected features in order to reduce computational time. Therefore, various works have utilized metaheuristic algorithms in feature selection methods such as Genetic Algorithm (GA), Particle Swarm Optimization (PSO), and Harris Hawks Optimization (HHO) [5], [7].

Distributed ML is a valuable approach, it aims to train one or more ML models for a network of users, each having a local dataset. Thus, distributed ML reduces data transmissions within centralized ML and minimizes the risks of privacy leaks. In addition, it can reduce the risk of a single point of failure compared to centralized ML [8]. Distributed ML can be applied in various applications such as healthcare [9] and wireless network [2]. In this study, we propose a hybrid model based on the HHO and Random Weight Network (RWN) algorithms to detect botnet attacks launched from compromised IoT devices. The proposed approach performs wrapper FS based on two main stages: centralized and distributed ML. Wrapper FS consists of three repeated steps including search algorithm, learning algorithm, and an evaluation measure. In our work, we used HHO as a search algorithm to select the near-optimal feature subset of the input features and optimized the RWN structure simultaneously to increase the prediction power. Then, RWN is applied as a learning algorithm to fit the training dataset according to the selected solution. Finally,

evaluation measures are applied to assess the quality of the selected solution. The proposed approach is compared with other metaheuristics approaches [10].

The contributions of this work can be summarized as

- 1) We propose an intrusion detection system based on HHO with RWN.
- 2) We apply RWN as the base classifier in wrapper FS, unlike most of the literature that uses KNN.
- 3) We utilize the HHO algorithm to achieve two different objectives simultaneously, including, near-optimal subset of features and number of hidden neurons in RWN.
- 4) We leverage distributed ML to maintain data privacy and apply the proposed approach using a distributed ML scheme.

The rest of the paper is organized as follows. Section II presents the background and related works of Harris Hawks Optimization, Random Weight Network algorithms, and Decentralized machine learning. The methodology and proposed approach are described in detail in Section III. The conducted experiments and the obtained results are discussed in Section IV. Finally, we conclude our work and provide suggestions for future directions in Section V.

II. BACKGROUND AND RELATED WORK

A. Harris Hawks Optimization (HHO)

HHO is a meta-heuristic optimization algorithm developed by A. Heidari et al. [11]. The HHO algorithm was inspired by the behavior of Harris Hawks. Precisely, HHO uses a multi-agent system where each agent represents a solution and collaborates with other agents to search for the global optimal solution. The algorithm starts with a set of initial solutions, and then updates the solutions by exchanging information and searching in a new direction. The algorithm terminates when a stopping criterion is met, such as reaching a maximum number of iterations or finding a solution that meets a certain fitness threshold. HHO uses a combination of global and local search techniques to balance the exploration and exploitation of a search space in order to find the global optimum solution. In the exploration phase, candidate solutions are randomly generated and evaluated for potential optimization. The selection of the solution generation strategy is based on a probability of either considering the location of already discovered solutions or relying on randomly determined positions. The exploitation phase of the HHO algorithm is a key component that influences the optimization performance. In this phase, the algorithm uses the surprise pounce strategy to search for optimal solutions in the problem space. The algorithm follows four different chasing strategies: Soft Besiege, Hard Besiege, Soft Besiege with progressive rapid dives, and Hard Besiege with advanced fast dives. The choice of strategy is based on the energy of the prey, where the prey energy loses its energy while escaping the hawk. Thus, the hawks alternate between different exploitative behaviors based on the prey's energy during running.

HHO is applied in different and broad applications in the literature. For instance, O. Alzubi et al. [4] proposed an SVM

combined with HHO for Android malware detection. Their research relied on two targets, the first goal was to determine the best hyperparameters for the SVM, and the second was to determine the weights of the features to determine the most important ones, thus improving the detection process by using the HHO algorithm. Their approach was compared against existing techniques using four different datasets. The results showed superior performance over other metaheuristic algorithms and state-of-art classifiers. Another work also mentioned the importance of HHO [12]. In this study, S. Sockalingam et al. proposed three hybrid ML approaches with feature selection methods for IDS: SVM-PSO, SVM-HHO-PSO, and SVM-HHO. The performance of these methods was evaluated using the NSL-KDD dataset and compared with various classifiers. The experimental outcomes indicated that SVM-HHO-PSO achieved the best results compared to other methods.

B. Random Weight Networks (RWN)

RWN is a computational neural network model developed by Schmidt et al. [13] to handle the training process of a Single Hidden Layer Feedforward Neural Network (SLFN), where a node can be a subnet that consist of extra hidden node. RWN has overcome the problems of back-propagation, such as slow convergence and high probability of being trapped in a local minimum. In RWN, the input weights and the hidden biases are initialized randomly; then, the output weights are analytically computed using the Moore–Penrose generalized inverse method. Compared to other gradient descent methods used in SLFN, the RWN learning rate is speedy and has better generalization performance. Moreover, RWN does not need human intervention to set the parameters manually such as learning rate, number of epochs, etc. RWN has only one parameter that needs to be initialized, which is the number of hidden neurons.

RWN is a powerful learning algorithm, which is used in a wide range of applications. For example, H. Faris et al. [5] proposed a hybrid email spam detection system based on GA and RWN. The proposed approach performs a wrapper FS method using an RWN classifier. The GA is used to select the optimal features and determine the number of neurons in the hidden layer of the RWN. Their approach detected spam emails and achieved excellent results in terms of accuracy, recall, and precision. Another hybrid method proposed by E. Rawashdeh et al. in [14]. In this study, the authors depended on RWN and PSO. The aim of the work was to optimize the structure of the RWN and to find the best subset of features. PSO was used to find the best subset of features, as well as the number of hidden neurons in RWN. The proposed approach was evaluated on thirty datasets, compared with other state-of-the-art methods, and showed superior results in most datasets.

C. Distributed Machine Learning (DML)

In this approach of learning, a generic model is distributed by the server to all clients or devices. The devices then customize the model through local training and testing with

their own data, enabling predictions and insights from live data generated by the device. This approach keeps the data local, reducing security and privacy concerns, but the downside is that IoT devices are not well-suited for intensive computation [2].

Distributed ML has gained more attention in recent years. For instance, F. Zerka et al. [9] applied several ML algorithms using a distributed framework to preserve medical data privacy. Their approach was compared with the centralized ML approach using four small medical datasets. The results show that the distributed approach delivers similar performance to the centralized approach, while preserving privacy of the patient data. A. Tuladhar et al. [15] investigated a distributed ML model by ensemble using three classifiers: ANNs, SVM, and Random Forests (RF). Their approach was evaluated on four medical datasets. They found improvement in results when increasing the number of locally trained models in the ensemble. The authors suggested using the proposed approach on small datasets.

According to the No Free Lunch theorem (NFL) [16], there is no single optimization algorithm that outperforms the others in all optimization problems. Therefore, this field of research offers opportunities for improvement and the development of new techniques that can tackle a wider range of problems and applications. This will ultimately lead to more competitive and improved results when compared to current algorithms. Overall, it can be understood from the literature that applying evolutionary algorithms with RWN is gaining more attention from researchers. HHO is a recent optimization algorithm that has been applied in different applications and has achieved promising results compared to other metaheuristic techniques. Moreover, it provides good exploration and exploitation. Therefore, it would be wise to use these properties with a robust learning algorithm, such as RWN. In conclusion, the proposed approach differs from previous studies by proposing a wrapper FS based on HHO and RWN algorithms to solve the IoT botnet detection problem, and applying the proposed approach within distributed ML that addresses IoT security and privacy issues.

III. METHODOLOGY

The proposed work is conducted based on a two-stage: centralized and distributed ML models. We apply the FS method, model construction, evaluation, and assessment in each stage. The main contribution lies in FS and the phases of model construction, where a new model based on HHO and RWN is proposed. This section presents the details of the proposed approach, which is based on using HHO for FS while simultaneously optimizing the RWN structure.

A. Data Preprocessing

Two benchmark datasets were used for this work: N-BaIoT dataset [17] and Phishing legitimate dataset [18]. The N-BaIoT dataset is obtained from the University of California at Irvine (UCI) machine learning repository. This dataset represents a real IoT network consisting of nine devices: a baby monitor,

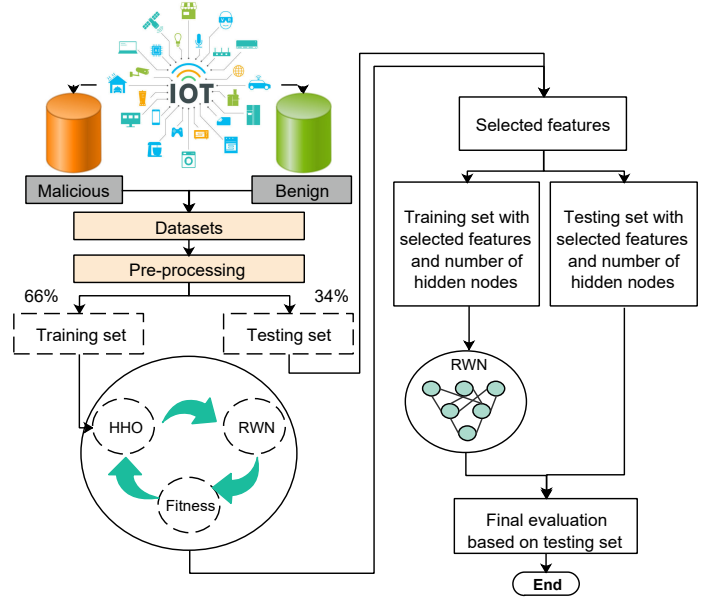


Fig. 1. An overview of the proposed approach.

two doorbells, four security cameras, a thermostat, and a webcam. The second dataset was collected from Kaggle datasets. The dataset comprises 48 features extracted from 10,000 web pages, with 5000 being phishing pages and the other 5000 being legitimate ones [18]. Using the preliminary dataset without any preprocessing may impact the overall performance of the obtained model. Because we deal with massive and real datasets, they may contain inconsistent and redundant data. In order to get the best possible results, we apply data integration and data normalization. In the integration step, we integrated the data for the N-BaIoT dataset according to each device type. For example, the four different types of security cameras are merged into one file. All the devices in the N-BaIoT dataset have 115 features and 7,062,606 instances. These devices typically connect to IoT networks through Wi-Fi. For each device, data were collected during normal operation and various attacks conducted by the BASHLITE and Mirai botnet. The total number of attacks carried out by BASHLITE and Mirai were 2,838,272 and 3,668,402 respectively. The integration step's benefit is reducing the number of generated models [17]. For the normalization step, we apply the Min-Max normalization method to both datasets to make all the input values within a consistent scale [0,1].

B. Wrapper Feature Selection based on HHO-RWN

In this work, we apply an FS method on the training dataset to eliminate irrelevant features, reduce data dimensionality, and increase prediction performance. Two well-known methods in feature selection are filter-based and wrapper-based approaches. In our work, we used a wrapper-based approach. Wrapper FS consists of three main components: the search algorithm, learning algorithm, and evaluation of the features. Wrappers are more potent than filters when accuracy is more

important than speed. This is because they explore the relevant subset of features in the search space of a particular classifier, where most studies use the same classifier used in the learning process [5]. On the other hand, the drawback of the wrappers is that they require a high computational time. Most studies use fast classifiers such as KNN as a primary classifier [5].

In our proposed approach, we utilize RWN as the base classifier; in addition to the fast-learning property, RWN has good generalization performance. Our wrapper-based approach selects HHO to search for the relevant feature subsets. In order to apply a metaheuristic optimization algorithm for a given task, two crucial design issues have to be addressed: the solution representation and the fitness function used to evaluate the solution, which are discussed below:

- 1) Solution Representation: A hawk in HHO represents a candidate solution for the targeted problem. A solution in our work consists of two parts. The first part is a set of binary bits 1 or 0, which indicate if the corresponding features are selected or not. The second part of the candidate solution consists of a group of binary bits that determine the number of hidden nodes in RWN. The length of the solution is $L + M$, where L is the number of features in the dataset, and M is the number of bits reserved to represent the maximum number of hidden neurons.
- 2) Fitness Function: A fitness function is needed to assess the quality of the solutions. In this work, we use a fitness function that addresses three objectives: increasing the classification accuracy, reducing the dimensionality of the dataset by selecting the relevant features, and decreasing the complexity of the RWN in terms of the number of hidden nodes. This fitness function is defined in Eq. 1.

$$Fitness = \alpha Err + \beta \frac{f}{F} + \gamma \frac{n}{N} \quad (1)$$

The parameters α , β , and γ are three factors within the range [0–1] that control the weight of each of the classification rate, number of selected features, and hidden neurons, respectively. Err represents the classification error rate of the RWN classifier, f denotes the number of selected features, F is the total number of original features in the dataset, n is the number of neurons determined by the evaluated HHO solution, and N is the maximum number of possible neurons in the RWN. The maximum number of neurons is set to 1024, which is represented by ten elements in the solution. Usually, the error rate is measured as ($Err = 1 - Acc$), where Acc represents the classification accuracy. To consider the imbalanced datasets, we use the F-measure instead of accuracy in the error rate measure. Thus, the error rate in our case becomes ($Err = 1 - F_measure$). After we obtained the selected features from the FS process, we must remove the irrelevant features and keep only the selected features from the training and testing data which will highly improve the performance measure. The proposed approach is illustrated in Fig.1. The code is available in the GitHub [19].

As mentioned earlier, the proposed approach was applied in two stages: centralized and distributed ML. In the centralized ML model, we trained the proposed approach and other traditional ML techniques by using the entire training dataset. Then we use the centralized ML model as a reference to compare the performance of each corresponding distributed ML model in each dataset. In contrast, the distributed ML models, representing various IoT devices, were trained on local datasets. We split the training datasets by sampling without replacement method to ensure the diversity (i.e. different parts of the training datasets) for each user. So, each user has local data and applies the proposed approach and other ML techniques, thus distributed ML contributes to preserve the data privacy.

IV. RESULTS AND DISCUSSION

This section presents a performance evaluation of the proposed approach through experiments on the datasets. All the experiments were performed using a PC with Intel Core (TM) i7-165G7 2.8 GHz and 16 GB RAM. The proposed approach was implemented and tested in Python 3.9.12. Initially, the datasets are divided into (66% and 34%) for training and testing, respectively. The training dataset is further distributed into (75% and 25%) for training and validation, respectively.

Since Evolutionary Algorithms (EAs) are based on randomness, experiments must be repeated several times to reduce the random effect in EAs performance. Therefore, the proposed approach was tested under 30 independent runs, while the number of iterations was 100 and the population size was 200. Commonly, the population size should be large enough to guarantee the diversity of the solutions [20]. Most recent references have set the value of the population size to 200 or less [7], [10]. Therefore, we used the maximum population size value of many studies. Also, many previous works have set the values of α , β , and γ , fitness function parameters to 0.99, 0.01, and 0.01, respectively [5], [7]. Therefore, this paper uses the same values of these parameters in the fitness function. In addition, we compare the performance with other known classifiers commonly used in the literature, including KNN, SVM, Adaboost, and DT. This experiment aims to show the motivation for using RWN as a primary classifier within the FS method and as a final classifier. Because the datasets are imbalanced, considering the accuracy ratio for evaluation is misleading. Therefore, we should examine other metrics such as recall, precision, and F-measure. For all results, the best results were indicated by a bold typeface. The results of accuracy, recall, precision, and F-measure values of the centralized and distributed ML models are shown in Tables I and II, respectively. According to the HHO-RWN results in Table I, we can see that all average accuracy values are enhanced compared to SVM and Adaboost classifiers. The accuracy rate has improved up to 2.6% compared to HHO-SVM in Security camera device. Regarding the average precision results, we can observe that all values in HHO-RWN are higher than other classifiers. The precision enhancement rate reached 6.6% in Phishing legitimate dataset. As for the average F-measure,

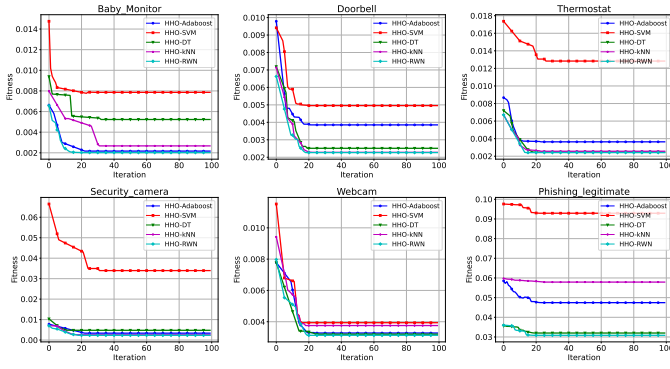


Fig. 2. The convergence curves for centralized ML models during training iterations.

HHO-RWN outperforms the other classifiers with 4 out of 5 devices in the N-BaIoT dataset. It also achieved the best average F-measure result in Phishing legitimate dataset. The maximum result accomplished by HHO-RWN with 99.9%. The F-measure rate has improved by 8.0% compared to HHO-SVM in Webcam device. Table II illustrates the results for the distributed ML model. We can observe that HHO-RWN and HHO-DT obtained the highest F-measure with 99.9% in the Webcam dataset, and HHO-Adaboost achieved the second highest with 99.5%. The F-measure rate has improved up to 9.3%. The precision rate has enhanced up to 14.5% in Phishing legitimate dataset. According to the average recall results, the maximum result achieved by HHO-RWN with 99.0%, and the improvement rate reached 24.0% in the Security camera device. Additionally, we compare the performance of centralized and distributed ML models. The average F-measure of distributed ML yields the best results in the Security camera device with 99.9%, and it shares the same results with the centralized ML model in the Baby Monitor device with 99.8% and in the Webcam device with 99.9%, and is very competitive in the other cases. Overall, the results in the distributed ML scheme showed promising performance. In the distributed ML scheme, we trained the proposed approach on a portion of the training dataset. While in the centralized scheme, the proposed approach has been trained in the entire training dataset, leading to higher generalization and better performance.

The convergence curves of the HHO-RWN in centralized and distributed ML models with other classifiers are shown in Figs. 2 and 3, respectively for all datasets, according to the measurement of fitness. It can be seen that the different selection schemes show a similar convergence pattern. However, the proposed approach is relatively preferable with regards to the convergence rate. Noting that 100 iterations are used to monitor convergence in all cases. It is reasonable to say that the best feature subsets and the best number of hidden neurons that are selected by the proposed approach enable it to obtain higher values based on the four metrics measured on the testing dataset. Table III shows the comparison of average accuracy, recall, and precision values between HHO-RWN and other metaheuristics. According to the collected results, HHO-RWN

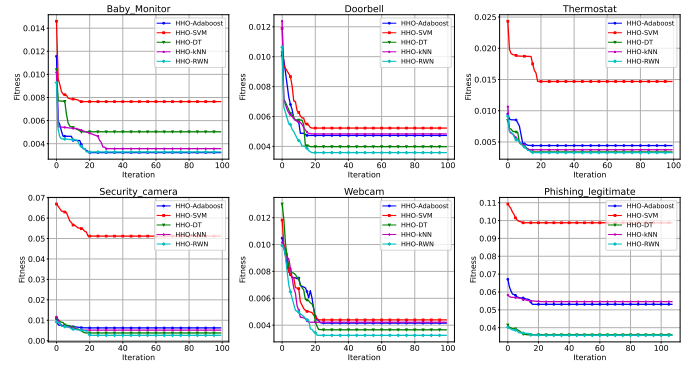


Fig. 3. The convergence curves for distributed ML models during training iterations.

achieved the highest average accuracy among all algorithms for two devices. HHO-RWN recorded the best performance with a 0.999% accuracy at the Baby monitor device. When evaluating HHO-RWN ability to correctly identify anomalies, the results were the best in two devices. Table III also reveals that HHO-RWN achieved the best average precision values among two devices.

Since privacy and security factors are essential in many applications, distributed ML is a promising learning solution. It enables the training of machine learning models locally, so there is no need to transfer the data to a central cloud. Thus, the reduction in heavy data transmissions will minimize the number of potential attacks consequently decreasing the risks of privacy leakage. Therefore, the choice of whether to build a centralized or distributed model depends on the target application and the nature of the data. We can say that choosing the appropriate learning scheme depends on the application's environment, priorities, and objectives while considering factors of privacy, performance, and computational resources.

V. CONCLUSION

Due to the dramatic increase in the number of IoT devices deployed online and the security sensitives of these devices, hackers and attackers exploit the increase of such devices to deploy different types of attacks. Intrusion detection systems are one of the techniques allocated to protecting the IoT network. The main aim of the proposed approach is to detect IoT botnet attacks by utilizing HHO to improve RWN and at the same time, to perform FS based on centralized and distributed ML models. Experimental results revealed that the proposed model performs well in centralized and distributed models to detect attacks on smart IoT devices. For future work, we plan to integrate the proposed approach using Federated Learning (FL) to improve security and privacy issues. In addition, investigate the efficiency of the proposed approach for other types of applications such as the healthcare system.

ACKNOWLEDGEMENTS

This research was supported by the Technology Innovation Institute (TII), Abu Dhabi, UAE, under the CyberAI project

TABLE I
EVALUATION RESULTS OF PROPOSED APPROACH AND OTHER COMPARATIVE METHODS UNDER THE CENTRALIZED LEARNING SCHEME.

Datasets	HHO-KNN				HHO-SVM				HHO-Adaboost				HHO-DT				HHO-RWN			
	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure
Baby_Monitor	0.996	0.989	0.993	0.994	0.991	0.954	0.991	0.979	0.997	0.992	0.988	0.992	0.990	0.993	0.993	0.985	0.999	0.996	0.995	0.998
Doorbell	0.999	0.989	0.987	0.993	0.996	0.982	0.982	0.954	0.995	0.990	0.973	0.992	0.994	0.995	0.992	0.977	0.998	0.984	0.996	0.997
Thermostat	0.999	0.958	0.978	0.992	0.984	0.983	0.984	0.988	0.998	0.851	0.972	0.996	0.998	0.995	0.933	0.976	0.995	0.968	0.995	0.999
Security_camera	0.998	0.991	0.985	0.970	0.974	0.720	0.974	0.963	0.997	0.980	0.991	0.992	0.997	0.993	0.991	0.960	1.000	0.992	1.000	0.990
Webcam	0.997	0.992	0.989	0.993	0.996	0.978	0.996	0.919	0.998	0.992	0.982	0.995	0.999	0.993	0.992	0.953	0.998	0.997	0.998	0.999
Phishing_legitimate	0.951	0.953	0.947	0.951	0.906	0.899	0.909	0.821	0.967	0.942	0.944	0.944	0.965	0.957	0.972	0.965	0.974	0.973	0.975	0.974

TABLE II
EVALUATION RESULTS OF PROPOSED APPROACH AND OTHER COMPARATIVE METHODS UNDER THE DISTRIBUTED LEARNING SCHEME.

Datasets	HHO-KNN				HHO-SVM				HHO-Adaboost				HHO-DT				HHO-RWN			
	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure	Acc	Rec	Prec	F-measure
Baby_Monitor	0.991	0.997	0.991	0.996	0.989	0.972	0.990	0.994	0.992	0.995	0.998	0.996	0.996	0.990	0.966	0.990	0.998	0.994	0.991	0.998
Doorbell	0.998	0.991	0.982	0.997	0.995	0.989	0.982	0.997	0.993	0.984	0.994	0.998	0.993	0.990	0.970	0.999	0.996	0.980	0.994	0.996
Thermostat	0.997	0.945	0.926	0.997	0.984	0.980	0.984	0.981	0.996	0.943	0.965	0.997	0.997	0.895	0.969	0.998	0.992	0.971	0.993	0.997
Security_camera	0.998	0.988	0.988	0.971	0.970	0.750	0.950	0.924	0.997	0.983	0.992	0.994	0.999	0.981	0.983	0.998	0.997	0.990	0.997	0.998
Webcam	0.996	0.990	0.992	0.990	0.990	0.988	0.994	0.906	0.996	0.996	0.996	0.995	0.999	0.998	0.996	0.999	0.995	0.996	0.994	0.999
Phishing_legitimate	0.941	0.886	0.927	0.930	0.909	0.857	0.827	0.898	0.969	0.958	0.959	0.958	0.959	0.936	0.935	0.959	0.969	0.970	0.972	0.963

TABLE III
COMPARISON BETWEEN HHO-RWN AND OTHER METAHEURISTICS IN TERMS OF ACCURACY, RECALL, AND PRECISION

Dataset	Accuracy				Recall				Precision			
	HHO-RWN	NSGA-II	MOPSO-Lévy	SPEA-II	HHO-RWN	NSGA-II	MOPSO-Lévy	SPEA-II	HHO-RWN	NSGA-II	MOPSO-Lévy	SPEA-II
Baby Monitor	0.999	0.565	0.937	0.604	0.996	0.985	0.920	0.967	0.995	0.479	0.710	0.521
Doorbell	0.998	0.487	0.989	0.801	0.984	0.693	0.780	0.902	0.996	0.256	1.000	0.559
Thermostat	0.995	0.289	0.998	0.327	0.968	0.149	0.997	0.157	0.995	0.022	0.957	0.000

(grant number: TII/DSRC/2022/3036).

REFERENCES

- [1] M. Aloqaily, S. Otoum, I. Al Ridhawi, and Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," *Ad Hoc Networks*, vol. 90, p. 101842, 2019.
- [2] B. Ghimire and D. B. Rawat, "Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things," *IEEE Internet of Things Journal*, 2022.
- [3] C. Koliass, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.
- [4] O. A. Alzubi, J. A. Alzubi, A. Al-Zoubi, M. A. Hassonah, and U. Kose, "An efficient malware detection approach with feature weighting based on harris hawks optimization," *Cluster Computing*, vol. 25, no. 4, pp. 2369–2387, 2022.
- [5] H. Faris, A.-Z. Ala'M, A. A. Heidari, I. Aljarah, M. Mafarja, M. A. Hassonah, and H. Fujita, "An intelligent system for spam detection and identification of the most relevant features based on evolutionary random weight networks," *Information Fusion*, vol. 48, pp. 67–83, 2019.
- [6] Z. Chkirbene, A. Erbad, R. Hamila, A. Mohamed, M. Guizani, and M. Hamdi, "Tidcs: A dynamic intrusion detection and classification system based feature selection," *IEEE Access*, vol. 8, pp. 95 864–95 877, 2020.
- [7] N. M. Hijazi, H. Faris, and I. Aljarah, "A parallel metaheuristic approach for ensemble feature selection based on multi-core architectures," *Expert Systems with Applications*, vol. 182, p. 115290, 2021.
- [8] Y. Jiang, K. Zhang, Y. Qian, and L. Zhou, "Anonymous and efficient authentication scheme for privacy-preserving distributed learning," *IEEE Transactions on Information Forensics and Security*, 2022.
- [9] F. Zerka, V. Urovi, F. Bottari, R. T. Leijenaar, S. Walsh, H. Gabrani-Juma, M. Gueuning, A. Vaidyanathan, W. Vos, M. Occhipinti et al., "Privacy preserving distributed learning classifiers—sequential learning with small sets of data," *Computers in Biology and Medicine*, vol. 136, p. 104716, 2021.
- [10] M. Habib, I. Aljarah, and H. Faris, "A modified multi-objective particle swarm optimizer-based lévy flight: An approach toward intrusion detection in internet of things," *ARABIAN JOURNAL FOR SCIENCE AND ENGINEERING*, 2020.
- [11] A. A. Heidari, S. Mirjalili, H. Faris, I. Aljarah, M. Mafarja, and H. Chen, "Harris hawks optimization: Algorithm and applications," *Future generation computer systems*, vol. 97, pp. 849–872, 2019.
- [12] S. Sokkalingam and R. Ramakrishnan, "An intelligent intrusion detection system for distributed denial of service attacks: A support vector machine with hybrid optimization algorithm based approach," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 27, p. e7334, 2022.
- [13] W. F. Schmidt, M. A. Kraaijveld, R. P. Duin et al., "Feed forward neural networks with random weights," in *International conference on pattern recognition*. IEEE Computer Society Press, 1992, pp. 1–1.
- [14] E. F. Rawashdeh, I. Aljarah, and H. Faris, "A cooperative coevolutionary method for optimizing random weight networks and its application for medical classification problems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 321–342, 2021.
- [15] A. Tuladhar, S. Gill, Z. Ismail, N. D. Forkert, A. D. N. Initiative et al., "Building machine learning models without sharing patient data: A simulation-based analysis of distributed learning by ensembling," *Journal of biomedical informatics*, vol. 106, p. 103424, 2020.
- [16] D. H. Wolpert and W. G. Macready, "No free lunch theorems for optimization," *IEEE transactions on evolutionary computation*, vol. 1, no. 1, pp. 67–82, 1997.
- [17] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, and Y. Elovici, "N-baiot—network-based detection of iot botnet attacks using deep autoencoders," *IEEE Pervasive Computing*, vol. 17, no. 3, pp. 12–22, 2018.
- [18] C. L. Tan, "Phishing dataset for machine learning: Feature evaluation," *Mendeley Data*, vol. 1, 2018.
- [19] N. Hijazi, M. Aloqaily, B. Ouni, F. Karray, and M. Debbah, "Harris hawks feature selection in distributed machine learning for secure iot environments." [Online]. Available: <https://github.com/Artificialleap-MBZUAI/Harris-Hawks-Feature-Selection-in-Distributed-Machine-Learning-for-Secure-IoT-Environments>
- [20] H. Fukumoto and A. Oyama, "Study on improving efficiency of multi-objective evolutionary algorithm with large population by m2m decomposition and elitist mate selection scheme," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2018, pp. 1180–1187.