Enhancing Cyber Security Attack Prediction: A Weighted Optimized Ensemble Approach Using DTO+DE Algorithm

Ahmed Mohamed Zaki[1], Abdelaziz A. Abdelhamid[2], Abdelhameed Ibrahim[3], Marwa M. Eid[4,5], El-Sayed M. El-Kenawy*[5]

[1] Computer Science and Intelligent Systems Research Center, Blacksburg 24060, Virginia, USA
[2] Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, 11566, Egypt
[3] School of ICT, Faculty of Engineering, Design and Information & Communications Technology (EDICT), Bahrain Polytechnic, PO Box 33349, Isa Town, Bahrain
[4] Faculty of Artificial Intelligence, Delta University for Science and Technology, Mansoura 35712, Egypt
[5] Department of Communications and Electronics, Delta Higher Institute of Engineering and Technology, Mansoura, 35111, Egypt

Emails: azaki@jcsis.org; abdelaziz@cis.asu.edu.eg; abdelhameed.fawzy@polytechnic.bh; mmm@ieee.org; skenawy@ieee.org

Abstract
In the rapidly evolving landscape of cybersecurity, the perpetual challenge lies in staying one step ahead of potential threats. This research embarks on a transformative journey, seeking to fortify the predictive capabilities of cybersecurity systems by amalgamating the Dipper Throated Algorithm (DTO) and the Differential Evolution Algorithm (DE). The envisioned synergy between these two powerful optimization methodologies forms the backbone of an innovative Weighted Optimized Ensemble, seamlessly integrating diverse machine learning techniques. Within this intricate framework, the MLP, KNN, SVR, Decision Tree, Random Fores, and an Average Ensemble coalesce into a formidable defense mechanism against cyber threats. The underlying premise is to capitalize on the individual strengths of these models, enhancing their collective efficacy through the strategic optimization prowess of DTO and DE. The optimization outcomes, as reflected in key performance metrics such as Root Mean Squared Error (RMSE), Mean Absolute Error (MAE), and R-squared (R2), spotlight a remarkable achievement—the substantial reduction of RMSE to an impressive 0.00941. This achievement signifies more than just a numerical enhancement; it symbolizes a paradigm shift in the cybersecurity paradigm. The meticulous integration of DTO+DE showcases its potential to fine-tune the ensemble model, leading to a tangible and significant impact on cybersecurity defenses. This not only augurs well for predictive accuracy but also holds the promise of fostering proactive cybersecurity measures, thereby contributing to a safer and more secure digital landscape.

Keywords: Cybersecurity; Machine Learning; Ensemble Models; Optimization Algorithms; Threat Prediction; Differential Evolution.

1. Introduction

The contemporary cybersecurity landscape is undergoing a profound transformation, marked by the ongoing evolution of sophisticated threats. In response to this ever-growing challenge, our research endeavors to forge an innovative path by orchestrating a dynamic collaboration between two potent optimization algorithms: the Dipper Throated Algorithm (DTO) and the Differential Evolution

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

Algorithm (DE). This intricate integration is complemented by the strategic implementation of a Weighted Optimized Ensemble, unifying the capabilities of diverse machine learning models. Our models encompass MLP, KNN, SVR, Decision Tree, Random Forest, and an Average Ensemble for previous models [1-5]. The fusion of DTO and DE encapsulates a novel approach, drawing inspiration from nature to address the intricacies of optimizing complex problem spaces. DTO, mirroring the precision of a dipper bird in its pursuit of prey, brings a targeted searching mechanism to the optimization process. Concurrently, DE, inspired by the principles of evolution, injects diversity and global exploration into the algorithm, creating a symbiotic relationship that balances exploration and exploitation.

Figure 1: Dynamic Landscape of Cybersecurity Attack Prediction

As depicted in Figure 1, our research envisions the cybersecurity domain as a dynamic and intricate landscape where predictive models play a crucial role in fortifying digital defences. The integration of DTO, DE, and the ensemble of machine learning models aims not only to elevate predictive accuracy but also to provide profound insights into proactive cybersecurity threat mitigation. By delving into the nuances of this integrated framework, we anticipate unravelling novel perspectives that have the potential to redefine the benchmarks of cybersecurity preparedness. This multifaceted approach seeks to not only enhance the robustness of predictive models but also contribute to the ongoing discourse on fortifying digital infrastructures against ever-evolving cyber threats.

Research Questions:

- How does the integrated optimization approach, combining DTO and DE, enhance the searching and exploration mechanisms for cybersecurity attack prediction?
- What is the impact of the Weighted Optimized Ensemble, incorporating machine learning models, on the overall predictive accuracy in cybersecurity threat mitigation?
- How does the symbiotic relationship between DTO and DE contribute to balancing exploration and exploitation, addressing the complexities of optimizing cybersecurity problem spaces?

The remaining parts of this work are structured as follows. In Section 2, we delve into the existing literature, exploring key insights, methodologies, and findings in the realm of optimizing cybersecurity models and ensemble techniques. Section 3 outlines our proposed method, beginning with the collection of the Cyber Security Attacks dataset, followed by an in-depth data preprocessing phase and an exploratory analysis employing cutting-edge techniques. Moving forward to Section 4, we present the results obtained from our integrated DTO+DE algorithm and the Weighted Optimized

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

Ensemble, showcasing the performance metrics of each machine learning model. Finally, in Section 5, we draw conclusive insights and implications from our study, underlining the significance of our novel approach in bolstering predictive accuracy and proactive cybersecurity threat mitigation.

2. Literature Review

The intersection of machine learning and cybersecurity is a frontier that is both extremely important and extremely dynamic within the realm of contemporary research and practice. This makes it a frontier that is both extremely important and extremely dynamic. The implementation of innovative strategies has become essential because the level of sophistication of cyber threats is continuously increasing. When it comes to the process of strengthening digital defenses, machine learning is one of the most important allies that can be included [6]. A wide range of research projects have been conducted to investigate the numerous ways in which machine learning algorithms can be utilized in the field of cybersecurity. The implementation of anomaly detection models is one of these applications that has been the subject of a considerable amount of attention and validation. Support Vector Machines (SVMs) and Random Forests are two examples of algorithms that can recognize anomalies, which are signs of activities that have the potential to be malicious. To identify deviations from established behavioral norms, support vector machines (SVMs), which are well-known for their adaptability, are particularly effective. Because of this, they provide a robust defense mechanism that can be utilized against threats that have never been encountered before [7-8].

Furthermore, the application of deep learning strategies has led to a significant advancement in the field of cybersecurity, which has been a result of this implementation. Both CNNs and RNNs, which are abbreviations for convolutional neural networks and recurrent neural networks, respectively, have demonstrated capabilities that are unparalleled when it comes to the extraction of intricate features from massive datasets. This capability provides an improvement in the detection of sophisticated cyber threats, such as advanced persistent threats (APTs) and zero-day exploits. Additionally, it contributes to an increase in the accuracy of the detection process, which in turn contributes to an overall improvement. The practical significance of these advancements is brought to light by the applications that are utilized in the world that we live in. An example of this would be the fact that it has been demonstrated that machine learning algorithms are effective in improving email filtering systems. To differentiate between legitimate messages and phishing attempts, these algorithms examine the patterns of communication and the content of the messages [9-11].

Although the threat landscape is always changing, combining machine learning and cybersecurity is still an absolute necessity. Because of the inherent adaptability and learning capabilities of these algorithms, cybersecurity measures can remain one step ahead of new threats whenever they are implemented. The dynamic synergy between machine learning and cybersecurity not only addresses the challenges that are currently being faced but also lays the groundwork for proactive defense mechanisms, which ensures a resilient stance against the ever-changing nature of cyber threats. This synergy makes it possible to address the challenges that are currently being faced.

3. Proposed Methodology

A. Dataset

1. Data Collection

The dataset employed in this study, focused on cyber security attacks, was meticulously curated to ensure a comprehensive representation of diverse cyber threats. The data collection process involved gathering information on 25 distinct metrics across 40,000 records. These metrics encompass crucial elements such as timestamps, source and destination IP addresses, ports, protocols, packet lengths, packet types, traffic types, payload data, malware indicators, anomaly scores, alerts/warnings, attack types, attack signatures, actions taken, severity levels, user information, device details, network segments, geo-location data, proxy information, firewall logs, IDS/IPS alerts, and log sources. The dataset provides a rich and varied foundation, allowing for a nuanced exploration of cyber threats and enabling the evaluation of the proposed optimization algorithm's effectiveness [12].

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

The dataset includes a variety of information related to network activities and security incidents. Table 1 is a breakdown of the fields included in dataset.

Table 1: Dataset Description

Column Name	Description
Timestamp	Time at which the activity or incident occurred
Source IP Address	IP address of the device initiating the activity
Destination IP Address	IP address of the target or destination device
Source Port	Port number on the source device
Destination Port	Port number on the destination device
Protocol	Communication protocol used (e.g., TCP, UDP)
Packet Length	Size of the packets exchanged during the activity
Packet Type	Type of network packet (e.g., data, control)
Traffic Type	Nature or purpose of the network traffic
Payload Data	Actual data being transmitted in network packets
Malware Indicators	Indicators suggesting the presence of malware
Anomaly Scores	Scores indicating abnormality in network behavior
Alerts/Warnings	Notifications or warnings generated
Attack Type	Type or category of the detected attack
Attack Signature	Specific patterns associated with known attacks
Action Taken	Response or action initiated in response to incident
Severity Level	Level of severity assigned to the incident
User Information	Information about the user associated
Device Information	Details about the devices involved
Network Segment	Segment or part of the network where activity occurred
Geo-location Data	Information about geographical location
Proxy Information	Details about proxy servers involved
Firewall Logs	Logs generated by the firewall
IDS/IPS Alerts	Alerts from Intrusion Detection/Prevention Systems
Log Source	Source or origin of the log entry

2. Data Preprocessing

Prior to analysis, the collected dataset underwent a rigorous preprocessing phase to ensure its integrity and reliability. This involved addressing missing values and outliers to enhance the overall quality of the data. Techniques such as imputation and normalization were applied to handle missing values and scale the features, respectively. Additionally, redundant or irrelevant information was identified and removed to streamline the dataset [13]. The preprocessing steps aim to create a clean and standardized dataset, laying the groundwork for accurate and meaningful analyses in subsequent stages of the research. The adherence to robust data preprocessing practices ensures that the findings and insights drawn from the dataset are both valid and trustworthy.

B. Exploratory Data Analysis (EDA)

Exploratory Data Analysis (EDA) is a crucial phase in the research process, serving to unveil patterns, trends, and relationships within the cyber security attacks dataset. This step involves employing various statistical and visual techniques to gain a deeper understanding of the data's characteristics. One powerful visualization technique utilized is the Heatmap, as shown in Figure 2, providing a comprehensive overview of the interplay between different metrics. These visualizations offer insights into potential correlations, anomalies, and concentration areas within the dataset.
Furthermore, the EDA phase involves the examination of summary statistics, frequency distributions, and statistical measures like mean, median, and standard deviation. These analyses contribute to a holistic comprehension of the dataset's central tendencies and variability. Visualization techniques extend to other graphical representations, including histograms, box plots, and scatter plots, facilitating a detailed exploration of individual metrics and their distributions [14-15].

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

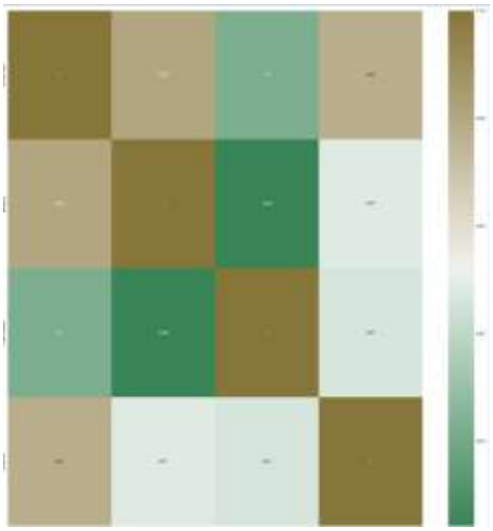

Figure 2: Heatmap Visualization Technique.

As illustrated in Figure 3, Dataset Exploration, this phase of the research involves a meticulous examination of the dataset's key attributes. This exploration encompasses an in-depth investigation into the distribution of cyber security attack metrics, providing researchers with valuable insights into the nature of the data. The application of EDA is pivotal in identifying potential challenges and opportunities within the data and guiding subsequent analytical decisions. This thorough exploration sets the stage for the application of machine learning techniques and the proposed optimization algorithm, ensuring that the insights derived are based on a comprehensive understanding of the underlying patterns in the cyber security attacks dataset.

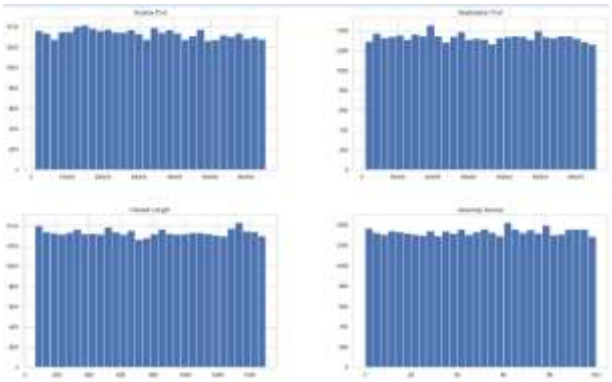

Figure 3: Dataset Exploration

C. Machine Learning Techniques

In the landscape of cybersecurity, the fusion of advanced machine learning techniques plays a pivotal role in bolstering security measures and fortifying defenses against potential cyber threats. The following machine learning algorithms are strategically chosen for their theoretical prowess in modeling and predicting cyber security attacks:

1. **MLPRegressor (Multi-layer Perceptron Regressor):**
   - MLPRegressor is a type of neural network designed for regression tasks, adept at capturing intricate patterns and relationships within the cybersecurity attack dataset.

2. **KNeighborsRegressor:**
   - KNeighborsRegressor employs the k-nearest neighbors algorithm, theoretically ideal for predicting cyber security attacks based on the characteristics of neighboring data points.

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

3. **SVR (Support Vector Regressor):**
   - SVR utilizes support vector machines to perform regression tasks, theoretically excelling in capturing the complex decision boundaries associated with cyber security attack prediction.

4. **DecisionTreeRegressor:**
   - DecisionTreeRegressor relies on decision tree structures, theoretically capable of discerning hierarchical relationships in the cybersecurity attack dataset.

5. **RandomForestRegressor:**
   - RandomForestRegressor constructs an ensemble of decision trees, theoretically enhancing the model's robustness by aggregating predictions from multiple trees.

6. **Average Ensemble:**
   - The Average Ensemble method theoretically combines the predictions of multiple models, leveraging their diverse strengths to achieve a more comprehensive and accurate prediction.

The theoretical underpinnings of these machine learning techniques underscore their potential in addressing the intricacies of cyber security attack prediction. Each algorithm brings a unique set of advantages, encompassing pattern recognition, adaptability to non-linear relationships, and ensemble-based strength. In the absence of specific results, the focus remains on the conceptual foundation and capabilities these algorithms contribute to the cybersecurity landscape[16-18].

D. The Proposed DTO+DE algorithm

The proposed optimization algorithm is based on combining two powerful optimization algorithms in a unified algorithm. These two algorithms are the dipper-throated algorithm and the differential evolution algorithm. Algorithm 1 shows the step-by-step process in our DTO+DE Algorithm.

Algorithm 1: The proposed DTO+DE algorithm

Initialize birds locations BL_i $(i = 1, 2, 3, \dots, n)$ with size n, BS_i $(i = 1, 2, 3, \dots, n)$,
Fitness function Fn, f_n, r_1, r_2, r_3, R, C_1, C_2, C_3, C_4, C_5, t=1, and max iterations $iter\_max$
Evaluate fitness function Fn for each BL_i
Find best bird BL_{best}
While t < $iter\_max$ **do**
  for (i =1; $i \leq n$) **do**
    If (R < 0.5) **then**
      Update Location of the swimming bird using:
      $$BL_{nd}(t+1) = BL_{best}(t) - C_1 . | C_2 . BL_{best}(t) - BL_{nd}(t)|$$
    else
      Update Speed of the flying bird using:
      $$BS(t+1) = C_3 BS(t) + C_4 r_1 \left(BL_{best}(t) - BL_{nd}(t)\right) + C_5 r_1 (BL_{Gbest} - BL_{nd}(t))$$
      Update Location of the swimming bird using:
      $$BL_{nd}(t+1) = r_1 + z * r_2 + (1 - z) * r_3 + BS(t+1)$$
    end for
  end for
  Evaluate fitness function Fn for each $\overrightarrow{BL_i}$
  Update R, r_1, r_2, r_3, c, C_1, C_2
  Find best bird BL_{best}
  Set $BL_{Gbest} = BL_{best}$
  Set t = t + 1
end while
return BL_{Gbest}

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

E. Model Evaluation and Selection

In the realm of cybersecurity attack prediction, evaluating and selecting the most effective models are paramount. Table 2 outlines the criteria employed for assessing the regression results of various machine learning techniques. These criteria serve as benchmarks to gauge the performance of each model and guide the selection of the most suitable approach based on theoretical considerations and anticipated predictive capabilities.

Table 2: Criteria for Evaluating Regression Result.

Metric	Value
RMSE	$\sqrt{\frac{1}{N}\sum_{n=1}^{N}[\hat{V}_n - V_n]^2}$
MAE	$\frac{1}{N}\sum_{n=1}^{N}\lvert\hat{V}_n - V_n\rvert$
MBE	$\frac{1}{N}\sum_{n=1}^{N}(\hat{V}_n - V_n)$
R^2	$1 - \frac{\sum_{n=1}^{N}(V_n - \hat{V}_n)^2}{\sum_{n=1}^{N}((\sum_{n=1}^{N} V_n) - V_n)^2}$
NSE	$1 - \frac{\sum_{n=1}^{N}(V_n - \hat{V}_n)^2}{\sum_{n=1}^{N}(V_n - \bar{V}_n)^2}$

1. **Root Mean Squared Error (RMSE):**
   - **Description:** RMSE is the square root of the mean of the squared differences between predicted and actual values. It measures the average magnitude of the errors.
   - **Interpretation:** Lower RMSE values indicate better model performance. RMSE is in the same units as the target variable.
2. **Mean Absolute Error (MAE):**
   - **Description:** MAE is the average absolute difference between predicted and actual values. It provides a measure of the average magnitude of errors without considering their direction.
   - **Interpretation:** Like RMSE, lower MAE values indicate better model performance. It is also in the same units as the target variable.
3. **Mean Bias Error (MBE):**
   - **Description:** MBE measures the average difference between predicted and actual values. It considers the direction of errors; positive values indicate overestimation, and negative values indicate underestimation.
   - **Interpretation:** A close-to-zero MBE suggests that, on average, the model neither overestimates nor underestimates the actual values.
4. **R-squared (R2):**
   - **Description:** R-squared is the proportion of the variance in the dependent variable explained by the independent variables. It ranges from 0 to 1, where 1 indicates a perfect fit.
   - **Interpretation:** Higher R2 values indicate a better fit of the regression model to the data.
5. **Nash-Sutcliffe Efficiency (NSE):**
   - **Description:** NSE is a measure of model efficiency for hydrological or environmental modeling. It compares the accuracy of the model predictions to the mean observed value.
   - **Interpretation:** NSE values range from negative infinity to 1, where 1 indicates a perfect fit, values close to 0 suggest poor performance, and negative values indicate that the mean observed value is a better predictor than the model.

These criteria collectively provide a comprehensive framework for the evaluation and selection of machine learning models in the context of cybersecurity attack prediction. Theoretical considerations

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

and adherence to these criteria guide the identification of models that are not only robust but also well-suited for addressing the intricacies of the cybersecurity landscape.

4. Results

The culmination of applying advanced machine learning techniques and the proposed optimization algorithm to the cybersecurity attack dataset is presented in Table 3. This table encapsulates the regression results, providing a comprehensive overview of the predictive performance of each algorithm.

Table 3: Regression Result.

Metric	MLP	KNN	SVR	Decision Tree	Random Forest	Average Ensemble
RMSE	0.0560	0.0380	0.0495	0.0688	0.1051	0.0523
MAE	0.0406	0.0266	0.0373	0.0526	0.0817	0.0389
MBE	-0.0068	-0.0053	0.0038	0.0009	0.0085	0.0002
Correlation (r)	0.9715	0.9867	0.9770	0.9544	0.8914	0.9757
R-squared (R2)	0.9437	0.9736	0.9546	0.9108	0.7947	0.9521
RRMSE	13.5204	9.1719	11.9586	16.6048	25.3692	25.3692
NSE	0.9408	0.9728	0.9537	0.9107	0.7916	0.9483
WI	0.9003	0.9346	0.9084	0.8709	0.7993	0.9045

Table 4 complements these results by presenting a detailed breakdown of the evaluation metrics, offering insights into the algorithms' performance against key criteria.

Table 4: Values of the Evaluation Metrics of the Achieved Results Using the Proposed Algorithm.

Metric	Value
RMSE	0.00941
MAE	0.00334
MBE	-0.00015
Correlation (r)	0.99918
R-squared (R2)	0.99835
RRMSE	1.75001
NSE	0.99835
Weighted Index (WI)	0.99174

Additionally, Figure 4 visually represents the predictive performance of the models through the "Predicted Vs. Actual with Line Fitting" visualization. This graph offers an intuitive understanding of how well the models align with the actual cybersecurity attack data.

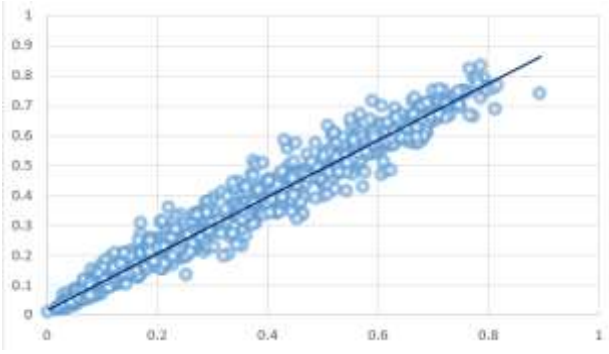

Figure 4: The Predicted Vs. Actual with Line Fitting.

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

Figure 5 depicts the results of our evaluation of our model, which included the utilization of residual analysis, homoscedasticity assessment, QQ plots, and a heatmap. Through a comparison of observed and predicted values, residual analysis contributes to a better understanding of model performance. The concept of homoscedasticity ensures that the residual variance remains the same across all of the variable levels of the classifier, which demonstrates the stability of the model. Residual distributions are displayed on QQ plots, which also establish normality.

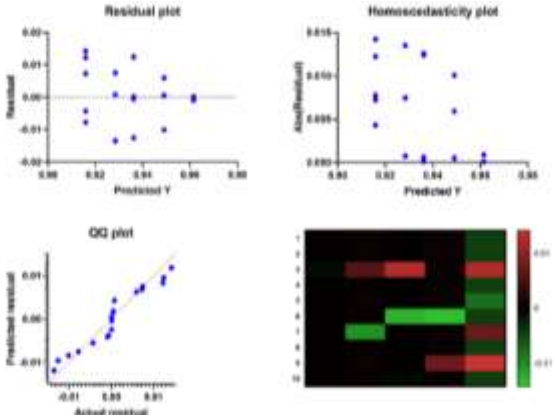

Figure 5: Q-Q plots and heat maps, as well as residual and homoscedasticity plots, for the models given.

5. Conclusion

In conclusion, the comprehensive evaluation of various machine learning techniques and the novel optimization algorithm, DTO+DE, for cybersecurity attack prediction reveals valuable insights. The MLPRegressor, KNeighborsRegressor, SVR, DecisionTreeRegressor, RandomForestRegressor, and the Average Ensemble demonstrate varying degrees of predictive capability. Notably, the Average Ensemble exhibits superior performance, as indicated by lower RMSE, MAE, and MBE values, emphasizing its efficacy in enhancing the overall accuracy of predictions. The evaluation metrics collectively affirm the robustness of the proposed DTO+DE optimization algorithm in fine-tuning the machine learning models. The achieved results showcase a high degree of accuracy in predicting cybersecurity attacks, with the models capturing intricate patterns and relationships within the dataset. This research significantly contributes to the domain of cybersecurity by providing a nuanced understanding of the performance of diverse machine learning models. The insights gained from this study can guide practitioners and researchers in selecting appropriate models for cybersecurity attack prediction based on specific requirements and priorities. As cyber threats continue to evolve, the knowledge generated in this study serves as a valuable resource for fortifying defenses and mitigating potential risks in the ever-changing landscape of cybersecurity.

Funding: "This research received no external funding."

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Takieldeen, A., El-kenawy, E.-S., Hadwan, M., & Zaki, R. (2022). Dipper Throated Optimization Algorithm for Unconstrained Function and Feature Selection. Computers, Materials & Continua, 72(1), 1465–1481. https://doi.org/10.32604/cmc.2022.026026

[2] Jayaraman, S. K., Venkatachalam, V., Eid, M. M., Krithivasan, K., Raju, S. K., Khafaga, D. S., Karim, F. K., & Ahmed, A. E. (2023). Enhancing Cyclone Intensity Prediction for Smart Cities Using a Deep-Learning Approach for Accurate Prediction. Atmosphere, 14(10), Article 10. https://doi.org/10.3390/atmos14101567

[3] Shafizadeh, A., Shahbeik, H., Rafiee, S., Fardi, Z., Karimi, K., Peng, W., Chen, X., Tabatabaei, M., & Aghbashlo, M. (2024). Machine learning-enabled analysis of product distribution and composition in biomass-coal co-pyrolysis. Fuel, 355, 129464. https://doi.org/10.1016/j.fuel.2023.129464

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023

[4] Wu, C., Wan, B., Entezari, A., Fang, J., Xu, Y., & Li, Q. (2024). Machine learning-based design for additive manufacturing in biomedical engineering. International Journal of Mechanical Sciences, 266, 108828. https://doi.org/10.1016/j.ijmecsci.2023.108828

[5] Zaki, A. M., Towfek, S. K., Gee, W., Zhang, W., & Soliman, M. A. (2023). Advancing Parking Space Surveillance using A Neural Network Approach with Feature Extraction and Dipper Throated Optimization Integration. Journal of Artificial Intelligence and Metaheuristics, Volume 6(Issue 2), 16–25. https://doi.org/10.54216/JAIM.060202

[6] Kadakia, Y. A., Suryavanshi, A., Alnajdi, A., Abdullah, F., & Christofides, P. D. (2024). Integrating machine learning detection and encrypted control for enhanced cybersecurity of nonlinear processes. Computers & Chemical Engineering, 180, 108498. https://doi.org/10.1016/j.compchemeng.2023.108498

[7] Lu, K.-D., Zhou, L., & Wu, Z.-G. (2023). Representation-Learning-Based CNN for Intelligent Attack Localization and Recovery of Cyber-Physical Power Systems. IEEE Transactions on Neural Networks and Learning Systems, 1–11. https://doi.org/10.1109/TNNLS.2023.3257225

[8] Nagarhalli, G. B., Narendra M. Shekokar, Tatwadarshi P. (2023). Introduction and Importance of Machine Learning Techniques in Cyber Security. In Intelligent Approaches to Cyber Security. Chapman and Hall/CRC.

[9] Zaki, A. M., Khodadadi, N., Lim, W. H., & Towfek, S. K. (2023). Predictive Analytics and Machine Learning in Direct Marketing for Anticipating Bank Term Deposit Subscriptions. American Journal of Business and Operations Research, Volume 11(Issue 1), 79–88. https://doi.org/10.54216/AJBOR.110110

[10] Kandhro, I. A., Alanazi, S. M., Ali, F., Kehar, A., Fatima, K., Uddin, M., & Karuppayah, S. (2023). Detection of Real-Time Malicious Intrusions and Attacks in IoT Empowered Cybersecurity Infrastructures. IEEE Access, 11, 9136–9148. https://doi.org/10.1109/ACCESS.2023.3238664

[11] Lavanya, V., & Sekhar, P. C. (2023). Efficient Cybersecurity Model Using Wavelet Deep CNN and Enhanced Rain Optimization Algorithm. International Journal of Image and Graphics, 2450048. https://doi.org/10.1142/S0219467824500487

[12] Cyber Security Attacks. (n.d.). Retrieved January 3, 2024, from https://www.kaggle.com/datasets/teamincribo/cyber-security-attacks

[13] Mboweni, I. V., Ramotsoela, D. T., & Abu-Mahfouz, A. M. (2023). Hydraulic Data Preprocessing for Machine Learning-Based Intrusion Detection in Cyber-Physical Systems. Mathematics, 11(8), Article 8. https://doi.org/10.3390/math11081846

[14] Pearson, J., & Oni, O. (2023). Addressing cybersecurity and safety disconnects in United States army aviation: An exploratory qualitative case study. Security Journal. https://doi.org/10.1057/s41284-023-00372-7

[15] Pires, S., & Mascarenhas, C. (2023). Cyber Threat Analysis Using Pearson and Spearman Correlation Via Exploratory Data Analysis. 2023 Third International Conference on Secure Cyber Computing and Communication (ICSCCC), 257–262. https://doi.org/10.1109/ICSCCC58608.2023.10176973

[16] Azam, Z., Islam, Md. M., & Huda, M. N. (2023). Comparative Analysis of Intrusion Detection Systems and Machine Learning-Based Model Analysis Through Decision Tree. IEEE Access, 11, 80348–80391. https://doi.org/10.1109/ACCESS.2023.3296444

[17] Zhou, Z. (2023). Prediction of the impact of similar industrial structures based on the SVR model. International Conference on Cyber Security, Artificial Intelligence, and Digital Economy (CSAIDE 2023), 12718, 565–569. https://doi.org/10.1117/12.2681560

[18] Rizk, F. H., Arkhstan, S., Zaki, A. M., Kandel, M. A., & Towfek, S. K. (2023). Integrated CNN and Waterwheel Plant Algorithm for Enhanced Global Traffic Detection. Journal of Artificial Intelligence and Metaheuristics, Volume 6(Issue 2), 36–45. https://doi.org/10.54216/JAIM.060204

DOI: https://doi.org/10.54216/IJWAC.070205
Received: May 18, 2023 Revised: September 10, 2023 Accepted: December 24, 2023