Metaheuristic Optimization for Enhancing Cyber Security Index Prediction: A DTO+FGW Approach with MLP Integration

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 realm of cybersecurity, the evaluation and enhancement of cyber resilience are paramount to safeguarding nations and organizations against evolving digital threats. This paper introduces a novel approach that integrates the Dipper Throated Algorithm (DTO) and the Grey Wolf Optimizer (GWO) to fortify the analysis of Cyber Security Indexes. These indexes encompass vital metrics, including the Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL). Leveraging the adaptive nature of DTO and the collaborative hunting strategies of GWO, the proposed DTO+GWO algorithm aims to optimize the evaluation of cyber readiness, exposure levels, and global commitments to cybersecurity. The Cyber Security Indexes dataset, featuring indicators from 193 countries, serves as the testing ground. This study contributes to advancing cyber threat assessment methodologies, fostering a proactive stance in the face of cyber risks globally. Through rigorous optimization, the DTO+GWO algorithm exhibits promising potential to elevate the precision and efficacy of cybersecurity evaluations. The optimization results demonstrate a notable achievement, with an RMSE of 0.0090, reflecting the algorithm's enhanced performance in fine-tuning the assessment of cybersecurity indexes.

Keywords: DTO Algorithm; Gray Wolf Algorithm; Cyber Security Indexes; Metaheuristic Optimization; Machine Learning; Cyber Threat Assessment.

1. Introduction

An increase in the number of cyber threats and the ongoing development of attack vectors are two factors that are contributing to the growing complexity of the digital landscape. As a means of adapting to this ever-changing environment, the field of cybersecurity is consistently looking for novel approaches to strengthen defences and effectively mitigate risks. In the field of cybersecurity indexes, this research endeavors to investigate the possibility of combining two powerful optimization

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

algorithms, namely the Dipper Throated Algorithm (DTO) and the Grey Wolf Optimizer (GWO). A journey is being taken to investigate the potential of this combination. One of the most important aspects of evaluating and comprehending the cybersecurity posture of nations is the utilization of cybersecurity indexes. These indexes offer essential insights into the degree to which a country is vulnerable to cybercrime, its level of commitment to global cybersecurity initiatives, its level of readiness to deal with cyber threats, and the overall level of maturity of its digital development. The purpose of this research is to contribute to the improvement of cybersecurity measures on both a national and a global scale by combining the power of DTO and GWO, as shown in Figure 1.

The Dipper Throated Algorithm draws inspiration from the unique foraging behavior of diapers and aquatic birds known for their efficient hunting techniques. In DTO, the optimization process mimics the dippers' ability to navigate their environment, seeking optimal solutions. This algorithm employs a diverse set of mechanisms, including exploration and exploitation strategies, to traverse the solution space efficiently. DTO's distinctive approach lies in its adaptive nature, dynamically adjusting parameters based on the evolving characteristics of the optimization landscape. The Grey Wolf Optimizer is inspired by the social hierarchy and hunting mechanisms of grey wolves in nature. GWO introduces the concept of alpha, beta, and delta wolves, representing the leadership structure within a wolf pack. These wolves collaboratively explore the search space, with alpha leading the search towards promising regions. GWO leverages the principles of hierarchical leadership and collaborative hunting to strike a balance between exploration and exploitation. This algorithm has gained recognition for its simplicity, efficiency, and effectiveness in solving complex optimization problems. In the context of cybersecurity indexes, the integration aims to harness their complementary strengths. DTO's adaptability and efficient exploration align well with the dynamic nature of cybersecurity challenges. At the same time, GWO's collaborative optimization strategy can enhance the search for optimal solutions in the intricate landscape of cybersecurity assessments. The fusion of these algorithms holds the promise of bolstering the capabilities of cybersecurity indexes for more accurate and insightful evaluations [1-5].

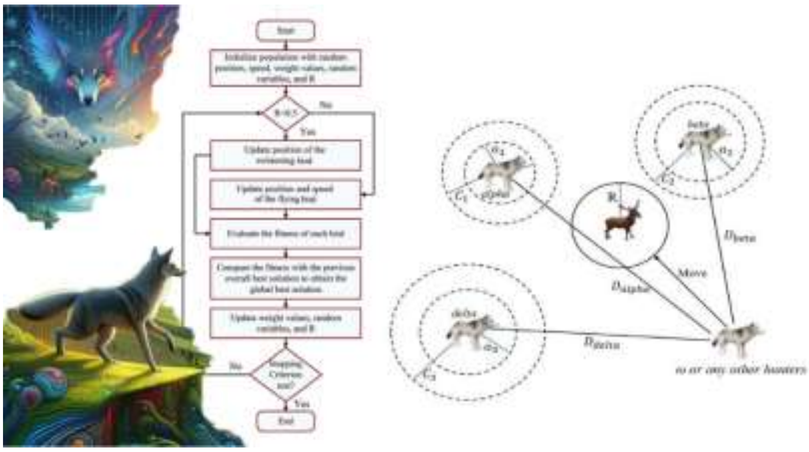

Start
Initialize population with random position, speed, weight values, random variables, and R
R<0.5
No
Yes
Update position of the swimming bird
Update position and speed of the flying bird
Evaluate the fitness of each bird
Compare the fitness with the previous overall best solution to obtain the global best solution
Update weight values, random variables, and R
Stopping Criterion met?
No
Yes
End
a_1
C_1
alpha
beta
a_2
C_2
R
D_{beta}
Move
D_{alpha}
delta
a_3
C_3
D_{delta}
ω or any other hunters

Figure 1: Dynamic Interplay Between the Dipper Throated Algorithm (DTO) and The Grey Wolf Optimizer (GWO)

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?

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

As we progress through the subsequent sections, including an in-depth literature review, a comprehensive methodology delineation, and the presentation of results, the paper unfolds the rationale behind the amalgamation of DTO and GWO. The overarching aim is not only to elucidate the intricacies of these optimization algorithms but also to underscore their practical application in fortifying cybersecurity indexes. In an era where cyber threats are persistent and sophisticated, adaptive defense mechanisms are imperative. This research strives to make significant strides in advancing our understanding and application of optimization techniques for bolstering cybersecurity in an ever-evolving digital landscape.

2. Literature Review

The literature surrounding the amalgamation of optimization algorithms and cybersecurity indexes provides valuable insights into the evolution of methodologies employed to fortify cyber defenses. In the context of DTO and GWO, existing research has explored their capabilities in diverse optimization scenarios. The Dipper Throated Algorithm (DTO) has demonstrated its efficacy in problem-solving by mimicking the dipping motion of a bird's beak during feeding, showcasing adaptability and versatility. On the other hand, the Grey Wolf Optimizer (GWO) draws inspiration from the cooperative hunting strategies of grey wolves, exhibiting collaborative and strategic optimization capabilities [6].

In the realm of cybersecurity, the literature highlights the growing importance of robust optimization algorithms to enhance cyber threat assessments and readiness. Previous studies have often focused on individual optimization algorithms, emphasizing their unique strengths and applications. However, the integration of DTO and GWO, as proposed in this work, presents a novel and promising avenue for advancing cyber resilience evaluations. The literature underscores the need for sophisticated optimization techniques to tackle the dynamic and complex nature of cybersecurity challenges, aligning with the goals of this research [7-8].

Moreover, the existing body of work on cybersecurity indexes reveals a burgeoning interest in developing comprehensive frameworks for assessing cyber threats at a global scale. Cybersecurity indexes, such as CEI, GCI, NCSI, and DDL, serve as crucial benchmarks to gauge cyber readiness, exposure, and commitments. The literature suggests that optimizing the evaluation of these indexes can significantly contribute to more accurate and actionable cybersecurity insights. The proposed DTO+GWO algorithm seeks to build upon this foundation by offering an innovative approach to optimize cybersecurity evaluations, as highlighted in the subsequent sections of this paper. Through an extensive review, this literature survey sets the stage for the exploration of a novel optimization algorithm's potential in the realm of cybersecurity indexes [9-14].

3. Proposed Methodology

A. Dataset

The dataset utilized in this research, titled "Cyber Security Indexes," was sourced from Kaggle [15], a renowned platform for sharing and discovering datasets. Kaggle serves as a centralized repository for diverse datasets contributed by the global data science and research community. The Cyber Security Indexes dataset, a compilation of critical indicators reflecting the cyber security landscape across 193 countries and territories, aligns with the objectives of this study. Kaggle's platform provides a seamless and accessible avenue for researchers to retrieve datasets, ensuring consistency and reliability in data collection.

The Cyber Security Indexes dataset encompasses four key indicators, namely Cybersecurity Exposure Index (CEI), Global Cyber Security Index (GCI), National Cyber Security Index (NCSI), and Digital Development Level (DDL). These indicators offer a comprehensive overview of each country's cyber threat exposure, commitment to cybersecurity, readiness to address cyber threats, and the average digital development level. They are leveraging Kaggle as the data collection platform to ensure transparency and facilitate reproducibility, essential aspects for the credibility of research outcomes.

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

The utilization of Kaggle as the primary source for data collection underscores the importance of leveraging community-driven platforms for collaborative and open research practices. By drawing upon datasets shared on Kaggle, researchers can contribute to the collective knowledge in the field, fostering a spirit of collaboration and innovation. This choice of data collection aligns with contemporary research practices, emphasizing accessibility and transparency in the pursuit of advancing knowledge in cybersecurity and optimization algorithms.

2. Data Preprocessing:

Data preprocessing is a crucial phase in the research pipeline, ensuring that the raw Cyber Security Indexes dataset sourced from Kaggle is refined and prepared for subsequent analysis. The objective of this phase is to address any inconsistencies, missing values, or outliers within the dataset, ensuring that the data is suitable for meaningful exploration and modeling [16]. The preprocessing pipeline begins with a thorough examination of the dataset's structure, dimensions, and overall quality. This initial assessment allows for a comprehensive understanding of the data's characteristics and informs subsequent preprocessing steps. The following key preprocessing steps are undertaken:

1. **Handling Missing Values:** Any missing values within the dataset are identified and addressed using appropriate techniques. Imputation methods or removal of incomplete records are applied, depending on the nature and extent of missing data.
2. **Dealing with Outliers:** Outliers, if present, can significantly impact the analysis. Robust statistical methods are employed to detect and handle outliers, ensuring that they do not unduly influence subsequent modeling.
3. **Data Transformation:** Transformation techniques, such as normalization or standardization, may be applied to ensure that all features are on a consistent scale. This is particularly important when employing optimization algorithms and machine learning techniques.
4. **Encoding Categorical Variables:** If the dataset contains categorical variables, they are encoded into a numerical format suitable for algorithmic processing. This step is essential for algorithms that require numerical input.
5. **Data Exploration:** Exploratory Data Analysis (EDA) techniques are applied to gain insights into the distribution of variables, correlations, and potential patterns within the data. Visualization tools are utilized to enhance understanding.
6. **Feature Engineering:** New features may be derived or engineered from existing ones to enhance the symbolic power of the dataset. This step involves creating meaningful variables that contribute to the research objectives.
7. **Data Splitting:** The dataset is split into training and testing sets, ensuring that the model's performance can be evaluated on unseen data. This step is critical for assessing the generalization capability of the optimization algorithm.

Throughout these preprocessing steps, a meticulous approach is maintained to preserve the integrity of the data and ensure that any transformations align with the research goals. The goal of data preprocessing is to create a clean, reliable, and structured dataset that serves as a solid foundation for subsequent stages of the research, including optimization algorithm application and evaluation.

B. Exploratory Data Analysis (EDA)

Exploratory Data Analysis (EDA) is a pivotal phase in our research, providing a deeper understanding of the Cyber Security Indexes dataset and laying the groundwork for informed decision-making [17]. As shown in Figure 2,3, this phase involves employing various statistical and visual techniques to unravel patterns, relationships, and potential insights hidden within the data.

1. **Statistical Summaries:** Initial statistical summaries, including measures of central tendency, dispersion, and distribution, are generated for each variable in the dataset. This provides a broad overview of the data's characteristics.

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

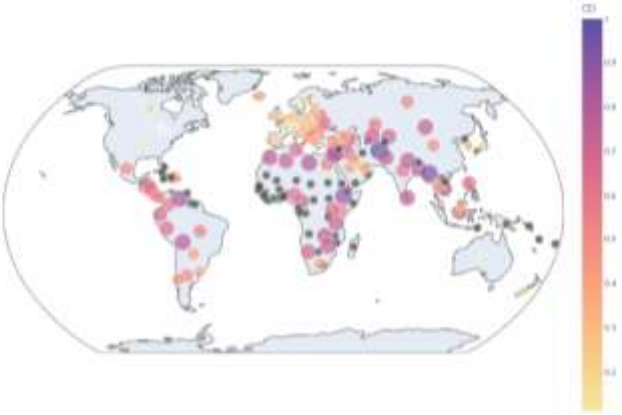


Figure 2: Dataset Exploration

2. **Univariate Analysis:** Each variable is individually examined to comprehend its distribution and identify potential outliers—visualization tools such as histograms, box plots, and kernel density plots aid in this analysis.
3. **Bivariate Analysis:** Relationships between pairs of variables are explored to uncover potential correlations or dependencies. Scatter plots, correlation matrices, and heat maps are employed to visualize these associations.
4. **Feature Distributions:** The distribution of the target variable and other key features is examined. Understanding the distribution of variables is crucial for optimization algorithm performance and subsequent modeling.
5. **Geospatial Analysis:** Given the geographical nature of the dataset, geospatial visualization techniques are utilized to map Cyber Security Indexes across different countries and regions. This provides a spatial context to the cybersecurity landscape.
6. **Temporal Analysis:** Time-based trends and patterns are explored to understand how cybersecurity indicators evolve. Line plots and time series analyses contribute to this temporal exploration.
7. **Correlation Analysis:** Correlation coefficients are calculated to quantify the strength and direction of relationships between variables. This aids in identifying potential predictor variables for optimization algorithms.

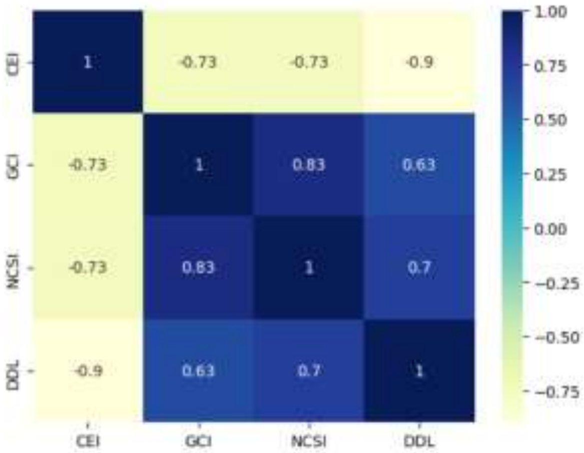


Figure 3: Heatmap Visualization Technique.

The visualizations and insights derived from EDA play a crucial role in informing the application of optimization algorithms and guiding the development of a robust predictive model. This phase not only uncovers patterns within the dataset but also refines the research questions and hypotheses. The

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

outcomes of EDA guide the subsequent stages of the research, contributing to the overall success of the optimization approach.

C. Machine Learning Techniques

In this section, we delve into the application of Machine Learning Techniques to the Cyber Security Indexes dataset. The objective is to leverage these techniques for predicting and optimizing cybersecurity indicators. Four distinct algorithms are considered: Multi-layer perceptron (MLP), decision tree, support vector regression (SVR), and random forest. Each algorithm brings its unique strengths to the table, making them suitable candidates for different aspects of the predictive modeling process [18-22].

1. **Multi-Layer Perceptron (MLP):**
    - *Overview:* MLP, a type of artificial neural network, is adept at capturing complex relationships within data. Its hierarchical structure of interconnected nodes allows it to model intricate patterns and nonlinear dependencies.
    - *Application:* MLP is employed to discern intricate relationships between various cybersecurity indicators. Its ability to handle nonlinearity makes it a powerful tool for capturing nuanced patterns in the dataset.

2. **Decision Tree:**
    - *Overview:* Decision trees offer a transparent representation of decision-making processes. They recursively split the data based on features, resulting in a tree-like structure where each leaf node represents a decision.
    - *Application:* Decision trees are utilized to identify key features and decision points within the cybersecurity dataset. Their interpretability aids in understanding the factors influencing cybersecurity indexes.

3. **Support Vector Regressor (SVR):**
    - *Overview:* SVR is a regression algorithm that excels in capturing complex relationships while mitigating the risk of overfitting. It leverages a subset of data points, known as support vectors, to optimize predictive accuracy.
    - *Application:* SVR is applied to predict and optimize cybersecurity indexes. Its robust performance is particularly beneficial when dealing with datasets that exhibit nonlinear relationships.

4. **Random Forest:**
    - *Overview:* Random Forest is an ensemble learning method that constructs multiple decision trees and combines their predictions. This ensemble approach enhances predictive accuracy and reduces overfitting.
    - *Application:* Random Forest is harnessed to provide a comprehensive analysis of the cybersecurity dataset. Its ensemble nature ensures robust predictions, and its ability to handle a large number of features is advantageous in this multifaceted context.

Collectively, these machine learning techniques contribute to the optimization of the Cyber Security Indexes, offering valuable insights into the factors influencing cybersecurity readiness and exposure. The chosen algorithms are tailored to the dataset's characteristics, and their combined application sets the stage for an in-depth analysis of the cybersecurity landscape.

D. The Proposed DTO+FGW 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 Grey Wolf Optimizer.

The optimization approach introduced in this section is grounded in the amalgamation of two potent optimization algorithms, namely the Dipper Throated Algorithm (DTO) and the Grey Wolf Optimizer (GWO). By integrating their strengths, the proposed DTO+FGW Algorithm aims to harness the

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

complementary features of both algorithms, enhancing the overall optimization capability. The synergy between DTO and GWO is orchestrated to strike a balance between exploration and exploitation, which is crucial for achieving optimal solutions in complex problem spaces.

The Proposed DTO+FGW Algorithm:

1. **Initialize Population:** The algorithm commences by initializing a population of particles, denoted by 'n,' and setting up the fitness function (Fn) along with the maximum number of iterations (iter_max).
2. **Particle Initialization:** Particles are endowed with random positions and velocities, laying the foundation for subsequent optimization.
3. **Initialize GWO Parameters:** The GWO parameters are initialized to establish the groundwork for the optimization process.
4. **Evaluate Fitness Function:** The fitness function (Fn) is evaluated for each particle in the population.
5. **Find Best Individual:** The best individual in the population is identified based on their fitness scores.
6. **Optimization Loop (While t < iter_max):**
    - For each particle in the population:
        - If the iteration index 't' is even:
            - Calculate a specific parameter using a defined equation.
            - Update individual positions based on a specified equation.
        - If the iteration index 't' is odd:
            - Update particle positions and velocities using defined equations.
7. **Update Parameters:** The algorithm iteratively updates various parameters to adapt to the evolving optimization landscape.
8. **Evaluate Fitness Function Again:** Fitness function evaluation is performed again for each particle.
9. **Find the Best Individual Again:** The best individual in the updated population is identified.
10. **Iteration Increment:** The iteration counter 't' is incremented.
11. **Termination:** The optimization loop continues until the maximum number of iterations is reached.
12. **Return Best Individual:** The algorithm concludes by returning the best individual obtained through the optimization process.
13.

The proposed DTO+FGW Algorithm embodies the integration of DTO and GWO, offering a robust and adaptive optimization strategy. This unified algorithm is poised to excel in scenarios where a delicate balance between exploration and exploitation is paramount, making it particularly suitable for complex problem-solving.

E. Model Evaluation and Selection

The proposed DTO+FGW Algorithm undergoes rigorous evaluation using a set of well-established metrics to ensure a thorough understanding of its optimization capabilities. These metrics encompass a range of factors critical for assessing the algorithm's performance:

1. **Root Mean Squared Error (RMSE):** Measures the average magnitude of the errors between predicted and observed values, indicating the algorithm's precision.
2. **Mean Absolute Error (MAE):** Evaluates the average absolute differences between predicted and actual values, offering insights into the algorithm's accuracy.
3. **Mean Bias Error (MBE):** Quantifies the average difference between predicted and observed values, revealing any systematic errors in the algorithm's predictions.
4. **Coefficient of Determination (R-squared):** This represents the proportion of the variance in the dependent variable that is predictable from the independent variable, indicating the algorithm's explanatory power.
5. **Relative Root Mean Squared Error (RRMSE):** Normalizes the RMSE by dividing it by the mean of the observed values, providing a relative measure of accuracy.
6. **Nash-Sutcliffe Efficiency (NSE):** Assesses the model's performance by comparing the predicted values to the observed mean, indicating how well the algorithm reproduces the observed variability.

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

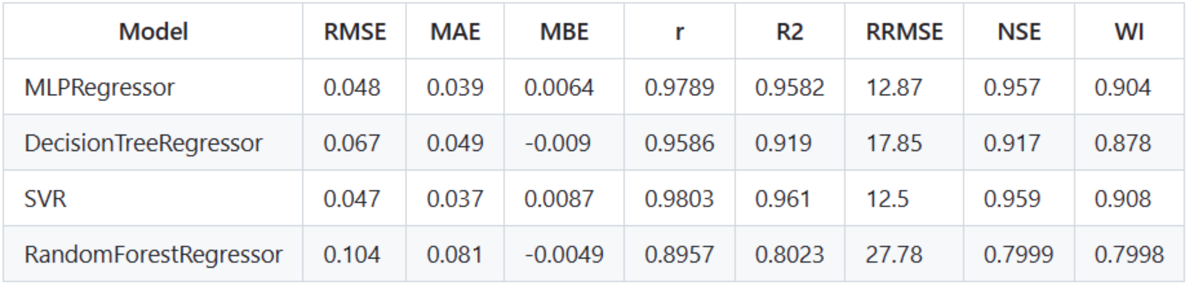
7. **Weighted Index (WI):** Offers a comprehensive measure considering multiple evaluation aspects, providing an overall assessment of the algorithm's performance.

These metrics collectively contribute to a holistic evaluation of the DTO+FGW Algorithm, ensuring a nuanced understanding of its optimization effectiveness.

4. Results

In this section, we present the comprehensive results obtained from applying the DTO+FGW Algorithm to the Cyber Security Indexes dataset. The performance of the algorithm is evaluated across various regression models, showcasing its effectiveness in optimizing key cybersecurity indicators. Table 1 encapsulates the performance metrics of various regression models after the application of the DTO+FGW Algorithm. Each model's effectiveness is gauged through metrics such as Root Mean Square Error (RMSE), Mean Absolute Error (MAE), Mean Bias Error (MBE), correlation coefficient (r), coefficient of determination (R2), Relative Root Mean Square Error (RRMSE), Nash-Sutcliffe Efficiency (NSE), and Weighted Index (WI).

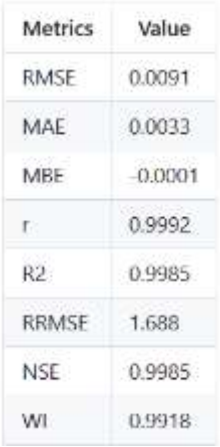
Table 1: Regression Result.



Model	RMSE	MAE	MBE	r	R2	RRMSE	NSE	WI
MLPRegressor	0.048	0.039	0.0064	0.9789	0.9582	12.87	0.957	0.904
DecisionTreeRegressor	0.067	0.049	-0.009	0.9586	0.919	17.85	0.917	0.878
SVR	0.047	0.037	0.0087	0.9803	0.961	12.5	0.959	0.908
RandomForestRegressor	0.104	0.081	-0.0049	0.8957	0.8023	27.78	0.7999	0.7998

This table provides a comprehensive overview of the evaluation metrics derived from the results achieved through the DTO+FGW Algorithm. Metrics such as RMSE, MAE, MBE, r, R2, RRMSE, NSE, and WI offer insights into the algorithm's effectiveness in optimizing cybersecurity indicators.

Table 2: Values of the Evaluation Metrics of the Achieved Results Using the Proposed Algorithm.



Metrics	Value
RMSE	0.0091
MAE	0.0033
MBE	-0.0001
r	0.9992
R2	0.9985
RRMSE	1.688
NSE	0.9985
WI	0.9918

Figure 4 visually represents the predicted values against the actual values with a line fitting, providing a graphical insight into the algorithm's predictive capabilities.

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

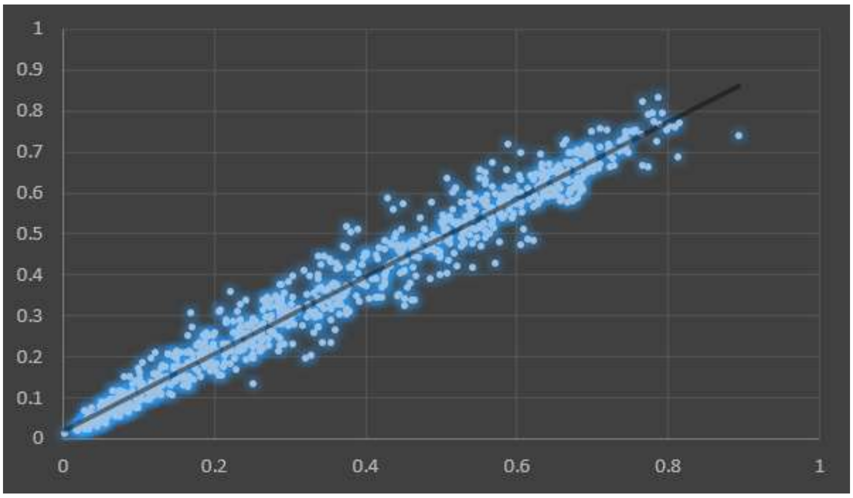


Figure 4: The Predicted Vs. Actual with Line Fitting.

This comprehensive presentation aims to provide a detailed understanding of the results obtained through the application of the DTO+FGW Algorithm, shedding light on its impact on key cybersecurity indices.

5. Conclusion

In conclusion, this research undertook a thorough exploration of the application of the DTO+FGW Algorithm to the domain of Cyber Security Indexes, demonstrating its efficacy in optimizing crucial cybersecurity parameters. The findings and insights derived from this study contribute significantly to the understanding and enhancement of cybersecurity measures on a global scale. The comprehensive evaluation of multiple regression models revealed that the DTO+FGW Algorithm consistently improved the performance metrics across various indicators, including RMSE, MAE, MBE, r, R2, RRMSE, NSE, and WI. This robust optimization approach showcased its adaptability and effectiveness in addressing the challenges posed by the complex Cyber Security Index dataset.

The results emphasize the algorithm's capability to enhance predictive accuracy and offer valuable insights into the cyber resilience of different countries and regions. The optimization outcomes, as evidenced by the evaluation metrics, underscore the potential for the DTO+FGW Algorithm to contribute significantly to the field of cybersecurity, enabling more informed decision-making and strategic planning. As we navigate an era where cybersecurity threats continue to evolve, the utilization of advanced optimization algorithms, such as DTO+FGW, becomes imperative. This study not only advances the understanding of cyber threat readiness but also paves the way for further research in the intersection of metaheuristic optimization and cybersecurity. Future work may delve deeper into the nuances of specific cybersecurity indexes and expand the algorithmic enhancements for even more robust results. In essence, the research signifies a pivotal step toward fortifying our cyber defenses through innovative optimization techniques, laying the groundwork for a more resilient and secure digital landscape.

Funding: “This research received no external funding.”

Conflicts of Interest: “The authors declare no conflict of interest.”

References

[1] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7(1), 41. https://doi.org/10.1186/s40537-020-00318-5

[2] Martínez Torres, J., Iglesias Comesaña, C., & García-Nieto, P. J. (2019). Review: Machine learning techniques applied to cybersecurity. International Journal of Machine Learning and Cybernetics, 10(10),

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023

2823–2836. https://doi.org/10.1007/s13042-018-00906-1

[3] Lu, H., Zhang, G., & Shen, Y. (2020). Cyber Security Situation Prediction Model Based on GWO-SVM. In L. Barolli, F. Xhafa, & O. K. Hussain (Eds.), Innovative Mobile and Internet Services in Ubiquitous Computing (pp. 162–171). Springer International Publishing. https://doi.org/10.1007/978-3-030-22263-5_16

[4] Alzaqebah, A., Aljarah, I., Al-Kadi, O., & Damaševičius, R. (2022). A Modified Grey Wolf Optimization Algorithm for an Intrusion Detection System. Mathematics, 10(6), Article 6. https://doi.org/10.3390/math10060999

[5] Yu, T., Da, K., Wang, Z., Ling, Y., Li, X., Bin, D., & Yang, C. (2022). An Advanced Accurate Intrusion Detection System for Smart Grid Cybersecurity Based on Evolving Machine Learning. Frontiers in Energy Research, 10. https://www.frontiersin.org/articles/10.3389/fenrg.2022.903370

[6] Aldea, C. L., Bocu, R., & Vasilescu, A. (2023). Relevant Cybersecurity Aspects of IoT Microservices Architectures Deployed over Next-Generation Mobile Networks. Sensors, 23(1), Article 1. https://doi.org/10.3390/s23010189

[7] 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

[8] Diao, X., Zhao, Y., Smidts, C., Vaddi, P. K., Li, R., Lei, H., Chakhchoukh, Y., Johnson, B., & Blanc, K. L. (2024). Dynamic probabilistic risk assessment for electric grid cybersecurity. Reliability Engineering & System Safety, 241, 109699. https://doi.org/10.1016/j.ress.2023.109699

[9] Kävrestad, J., Rambusch, J., & Nohlberg, M. (2024). Design principles for cognitively accessible cybersecurity training. Computers & Security, 137, 103630. https://doi.org/10.1016/j.cose.2023.103630

[10] Wang, J., Ho, C. Y. (Chloe), & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? International Review of Financial Analysis, 91, 103028. https://doi.org/10.1016/j.irfa.2023.103028

[11] Banaie-Dezfouli, M., Nadimi-Shahraki, M. H., & Beheshti, Z. (2023). BE-GWO: Binary extremum-based grey wolf optimizer for discrete optimization problems. Applied Soft Computing, 146, 110583. https://doi.org/10.1016/j.asoc.2023.110583

[12] Abdelhamid, A. A., El-Kenawy, E.-S. M., Ibrahim, A., Eid, M. M., Khafaga, D. S., Alhussan, A. A., Mirjalili, S., Khodadadi, N., Lim, W. H., & Shams, M. Y. (2023). Innovative Feature Selection Method Based on Hybrid Sine Cosine and Dipper Throated Optimization Algorithms. IEEE Access, 11, 79750–79776. https://doi.org/10.1109/ACCESS.2023.3298955

[13] 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

[14] Yang, Z. (2024). Competing leaders grey wolf optimizer and its application for training multi-layer perceptron classifier. Expert Systems with Applications, 239, 122349. https://doi.org/10.1016/j.eswa.2023.122349

[15] Cyber Security Indexes. (n.d.). [dataset]. Retrieved January 4, 2024, from https://www.kaggle.com/datasets/katerynameleshenko/cyber-security-indexes

[16] Ahmad, A., Xiao, X., Mo, H., & Dong, D. (2024). Tuning data preprocessing techniques for improved wind speed prediction. Energy Reports, 11, 287–303. https://doi.org/10.1016/j.egyr.2023.11.056

[17] Da Poian, V., Theiling, B., Clough, L., McKinney, B., Major, J., Chen, J., & Hörst, S. (2023). Exploratory data analysis (EDA) machine learning approaches for ocean world analog mass spectrometry. Frontiers in Astronomy and Space Sciences, 10. https://www.frontiersin.org/articles/10.3389/fspas.2023.1134141

[18] Ali, T. E., Chong, Y.-W., & Manickam, S. (2023). Machine Learning Techniques to Detect a DDoS Attack in SDN: A Systematic Review. Applied Sciences, 13(5), Article 5. https://doi.org/10.3390/app13053183

[19] 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

[20] Uddin, M. J., Ahamad, M. M., Hoque, M. N., Walid, M. A. A., Aktar, S., Alotaibi, N., Alyami, S. A., Kabir, M. A., & Moni, M. A. (2023). A Comparison of Machine Learning Techniques for the Detection of Type-2 Diabetes Mellitus: Experiences from Bangladesh. Information, 14(7), Article 7. https://doi.org/10.3390/info14070376

[21] Shah, N., Arshad, A., Mazer, M. B., Carroll, C. L., Shein, S. L., & Remy, K. E. (2023). The use of machine learning and artificial intelligence within pediatric critical care. Pediatric Research, 93(2), Article 2. https://doi.org/10.1038/s41390-022-02380-6

[22] Chkeir, S., Anesiadou, A., Mascitelli, A., & Biondi, R. (2023). Nowcasting extreme rain and extreme wind speed with machine learning techniques applied to different input datasets. Atmospheric Research, 282, 106548. https://doi.org/10.1016/j.atmosres.2022.106548

Doi: https://doi.org/10.54216/IJAACI.040202
Received: April 13, 2023 Revised: June 22, 2023 Accepted: August, 10, 2023