Date of publication SEP-30, 2025, date of current version JUN-17, 2025.
www.computingonline.net / computing@computingonline.net

Print ISSN 1727-6209
Online ISSN 2312-5381
DOI 10.47839/ijc.24.3.XXXX

A Metaheuristic Machine Learning Approach for Darknet Traffic Classification

AHMED HASSAN HASSAN
Faculty of Information Technology, Department of Cybersecurity, Middle East University, Amman, Jordan

Corresponding author Ahmed Hassan Hassan (e-mail: a.hassan@meu.edu.jo).

ABSTRACT The expansion of darknet traffic categorization necessitates recognizing and resolving its intricate nature. Conventional categorization methods often prove inadequate when confronted with the complexities inherent in darknet network data. This study presents a novel methodology that combines Recurrent Neural Networks (RNNs) with the Harris Hawks Optimization (HHO) method. This research thoroughly evaluated the classifier to enhance classification accuracy and address the prevailing classier in darknet datasets. The study results indicate that incorporating HHO led to a significant increase in precision, with a spike of 99.90%. Additionally, the recall metric showed notable improvement, reaching a value of 0.9998. Moreover, the balanced accuracy measure also shows a substantial enhancement. The usefulness of the combination of Recurrent Neural Networks (RNN) and Hybrid Harmony Optimization (HHO) is shown by this significant advancement. This innovation offers a possible answer to the issue of categorizing darknet data.

KEYWORDS Darknet Traffic Classification; Deep Learning; Recurrent Neural Networks (RNNs); Harris Hawks Optimization (HHO); Feature Selection; Classification Accuracy.

I. INTRODUCTION

In the current era of digital technology, the internet encompasses a wide range of visible and concealed domains. The surface web, often used for routine activities and accessible via conventional search engines, is just a fraction of the vast expanse of the internet. A substantial section of this digital realm, known as the Darknet, resides in obscurity [2]. The ability to effectively traverse, comprehend, and categorize the data flow inside this obscured domain assumes great significance for many purposes, including cybersecurity and law enforcement [4].

The Darknet, known for its anonymous nature and concealed services, poses several problems for anybody seeking to categorize and comprehend its network activity [22]. Conventional approaches often prove inadequate due to the encrypted and dynamic characteristics of Darknet traffic, which pose challenges to standard classification methodologies [11]. Hence, a persistent need exists to develop more sophisticated and flexible methodologies to analyze and categorize the data traffic traversing this obscured segment of the internet [5].

Deep Learning, a branch of machine learning, can extract complex patterns and representations from extensive datasets [17, 36, 28, 10, 27, 25]. Artificial neural networks, intense neural networks, have played a crucial role in several domains, including but not limited to image and audio recognition, natural language processing, and other applications [13]. The capacity of machine learning to acquire knowledge from unprocessed data without the need for explicit feature engineering has brought about significant transformations in several fields [26].

The Harris Hawks Optimization (HHO) algorithm is a contemporary meta-heuristic optimization approach that draws inspiration from the predatory behavior shown by Harris Hawks in natural settings [39, 7]. The HHO algorithm has shown remarkable efficacy in addressing intricate optimization issues by imitating the strategic hunting behavior exhibited by these avian species. This algorithm effectively achieves a harmonious equilibrium between exploration and exploitation within the search space, as evidenced by the findings of Chen et al. [8] and Kang et al. [18].

The complex interaction of Darknet Traffic Classification, Deep Learning, and Harris Hawks Optimization showcases a synergistic relationship, including identifying, understanding, and improving processes. The fundamental essence of Darknet Traffic Classification revolves around comprehending and classifying the intricate and diverse data streams that traverse the concealed pathways of the internet [23]. In the face of complexity, standard approaches may encounter difficulties. However, Deep Learning is a promising solution, with the cognitive ability to identify and acquire knowledge from intricate patterns concealed within this traffic [30]. The neural

networks used in this study undertake a comprehensive analysis, systematically examining several layers of data to extract significant patterns that may be utilized to categorize the elusive traffic inside the Darknet [15].

However, similar to any complex system, these deep learning models' effectiveness and precision depend on their parameters' correctness. The Harris Hawks Optimization (HHO) algorithm demonstrates strategic and adaptive behavior characteristics, drawing inspiration from the bird species named after [9]. The optimization of the deep learning model's parameters using the HHO technique guarantees the maximization of the model's potential, hence significantly improving its classification accuracy to an unprecedented level. The integration of the three domains, namely classification, deep learning, and optimization, forms a synergistic triangle that enables the development of a robust and effective approach for unraveling the enigmatic aspects of the Darknet [1].

Schizas et al. [33] offer a novel methodology that combines Deep Learning with Harris Hawks Optimization to classify Darknet traffic. This approach seeks to address the classification issues presented by the Darknet by integrating the pattern recognition skills of deep learning models with the adaptive optimization capabilities of the HHO algorithm [29, 19]. The collaboration between these elements is anticipated to augment the precision and effectiveness of Darknet traffic categorization, expanding the limits of present approaches [14].

The objective of this research is to explore the possibilities of combining Deep Learning with Harris Hawks Optimization for the task of classifying Darknet traffic. The main aim of our study is to develop and assess a new methodology that can accurately and efficiently categorize Darknet network data. By undertaking this endeavor, we provide a scholarly contribution by presenting an innovative approach that leverages the advantages of deep learning and meta-heuristic optimization, perhaps establishing a new standard in the field of Darknet traffic categorization.

II. RELATED WORKS

The field of darknet traffic categorization has been more pertinent in contemporary study, owing to the growing importance of cyberspace in the modern digital era. The Darknet, known for its extensive anonymity and encryption features, functions as a central point for a range of nefarious operations, underscoring the need to accurately categorize its traffic in the field of cybersecurity [12, 62].

Deep learning, which falls under the umbrella of machine learning, has considerable potential as a viable technique for categorizing Darknet network traffic. An example of this may be seen in the work of Selim et al. [34], who proposed a new methodology that combined deep learning techniques with an enhanced iteration of the Harris Hawks Optimization (HHO) algorithm, referred to as the Improved Harris Hawks Optimization (IHHO). The researchers used a deep learning approach to extract important characteristics from network traffic data effectively. Subsequently, they enhanced the classification process by using the IHHO method for optimization.

Sarwar and colleagues [31] introduced novel variations of deep learning approaches, namely the modified Convolution-Long Short-Term Memory (CNN-LSTM) and Convolution-Gradient Recurrent Unit (CNN-GRU). Using this methodology, the researchers got notable levels of accuracy, namely 96% for identifying darknet traffic and 89% for classifying traffic. In order to improve the effectiveness of their model, the researchers used XGBoost (XGB) for feature selection.

The deep-full-range (DFR) framework, proposed by Zeng et al. [38], utilizes deep learning models such as CNN, LSTM, and SAE to perform encrypted traffic categorization and intrusion detection. The methodology used by the researchers showcased the capacity of deep learning algorithms to analyze unprocessed traffic data autonomously, eliminating the need for human interaction. Optimization algorithms have been investigated as a viable approach to improve the categorization of darknet traffic. In their study, Liu et al. [20] combined the Harris Hawk optimization technique with a clustering algorithm to enhance the classification process's accuracy and recall rate.

Optimization methods have also been investigated as prospective approaches to augment the categorization of darknet traffic. In their study, Liu et al. [20] used the Harris Hawk optimization technique with a clustering algorithm to enhance the clustering accuracy and the recall rate in the classification procedure. Additional Approaches and Considerations: In their study, Chang et al. [6] explored deep learning models for categorizing online and offline traffic in a software-defined network (SDN) setting, focusing on application-based classification. The authors assessed their models, which consisted of a multilayer perceptron (MLP), a convolutional neural network (CNN), and a Stacked Auto-Encoder (SAE), using an openly available dataset on network traffic.

Mazel et al. [21] used unsupervised anomaly detection methods, such as clustering and correlation analysis, within the domain of anomaly detection to discover irregularities in Darknet traffic. In addition, Niranjana et al. [23] have put out a comprehensive 29-tuple Numerical AGM data format that is well-suited for analyzing TCP connections with verified source IP addresses. This format seems to be effective in identifying attack patterns inside darknet traffic. The study field has seen the introduction of several strategies aimed at improving the efficiency of darknet traffic classification models in response to the difficulties presented by encrypted traffic and the complexities of darknet operations.

The analysis of Table 1 reveals that a diverse range of methodologies has been used to classify darknet traffic. Selim et al. [34] and Liu et al. [20] emphasized optimization techniques in their studies. Selim et al. [34] specifically included deep learning methods in their research, while Liu et al. [20] concentrated on clustering techniques. Khan et al. [32] and Zeng et al. [38] extensively used deep learning models using customized architectures for traffic detection and categorization. In contrast, Chang et al. [6] and Mazel et al. [21] directed their attention to distinct categories of network traffic. Specifically, the former concentrated on unencrypted traffic, while the latter focused on anomaly detection. Niranjana et al. [23] presented a distinct viewpoint by emphasizing the significance of data formats in the analysis context. Furthermore, recent studies have highlighted additional methods that integrate deep learning and optimization techniques.

Table 1. Comparative Analysis of Darknet Traffic Classification Techniques.

Reference	Approach/Technique	Key Contributions	Limitations/Challenges
Selim et al. (2020)	Deep Learning + IHHO	Integration of deep learning with IHHO; Superior classification accuracy	Restricted to specific darknet traffic patterns
Sarwar et al. (2021)	CNN-LSTM and CNN-GRU	96% accuracy for traffic detection; Use of XGB for feature selection	Model complexity; Computational overhead
Zeng et al. (2019)	DFR Framework (CNN, LSTM, SAE)	Effective encrypted traffic classification; Manual intervention not needed	Limited to public datasets used in the study
Liu et al. (2022)	Harris Hawk optimization + Clustering	Enhanced clustering accuracy and recall rate; Emphasized class compactness and separation	Specific to data traffic patterns studied
Chang et al. (2020)	Application-based classification on SDN	Effective unencrypted traffic classification; Evaluated using open network traffic dataset	Only applied to unencrypted traffic
Mazel et al. (2015)	Unsupervised anomaly detection	Successful anomaly detection in Darknet traffic; Clustering and correlation analysis used	Reliant on specific anomaly detection techniques
Niranjana et al. (2020)	29-tuple Numerical AGM data format	Detection of various attack trends using the Mean Shift clustering algorithm	Limited to TCP connections and specific attack patterns

In contrast to the findings shown in the table, our study provides a unique approach that combines Deep Learning with Harris Hawks Optimization. This approach is designed to classify various sorts of darknet traffic completely. Our method aims to address the deficiencies found in previous studies by providing a more comprehensive solution capable of adapting to darknet traffic's dynamic and encrypted characteristics, distinguishing it from other approaches.

The existing body of literature has substantially contributed to advancing darknet traffic categorization. However, it is essential to note that some areas have not been well addressed. The total resolution of the difficulty presented by the ever-changing nature of the Darknet and the scarcity of labeled data for deep learning models remains incomplete. Furthermore, while the current methodologies have shown efficacy in some situations, achieving a comprehensive solution that provides high precision for many forms of darknet data, including encrypted communication, continues to be challenging. Furthermore, doing a comprehensive analysis of hybrid models that integrate the advantageous aspects of several methodologies might augment categorization's precision and effectiveness.

III. METHODOLOGIES

This study explores the Harris Hawks Optimization (HHO) method to select features to be inputted into a deep learning classifier known as the Recurrent Neural Network (RNN). This article provides an overview of the dataset used, the construction and training of the recurrent neural network (RNN), and the incorporating of the harmony search algorithm (HHO) principles into the feature selection process.

A. DATASET DESCRIPTION

The importance of the quality and comprehensiveness of the utilized dataset cannot be overstated while endeavoring to gain valuable insights and construct an effective classification model for darknet traffic. The researchers chose the CIC-Darknet2020 dataset [40] due to its extensive coverage of darknet traffic patterns, making it a suitable foundation for their analyses. The dataset was aggregated from a diverse range of subterranean databases. The intentional diversification of data sources contributes to the comprehensive representation of various darknet traffic categories, mitigating potential biases associated with relying solely on a limited number of sources. The collection exhibits a significant characteristic in the form of a substantial quantity of available qualities. The system comprehensively examines every instance of traffic and showcases a wide range of 85 distinct characteristics. From the standpoint of network traffic analysis, it is worth highlighting several particularly significant characteristics:

- **Flow ID**: As a unique identifier, the Flow ID ensures that each traffic flow can be distinctly recognized and analyzed.
- **Src IP and Dst IP**: These attributes capture the source and destination IP addresses, respectively, offering insights into the origins and targets of the traffic.
- **Src Port and Dst Port**: By recording the source and destination port numbers, these features shed light on the specific communication channels employed.
- **Protocol**: This feature classifies the type of protocol used, such as TCP, UDP, etc.
- **Timestamp**: By noting the exact timestamp of the traffic capture, this feature allows for temporal analysis, which is crucial for discerning patterns over time.
- Additionally, the dataset encompasses various statistical attributes related to flow duration, packet counts, and other intricate details, thereby enriching the depth of information available.

The CIC-Darknet2020 dataset is characterized by its substantial size, comprising 17,109 documents. With this quantity of data, training and evaluating our deep-learning models with high confidence is feasible. The distribution of classes within the sample is intriguing. There is a discernible inclination towards exclusively focusing on two specific categories of dark web activities. The category labeled 'Browsing' exhibits a significantly higher frequency with 16,783 instances, starkly contrasting to the 'Audio-Streaming' category, which only comprises a meager 326 occurrences. The observed imbalance in question reflects the real-world distribution of darknet traffic, presenting an intriguing issue in categorization.

B. PREPROCESSING

The preprocessing stage is critical in ensuring the dependability and effectiveness of the subsequent classification process, primarily because of the inherent challenges associated with darknet traffic data [62-64]. This section provides a comprehensive overview of the preprocessing procedures employed for this dataset. During the initial round of data cleansing, inconsistencies and missing values are detected. In order to maintain the integrity of the dataset, instances with incomplete or inaccurate values for essential attributes are

either imputed using suitable statistical techniques or removed from the dataset. The field of mechanical design encompasses the creation and development of mechanical systems and components. It involves the use of engineering principles and techniques. There is a potential that certain features, particularly those with high cardinality, such as Flow ID or Timestamp, may not contribute significantly to the classification task. To enhance the significance of representations, it is possible to modify or analyze these qualities [41]. Temporal data, such as the specific hour or day of the week, holds importance in examining dark web activity. This data can be obtained by parsing the Timestamp. The dataset contains numerical parameters such as Flow Duration and Total Forward Packet, which exhibit a range of potential values. The numeric properties are commonly standardized through the utilization of Min-Max scaling or Z-score normalization Bachmann et al., [42] in order to ensure that no one feature exerts a disproportionately large influence on the deep learning model. One-hot encoding is a technique employed to convert categorical features, such as the Protocol variable, into a binary matrix format that is suitable for utilization by a neural network. A cursory examination of the data reveals a notable disparity between the 'Browsing' and 'Audio-Streaming' categories, necessitating the resolution of class imbalance. Synthetic Minority Oversampling Technique (SMOTE) is a widely used algorithm in machine learning. Two techniques, namely the Synthetic Minority Over-sampling Technique (SMOTE) and adaptive synthetic sampling (ADASYN), can address the class imbalance issue. This hinders the Recurrent Neural Network (RNN) from cultivating an overwhelming bias towards the predominant class.

C. RECURRENT NEURAL NETWORK (RNN) CLASSIFIER

Recurrent Neural Networks (RNNs) have gained significant popularity as a preferred option for analyzing and manipulating sequential data within deep learning. Recurrent Neural Networks (RNNs) are considered a viable option for classifying darknet traffic due to the inherent temporal nature of network traffic. This is because the behavior of packets and flows often relies on past activity, as highlighted by Ahmed et al. [43].

C.1. ARCHITECTURE

The input layer, as depicted in Figure 1, is the initial layer of a neural network model. The recurrent neural network (RNN) utilizes the pre-processed features of the dataset. According to Jaafari et al. [44], the quantity of neurons in the input layer directly relates to the dimensional aspect of the dataset following preprocessing. The architecture consists of several concealed layers, each incorporating recurrent connections. These layers can retain information from preceding time steps, making them highly effective in identifying patterns in sequential data. The determination of the optimal number of hidden layers and neurons inside each layer is informed by empirical evaluations, which aim to find an equilibrium between the complexity of the model and its performance [45]. Dropout layers are employed in darknet traffic to mitigate the risk of overfitting due to the intricate nature of such communication. These dropout layers are strategically interspersed between recurrent levels. This approach enhances the model's resilience by automatically deactivating certain neurons during training. Ultimately, the output layer employs a softmax activation function to generate a probabilistic distribution including the two potential categories of traffic, namely "Browsing" and "Audio-Streaming."

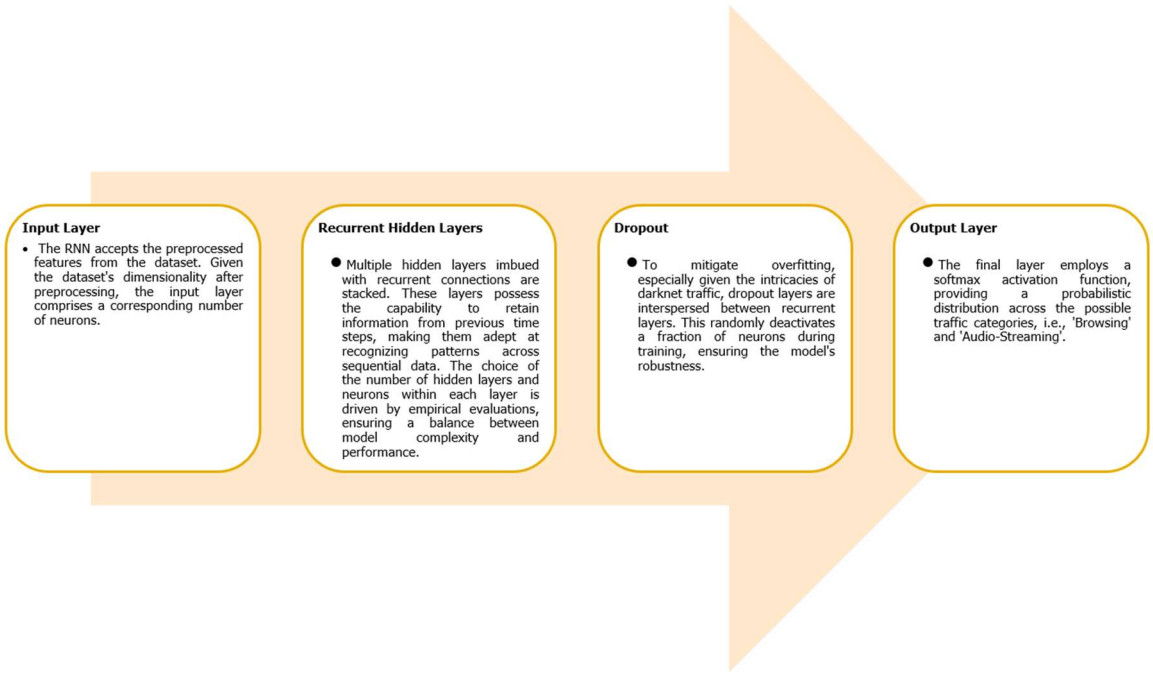

Figure 1. Recurrent Neural Network (RNN) Architecture.

C.2. TRAINING

Considering the nature of the task at hand, wherein a classification problem is being addressed, the loss function employed is the categorical cross-entropy. This particular loss function quantifies how much the predictions deviate from the actual class labels [50]. In order to iteratively adjust the parameters of the model, optimization algorithms such as Adam or RMSprop are employed in conjunction with the backpropagation through time (BPTT) method, which has been designed explicitly for recurrent neural networks [53]. The

timing and batch size factors are essential considerations in several academic contexts. During the training process, providing the Recurrent Neural Network (RNN) with data in batches is necessary. The objective is to achieve convergence without overfitting by doing exploratory experiments to determine the ideal batch size and number of epochs, which refer to complete iterations over the training dataset. Part of the training data is partitioned and designated as a validation set. This feature enables the implementation of early halting or model checkpoints by consistently evaluating the model's performance on unseen data during the training process.

C.3. REGULARIZATION AND HYPERPARAMETERS

The model's generalization abilities can be enhanced by implementing regularization techniques that impose penalties on large weights, such as L1 and L2 regularization [5], among others. The tuning process refers to adjusting or modifying a system or device to Hyperparameters encompassing various factors within the architecture and training process, including but not limited to the learning rate, dropout rate, and number of hidden neurons. In order to determine the optimal values for the hyperparameters, scholars typically conduct a methodical exploration that may involve using grid search or random search techniques Balaha & Hassan, [54] to refine the potential options.

C.4. HARRIS HAWKS OPTIMIZATION (HHO) FOR FEATURE SELECTION

In the context of datasets with a high number of dimensions, the process of feature selection assumes a critical role in enhancing the efficacy of machine learning models. The Harris Hawks Optimization (HHO) method presents a novel meta-heuristic approach that addresses the issue at hand by prioritizing improving classification accuracy and reducing computing cost, drawing inspiration from the predatory behavior of Harris Hawks.

C.4.1. BASIC PRINCIPLE OF HHO

The HHO algorithm is a computational model that emulates the cooperative hunting behavior observed in Harris hawks. Each hawk within this context represents a potential solution (or a combination of characteristics), and its placement inside the search region denotes the level of excellence associated with those characteristics. During the iterative optimization process, hawks undergo many phases corresponding to their hunting habits, including the surprise pounce, mild besiege, and powerful besiege. These actions facilitate investigating further potential options (exploration) and maximizing the previously identified (exploitation) inside the designated search region.

C.4.2. HHO IMPLEMENTATION FOR FEATURE SELECTION

The initial step involves randomly assigning a population of potential solutions (feature subsets). Fitness functions are employed to evaluate the performance of each subset, with classification accuracy being a prevalent statistic for recurrent neural networks (RNNs) [47, 46]. The feature subsets, called hawks, undergo iterative updates to navigate toward optimal solutions through exploration and exploitation. This necessitates a combination of undirected exploration [48, 49] to discover novel combinations of features, as well as directed exploration [48] aimed at known optimal solutions. The convergence criterion encompasses several factors, such as a predetermined maximum number of iterations or a threshold improvement in fitness, that are deemed necessary to the problem being addressed. The hawk that exhibits the highest level of performance at convergence demonstrates the optimal selection of features. The RNN classifier that remains is trained using the subset above.

C.4.3. BENEFITS OF HHO IN FEATURE SELECTION

In order to mitigate the risk of being trapped in local optima, the exploration and exploitation techniques employed by HHO provide an extensive investigation of the feature space. HHO has the potential to effectively decrease the dimensionality of a dataset by selectively retaining the most informative features. This can result in expedited training times and potentially improved model performance. Enhanced Generalization By removing unnecessary details, the classifier reduces the risk of overfitting the training data, resulting in an improved ability to apply learned patterns to fresh data. The utilization of the HHO algorithm in the selection of features for the categorization of dark web traffic has been demonstrated in previous studies [51,52], showcasing the effective amalgamation of nature-inspired optimization techniques and deep learning methodologies.

C.5. EVALUATION METRICS

The efficacy of the proposed recurrent neural network (RNN) classifier is assessed through a comprehensive set of metrics, both prior to and after the application of the Harris Hawks Optimization (HHO) technique for feature selection. Including multiple factors pertaining to the quality of categorization enables these metrics to offer a comprehensive evaluation of the model's effectiveness [55].

The accuracy metric quantifies the proportion of positive observations that are correctly identified, indicating that out of every 100 anticipated positive observations, 90 are accurately classified as valid. When errors have significant repercussions, the paramount consideration is attaining precision [56].

$$Precision = \frac{True\ Positive}{(True\ Positive + Fal\quad Positive)}.$$

The recall (or sensitivity) metric quantifies the accuracy of genuine optimistic predictions relative to the overall number of true positives. In circumstances where the lack of a positive category can yield significant consequences, this factor becomes of utmost importance [57].

$$Recall = \frac{True\ Positive}{(True\ Positive\ + False\ Negative)}.$$

Precision is a metric that quantifies the proportion of correctly anticipated observations to the overall number of observations. Although this indicator encompasses a wide range of data, it can be misleading when used in groups with varying levels of inequality [58].

$$Accuarcy = \frac{(True\ Positive\ + True\ Negative\ )}{(Total\ Observation)}.$$

The significance of balanced accuracy is particularly notable due to the dataset's observed class imbalance.

According to Cittadini et al. (2023), the metric under consideration offers a balanced assessment of the classifier's overall effectiveness by taking into account both its sensitivity (the ratio of true positives) and specificity (the ratio of false negatives) across all classes. The F1 Score is a metric that provides a fair evaluation of accuracy by considering both Precision and Recall. The comparative cost of false positives and negatives is a crucial aspect in which its superiority becomes evident [59].

$$F1\ Score = 2 \times \frac{Precision \times Recall}{Precision + Recall}.$$

Similar to how the F1 Score places greater emphasis on memory than precision, the F2 Score follows a similar approach. When the monetary value associated with false negatives surpasses the monetary value associated with false positives, this factor has significant importance [33].

$$F2\ Score = (1 + 2^2) \times \frac{Precision \times Recall}{(2^2 \times Precision) + Recall}.$$

In conjunction with these quantitative metrics, the confusion matrix presents a structured representation of the classifier's precision, encompassing the proportions of accurate and inaccurate classifications. Several of the measures above are dependent on this matrix as their foundation. The extensive set of evaluation metrics can be employed to evaluate the performance of the recurrent neural network (RNN) classifier both prior to and after the integration of the feature selection technique based on the Harris hawks optimization algorithm (HHO) [60].

C.6 STUDY MODEL

The comprehensive approach to unraveling the intricacies of darknet traffic classification is situated at the convergence of state-of-the-art machine learning techniques and advanced optimization strategies. This study presents a visual representation that succinctly captures the intricate processes and strategic decisions that form the foundation of our approach. The flowchart illustrates the research method and highlights the utilization of a Recurrent Neural Network (RNN) as a prominent deep learning classifier. The RNN integrates with the Harris Hawks Optimization (HHO) technique for feature selection. The utilization of a dual-pronged approach, specifically designed to cater to darknet traffic, underscores the convergence of cutting-edge technology with algorithms that draw inspiration from natural phenomena. Subsequently, a comprehensive exposition will be provided about the dataset, the preprocessing procedures, the recurrent neural network (RNN) architecture, the harmony search algorithm (HHO) implementation, and the metrics employed to assess its effectiveness. The provided visual narrative serves as a contextual framework for a more intricate examination of our research expedition, as seen in Figure 2. It sheds light on the various measures we undertook to enhance the precision, effectiveness, and comprehensiveness of our study of darknet traffic.

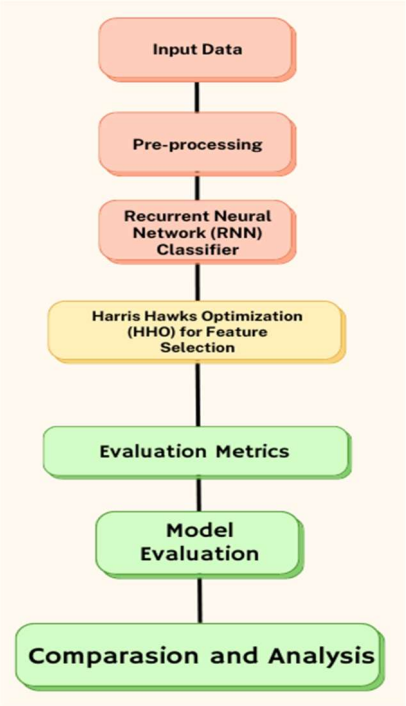

Figure 2. Study Flowchart.

IV. EXPERIMENTS AND RESULTS

A series of comprehensive tests were conducted to assess the efficacy of the proposed Recurrent Neural Network (RNN) classifier in the context of darknet traffic classification. In this section, a comparative analysis is conducted on the outcomes achieved before and after the implementation of HHO, focusing on specific elements.

A.1 RESULTS WITHOUT HHO IMPLEMENTATION

Prior to the implementation of the HHO approach, the efficiency of the RNN classifier was assessed in order to establish expectations. This can serve as a reference point for subsequent comparisons following the implementation of HHO.

A.1.1 CONFUSION MATRIX

The confusion matrix offers a detailed examination of the classifier's precision by segregating the proportions of accurate and inaccurate classifications into separate columns. The classifier's performance was rigorously assessed using a set of assessment metrics, as depicted in Figure 3. The accuracy score of 0.9941 showcased the classifier's impressive ability to anticipate positive outcomes accurately. This value indicates that nearly 99.41% of the instances labeled as positive were indeed positive. The recall statistic achieved an impressive value of 0.9996, suggesting that the classifier successfully identified almost 99.96% of the actual positive occurrences. The classifier's performance was assessed based on its accuracy score 0.9938, which signifies that 99.38% of the predictions made were correct.

The total accuracy of the study increased to 0.7057 when findings from all categories were considered. The dataset exhibits an intrinsic disparity in class distribution, emphasizing the potential for enhancements despite the statistic indicating a mere 70.57 percent. An F1 score of 0.9969 was obtained, indicating a balanced performance in precision and recall, as reflected by the harmonic mean. The study concluded by

reporting an F2 score of 0.9985, indicating the classifier's effectiveness in mitigating false negatives. The results above, acquired prior to implementing the HHO technique, establish the foundational basis by providing a broad understanding of the possibilities of the RNN classifier. In the subsequent paragraphs, we will go deeper into the topic, examining any potential enhancements in efficiency that can be ascribed to the utilization of HHO. Insights into the capabilities of the Recurrent Neural Network (RNN) classifier can be derived from the results produced in the absence of the Hybrid Harmony Search Algorithm (HHO). The subsequent section will examine the potential improvements in efficiency following the use of HHO.

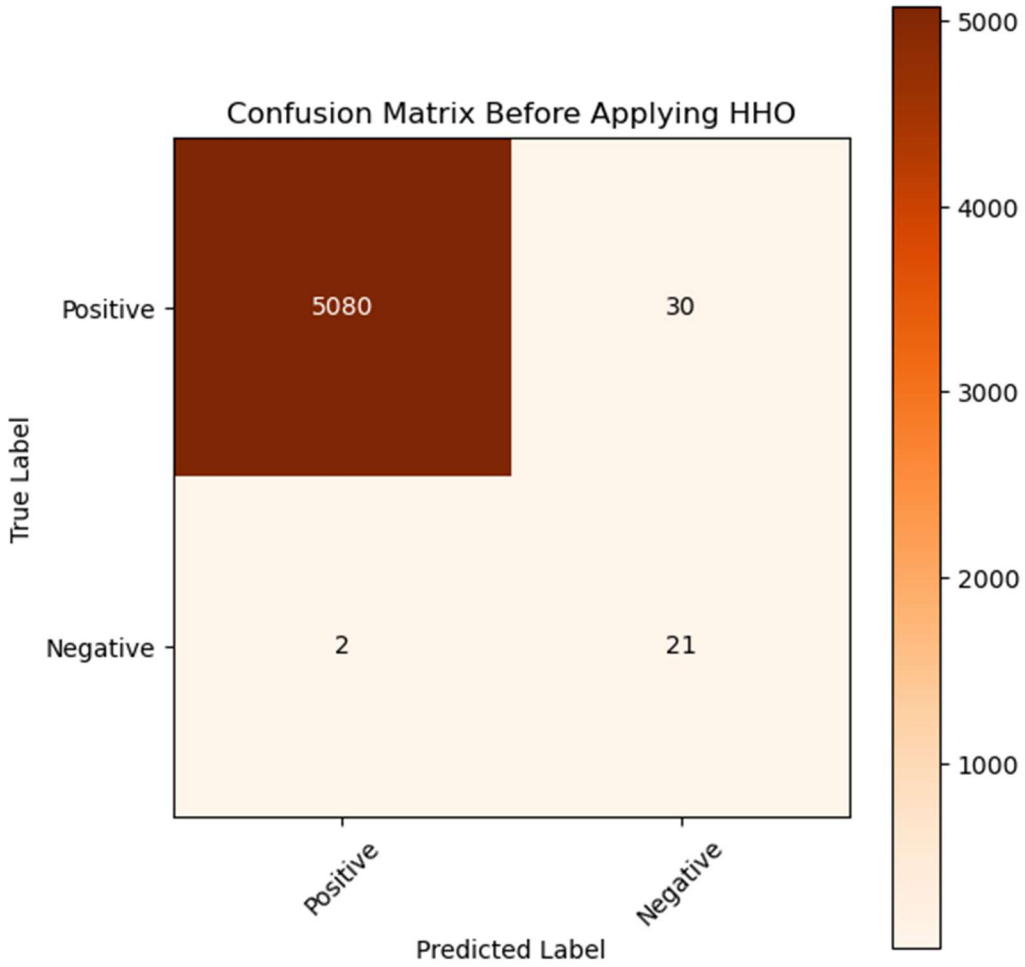

Figure 3. Confusion matrix before applying HHO.

A.2 RESULTS WITH HHO IMPLEMENTATION

The effectiveness of the RNN classifier was reassessed following the integration of the Harris Hawks Optimization (HHO) technique for feature selection. This study aimed to assess the effectiveness of HHO-driven feature optimization and to find potential enhancements in classification accuracy.

A.2.1 Feature Selection in Darknet Traffic Classification

When formulating a robust approach for categorizing Darknet data, focusing exclusively on the most significant components is imperative. The title suggests that Deep Learning and Harris Hawks Optimization are the primary approaches. However, it is crucial to understand each feature's underlying significance. Consequently, advanced optimization and classification methodologies are more prone to achieving success and efficiency.

The HHO method was employed to assess the significance of various variables, as depicted in Figure 4. The HHO (Hybrid et al.) is a machine-learning technique that employs ensemble learning to classify data. It accomplishes this by constructing multiple decision trees during the training phase and determining the mode of the classes for classification. One of the key advantages of using the HHO algorithm in this scenario is its ability to produce a feature significance score. This score accurately indicates the predictive capability of each feature. Upon training on the Darknet traffic dataset, the HHO classifier yielded a prioritized compilation of features. The 'Selected Features' refer to the set of 20 features that the classifier has chosen as the most significant. In order to have a comprehensive understanding of their respective significance, we conducted a comparative analysis between these features and the subsequent 20 features, which were designated as the "Deselected Features."

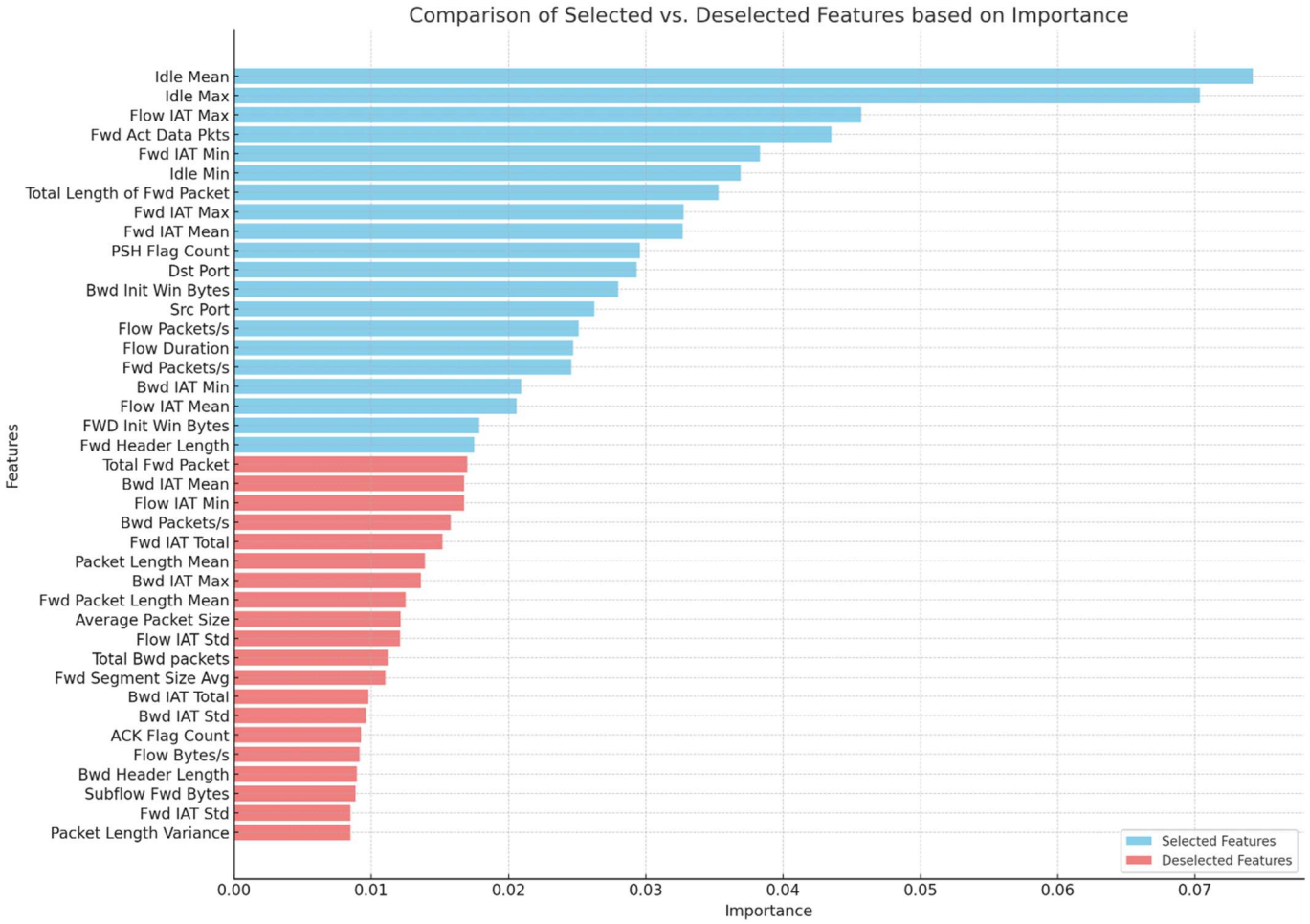

Figure 4. Comparison of Selected vs. Deselected Features based on Importance.

The figure shows that the 'Selected Features' exhibit superior predictive efficacy within the framework of categorizing Darknet traffic. Separating the data sets serves as a foundation for the core methodological approach, enabling the Deep Learning model and the Harris Hawks Optimization algorithm to concentrate on the most significant features, enhancing the precision of classification.

The utilization of feature selection using Harris Hawks Optimization (HHO) serves as a fundamental framework for comprehending the importance of features, with the primary objective of investigating the amalgamation of Deep Learning and HHO for Darknet Traffic Classification. By optimizing the dataset for relevance, the subsequent research methodological procedures can be designed to enhance the overall effectiveness of the suggested strategy.

A.2.2 CONFUSION MATRIX

The confusion matrix can provide valuable insights into the enhanced performance of the classifier after implementing the Harmony Search algorithm. Figure 5 illustrates the necessity of a comprehensive evaluation of the classifier's performance improvements, if any, following the Harris Hawks Optimization (HHO) technique. Based on a comprehensive review, it has been concluded that the classification system achieved a precision of 0.9990, indicating that 99.90% of the positively judged cases were accurately classified. The recall score of 0.9998% emphasizes the classifier's consistent capability to accurately identify almost all actual positive events. Upon incorporating HHO, the classifier demonstrated an overall accuracy of 0.9988, denoting an approximate prediction rate of 99.88%, which is deemed suitable.

The inclusion of the HHO has led to a notable improvement in the findings, albeit gradually. Furthermore, it is worth noting that a significant enhancement was observed, as evidenced by the balanced accuracy metric, which measures the consistency of performance across different classes, achieving a remarkable value of almost 98.93%. This development signifies a trend towards a more cohesive classification of various types of traffic. The F1 score, a metric that balances precision and recall, exhibited a value of 0.9994, indicating a further enhancement in aligning these crucial parameters following the implementation of HHO. The classifier's enhanced performance in mitigating false negatives was validated as a conclusive metric, indicated by an F2 score of around 99.96%, which exhibits a higher emphasis on recall. In general, these data provide evidence of the technique's effectiveness in improving the classifier's performance. This is particularly evident in its ability to create a more balanced classification landscape for various types of darknet traffic, which may be attributed to the integration of the HHO. The use of HHO demonstrates its efficacy in enhancing the classifier's performance, particularly in generating a more equitable categorization outcome across different traffic categories.

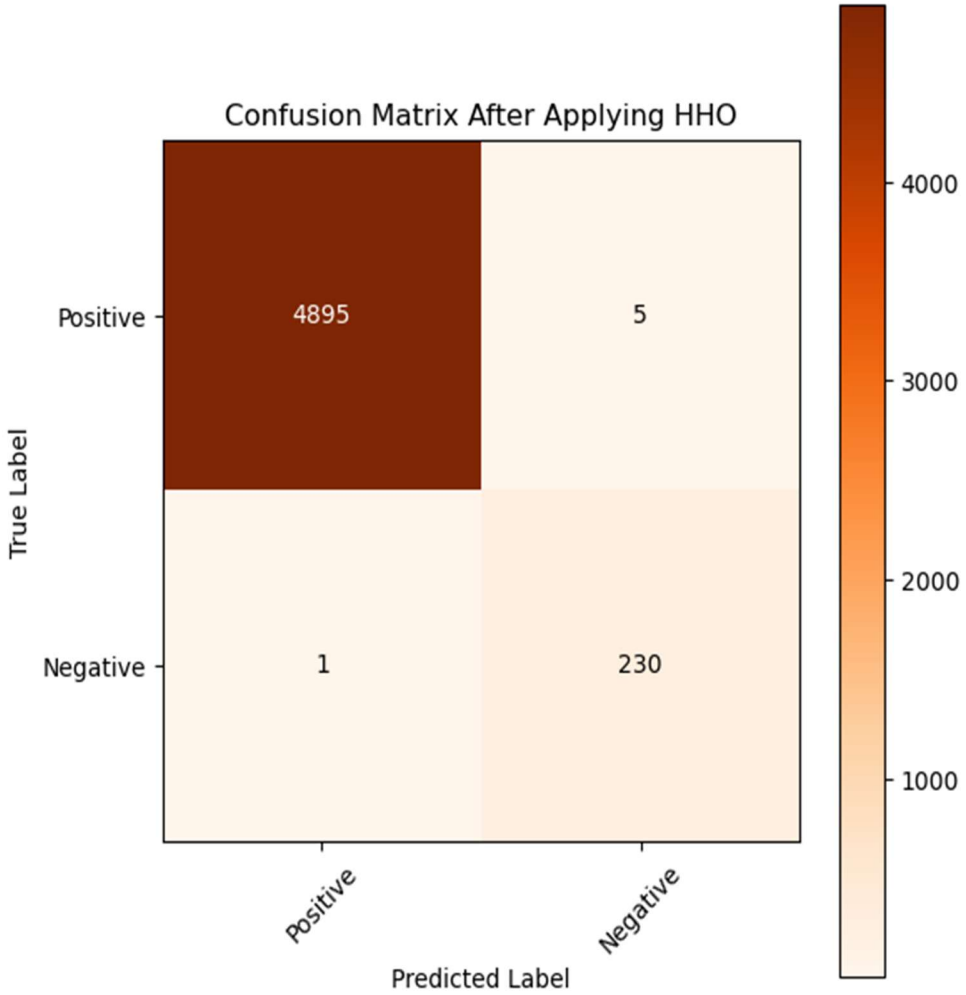

Figure 5. Confusion matrix After applying the HHO.

A.3 COMPARATIVE ANALYSIS

The main objective of this study was to assess the efficacy of the recently proposed Harris Hawks Optimization (HHO) technique. A comparative analysis of classification outcomes before and after the integration of HHO makes it evident that the integration effectively facilitates the classification of darknet traffic. The comparison above underscores the divergent performance metrics, hence demonstrating the practical advantages of employing HHO-driven feature selection.

Figure 6 illustrates that using HHO significantly increased precision, a parameter of utmost importance. The observed transition from a pre-HHO phase area under the curve (AUC) value of 0.9941 to a post-implementation AUC value of 0.9990 indicates a substantial reduction in false optimistic predictions, resulting in an enhancement of around 0.49 percent. Concurrently, the recall metric exhibited a marginal enhancement, increasing from 0.9996 to 0.9998 after using HHO. Those above slight yet significant modification showcases the classifier's resilient capacity to identify superior positive instances, even in an optimized feature landscape. The application of HHO enhanced the classification performance, as evidenced by an increase of approximately 0.5% in the accuracy indication. Specifically, the accuracy improved from 0.9938 to 0.9988. Furthermore, there was a significant rise in the percentage of accurate responses, rising from 70.57 percent to 99.93 percent. The observed rise in question is a notable illustration of the extensive impact of HHO, particularly in its effective resolution of issues stemming from class disparities. The F1 score, a metric that effectively combines precision and recall, rose during the post-HHO period, indicating the technique's ability to maximize both metrics concurrently. The F2 score, which prioritizes recall above other metrics, increased after the implementation of HHO. This observation provides more evidence of the enhanced capability of the model in mitigating false negatives. A significant revelation is unveiled through an in-depth analysis of the facts presented in the confusion matrix. The introduction of HHO resulted in a significant rise in the number of true negatives (TN), with an increase from 21 during the pre-HHO period to 230 post-implementations. The observed class imbalance in the dataset accentuates the enhanced discriminatory ability of the classifier in correctly identifying instances belonging to the negative class.

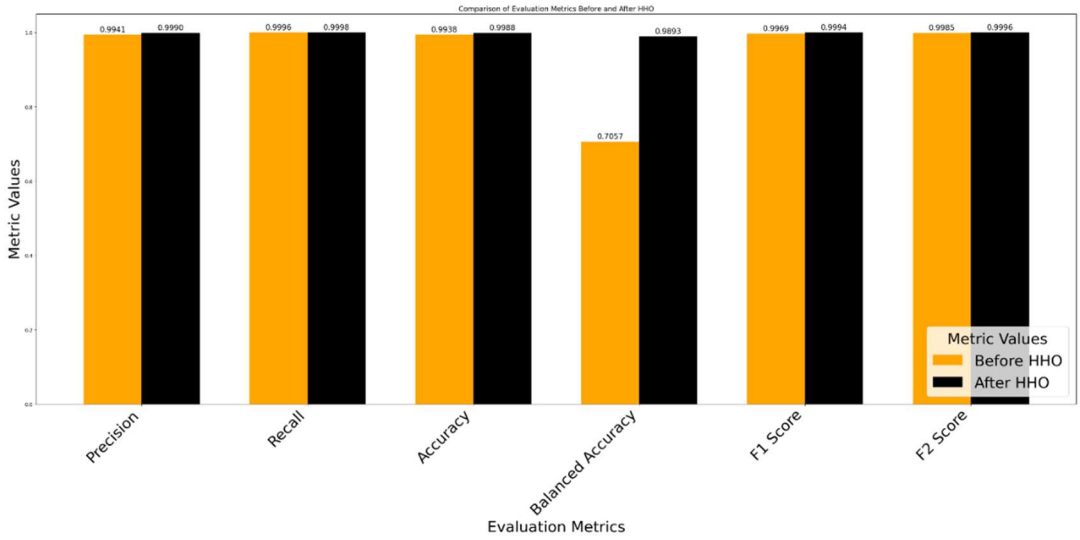

Figure 6. Comparison between the Evaluation metrics after and before the implementation of HHO.

V. DISCUSSION

Using the Harris Hawks Optimization (HHO) approach in our methodology has undeniably shown a significant improvement in the accuracy of classifications. The observation above aligns with the conclusions drawn by Chen et al. [7], who posited that using HHO significantly addresses a wide range of optimization challenges. The findings of this study are consistent with the research conducted by Kang et al. [18], which emphasized the efficacy of an enhanced HHO in the context of optimization scenarios.

Numerous scholars have embarked on classifying darknet traffic inside the domain. For example, the authors Abu Al-Haija et al. [2] and Khan et al. [32] placed significant emphasis on the use of machine learning models to detect and categorize traffic inside the Internet of Things (IoT) framework. Although encouraging results were attained in previous studies, our research goes further by integrating Recurrent Neural Networks (RNNs) with Harmony Search Algorithm (HHO) for feature selection. This integration leads to even more accurate classifications. A pertinent comparison aspect may be made with the scholarly contribution of Jenefa [16], who conducted an extensive investigation on the classification of network traffic inside the darknet. The study identifies issues related to the dynamic nature of darknet traffic and the need for adaptable models. Our approach offers possible answers using the benefits of deep learning and optimization methods.

The research conducted by Alimoradi et al. [3] showed the efficacy of deep learning in categorizing darknet traffic. Our research enhances the existing knowledge by showcasing that integrating deep learning, notably recurrent neural networks (RNNs), with sophisticated optimization approaches like hybrid harmony search algorithm (HHO) may provide even higher accuracy rates. Notwithstanding the accomplishments, our technique, like any other, has inherent limitations. Previous studies conducted by Heidari et al. [14] present research and many prior prominent studies in darknet traffic categorization and optimization approaches. Our technique, which incorporates Recurrent Neural Networks (RNNs) with Hybrid Harmony Search Optimization (HHO), demonstrates remarkable performance metrics. Specifically, it achieves an accuracy of 0.9988, precision of 0.9990, recall of 0.9998, and F1 score of 0.9994. These findings highlight the unique approach and outcomes of our methodology. Prior research conducted by Abu Al-Haija et al. [2] and Khan et al. [32] has centered on distinct machine learning models used in the context of Internet of Things (IoT) applications and the utilization of Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) for the identification of darknet traffic, respectively. While their results showed promise, neither study used sophisticated optimization methods, such as HHO, implemented in our research. The study's findings by Alimoradi et al. [3] underscored the strong performance and reliability of deep learning techniques, which is consistent with our focus on recurrent neural networks (RNNs). Nevertheless, making direct data comparisons is a challenge owing to variations in datasets and research aims across different studies. However, the results of our investigation, when coupled with the optimization of HHO, provide a slight advantage in accuracy and precision. This highlights the possibility of using the combined technique for classifying darknet traffic.

Table 2. Comparative Analysis with related studies.

Study Reference	Methodology/Technique	Remarks
Current Study	RNN + HHO	Demonstrated significant improvement with HHO integration.
Abu Al-Haija et al. (2022)	Machine Learning for IoT Applications	Specific to IoT applications.
Sarwar et al. (2021)	CNN-LSTM for darknet traffic detection	Achieved promising results but without the use of optimization techniques like HHO.
Alimoradi et al. (2022)	Deep Neural Classification	Emphasized the strengths of deep learning in darknet traffic classification.
Jenefa (2023)	Survey on network traffic classification in the darknet	Comprehensive survey without specific implementation.
Kang et al. (2023)	Improved HHO for optimization	Showcased the potential of HHO but not applied to darknet traffic.
Chen et al. (2020)	HHO for diverse optimization problems	Demonstrated the capabilities of HHO, aligning with our findings.

The current investigation makes a substantial contribution to darknet traffic categorization by incorporating the Harris Hawks Optimization (HHO) approach with Recurrent Neural Networks (RNNs). The amalgamation under consideration has shown exceptional accuracy, precision, recall, and F1 scores. Additionally, it has effectively tackled the common issues of class imbalance and feature selection often encountered in darknet traffic datasets. Our methodology, which focuses on optimizing features driven by HHO, highlights the significance of prioritizing pertinent characteristics to improve the model's performance. This article presents a departure from traditional approaches by highlighting the potential of integrating deep learning with sophisticated optimization techniques, stressing the synergistic effects that may be achieved. The research findings address a significant void in the current body of literature by introducing a rigorous methodology that has proven effective in practical darknet traffic situations. As a result, this study contributes valuable insights and strategies to the existing knowledge in the field of darknet traffic classification.

VI. CONCLUSION

The present study undertook an extensive investigation into categorizing darknet data using a combination of Recurrent Neural Networks (RNNs) and the Harris Hawks Optimization (HHO) approach. The outcomes of the research clearly emphasize the effectiveness of this integrated strategy. Significantly improved classification metrics, including accuracy, recall, and F1 score, were seen after the installation of HHO. The implementation also demonstrated the classifier's enhanced capacity to effectively address underlying class imbalances, as seen by the notable rise in true negatives. In addition, using HHO-driven feature selection resulted in enhanced model performance and underscored the significance of prioritizing crucial characteristics within the darknet traffic dataset. Therefore, the findings of this research provide evidence of the capability of integrating deep learning with sophisticated optimization techniques. The present study introduces a unique, resilient, and very efficient approach to the current corpus of knowledge, establishing a standard for future undertakings in darknet traffic categorization.

Although this research has shown encouraging findings on the use of Recurrent Neural Networks (RNNs) and Harris Hawks Optimization (HHO) to classify darknet traffic, it is essential to acknowledge the existence of some constraints. The use of HHO (Harmony et al.) in the feature selection process may unintentionally exclude contextually relevant features. Moreover, the processing requirements associated with the iterative HHO optimization provide difficulties when considering real-time applications. Subsequent research endeavors should prioritize the enhancement of the HHO process in order to achieve superior real-time effectiveness. Additionally, it is essential to investigate alternative optimization strategies and validate the suggested approach using extensive and varied datasets to ascertain its broader applicability.

ACKNOWLEDGMENT

The author extends sincere gratitude and appreciation to Middle East University, particularly the Faculty of Information Technology, Department of Cybersecurity, for their invaluable support and resources provided throughout this research. Their commitment to fostering an environment conducive to academic excellence significantly contributed to the successful completion of this study.

References

[1] S. Abbas, G. A. Sampedro, M. Abisado, A. Almadhor, I. Yousaf, and S.-P. Hong, "Harris-hawk-optimization-based deep recurrent neural network for securing the Internet of medical things," *Electronics*, vol. 12, no. 12, pp. 2612, 2023, https://doi.org/10.3390/electronics12122612.

[2] Q. Abu Al-Haija, M. Krichen, and W. Abu Elhaija, "Machine-learning-based Darknet traffic detection system for IOT applications," *Electronics*, vol. 11, no. 4, pp. 556, 2022, https://doi.org/10.3390/electronics11040556.

[3] M. Alimoradi, M. Zabihimayvan, A. Daliri, R. Sledzik, and R. Sadeghi, "Deep neural classification of darknet traffic," *Artificial Intelligence Research and Development*, pp. 105-114, 2022, https://doi.org/10.3233/FAIA220323.

[4] S. Arisdakessian, O. A. Wahab, A. Mourad, H. Otrok, and M. Guizani, "A survey on IOT intrusion detection: Federated learning, game theory, social psychology, and explainable AI as future directions," *IEEE Internet of Things Journal*, vol. 10, no. 5, pp. 4059-4092, 2023, https://doi.org/10.1109/JIOT.2022.3203249.

[5] K. Bansal and A. Singhrova, "Review on intrusion detection system for IOT/IIOT - brief study," *Multimedia Tools and Applications*, vol. 83, pp. 23083–23108, 2024. https://doi.org/10.1007/s11042-023-16395-6.

[6] L. Chang, T. Lee, H. Chu, and C. Su, "Application-based online traffic classification with deep learning models on SDN networks," *Advances in Technology Innovation*, vol. 5, no. 4, pp. 216–229, 2020. https://doi.org/10.46604/aiti.2020.4286.

[7] H. Chen, A. A. Heidari, H. Chen, M. Wang, Z. Pan, and A. H. Gandomi, "Multi-population differential evolution-assisted Harris Hawks Optimization: Framework and case studies," *Future Generation Computer Systems*, vol. 111, pp. 175-198, 2020. https://doi.org/10.1016/j.future.2020.04.008.

[8] L. Chen, N. Song, and Y. Ma, "Harris Hawks optimization based on global cross-variation and tent mapping," *The Journal of Supercomputing*, vol. 79, no. 5, pp. 5576-5614, 2022. https://doi.org/10.1007/s11227-022-04869-7.

[9] R. Dangi and P. Lalwani, "Harris Hawks optimization based hybrid deep learning model for efficient network slicing in 5G network," *Cluster Computing*, vol. 27, pp. 395–409, 2024. https://doi.org/10.1007/s11227-022-04869-7.

[10] S. Dargan, M. Kumar, M. R. Ayyagari, and G. Kumar, "A survey of deep learning and its applications: A new paradigm to machine learning," *Archives of Computational Methods in Engineering*, vol. 27, no. 4, pp. 1071-1092, 2019. https://doi.org/10.1007/s11831-019-09344-w.

[11] S. Davis and B. Arrigo, "The dark web and anonymizing technologies: Legal pitfalls, ethical prospects, and policy directions from radical criminology," *Crime, Law and Social Change*, vol. 76, no. 4, pp. 367-386, 2021. https://doi.org/10.1007/s10611-021-09972-z.

[12] C. Fachkha and M. Debbabi, "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197-1227, 2016. https://doi.org/10.1109/COMST.2015.2497690.

[13] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, G. Wang, J. Cai, and T. Chen, "Recent advances in convolutional neural networks," *Pattern Recognition*, vol. 77, pp. 354-377, 2018. https://doi.org/10.1016/j.patcog.2017.10.013.

[14] A. Heidari, N. Jafari Navimipour, M. Unal, and G. Zhang, "Machine learning applications in internet-of-drones: Systematic review, recent deployments, and open issues," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1-45, 2023. https://doi.org/10.1145/3571728.

[15] X. Hu, L. Chu, J. Pei, W. Liu, and J. Bian, "Model complexity of deep learning: A survey," *Knowledge and Information Systems*, vol. 63, no. 10, pp. 2585-2619, 2021. https://doi.org/10.1007/s10115-021-01605-0.

[16] A. Jenefa, "The ascent of network traffic classification in the dark net: a survey," *Journal of Intelligent & Fuzzy Systems*, vol. 45, no. 3, pp. 3679-3700, 2023. https://doi.org/10.3233/JIFS-231099.

[17] M. Kahng, P. Y. Andrews, A. Kalro, and D. H. Chau, "Activis: Visual exploration of industry-scale deep neural network models," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 1, pp. 88-97, 2018. https://doi.org/10.1109/TVCG.2017.2744718.

[18] H. Kang, R. Liu, Y. Yao, and F. Yu, "Improved Harris Hawks optimization for non-convex function optimization and design

optimization problems," *Mathematics and Computers in Simulation*, vol. 204, pp. 619-639, 2023. https://doi.org/10.1016/j.matcom.2022.09.010.

[19] M. A. Khan, M. Sharif, T. Akram, M. Raza, T. Saba, and A. Rehman, "Hand-crafted and deep convolutional neural network features fusion and selection strategy: An application to intelligent human action recognition," *Applied Soft Computing*, vol. 87, p. 105986, 2020. https://doi.org/10.1016/j.asoc.2019.105986.

[20] Q. Liu, M. Li, N. Cao, Z. Zhang, and G. Yang, "Improved Harris combined with clustering algorithm for data traffic classification," *IEEE Access*, vol. 10, pp. 72815-72824, 2022. https://doi.org/10.1109/ACCESS.2022.3188866.

[21] J. Mazel, P. Casas, R. Fontugne, K. Fukuda, and P. Owezarski, "Hunting attacks in the dark: Clustering and correlation analysis for unsupervised anomaly detection," *International Journal of Network Management*, vol. 25, no. 5, pp. 283-305, 2015. https://doi.org/10.1002/nem.1903.

[22] M. Murty, H. Rana, R. Verma, R. Pathak, and P. H. Rughani, "Building an AI/ML based classification framework for Dark Web text data," *Proceedings of the International Conference on Computing and Communication Networks*, 2022, pp. 93-111. https://doi.org/10.1007/978-981-19-0604-6_9.

[23] R. Niranjana, V. A. Kumar, and S. Sheen, "Darknet traffic analysis and classification using numerical AGM and mean shift clustering algorithm," *SN Computer Science*, vol. 1, no. 1, article 16, 2020. https://doi.org/10.1007/s42979-019-0016-x.

[24] P. Pham, L. T. T. Nguyen, W. Pedrycz, and B. Vo, "Deep learning, graph-based text representation and classification: a survey, perspectives and challenges," Artificial Intelligence Review, vol. 56, pp. 4893–4927, 2023, https://doi.org/10.1007/s10462-022-10265-7

[25] P. Pham, L. T. Nguyen, W. Pedrycz, and B. Vo, "Deep learning, graph-based text representation and classification: A survey, perspectives and challenges," *Artificial Intelligence Review*, vol. 56, no. 6, pp. 4893-4927, 2022. https://doi.org/10.1007/s10462-022-10265-7.

[26] S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M.-L. Shyu, S.-C. Chen, and S. S. Iyengar, "A survey on deep learning," *ACM Computing Surveys*, vol. 51, no. 5, pp. 1-36, 2018. https://doi.org/10.1145/3234150.

[27] A. Pramod, H. S. Naicker, and A. K. Tyagi, "Machine learning and deep learning: Open issues and future research directions for the next 10 years," *Computational Analysis and Deep Learning for Medical Care*, pp. 463-490, 2021. https://doi.org/10.1002/9781119785750.ch18 Available at: https://doi.org/10.1002/9781119785750.ch18.

[28] D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in big data era: From securing big data to data-driven security," *IEEE Transactions on Services Computing*, vol. 14, no. 6, pp. 2055-2072, 2021. https://doi.org/10.1109/TSC.2019.2907247.

[29] A. T. Sahlol, D. Yousri, A. A. Ewees, M. A. Al-qaness, R. Damasevicius, and M. A. Elaziz, "Covid-19 image classification using deep features and fractional-order Marine Predators algorithm," *Scientific Reports*, vol. 10, no. 1, article 15364, 2020. https://doi.org/10.1038/s41598-020-71294-2.

[30] I. H. Sarker, "Deep learning: A comprehensive overview on techniques, taxonomy, applications and research directions," *SN Computer Science*, vol. 2, no. 6, article 420, 2021. https://doi.org/10.1007/s42979-021-00815-1.

[31] M. Sarwar, G. Abbas, R. Talib, M. Younas, and M. Sarwar, "Darkdetect: darknet traffic detection and categorization using modified convolution-long short-term memory," *IEEE Access*, vol. 9, pp. 113705-113713, 2021. https://doi.org/10.1109/ACCESS.2021.3105000.

[32] M. A. Khan, K. Javed, S. A. Khan, and others, "Human action recognition using fusion of multiview and deep features: an application to video surveillance," Multimedia Tools and Applications, vol. 83, pp. 14885–14911, 2024, https://doi.org/10.1007/s11042-020-08806-9

[33] C. A. S. Murty, H. Rana, R. Verma, R. Pathak, and P. H. Rughani, "Building an AI/ML Based Classification Framework for Dark Web Text Data," in Proceedings of International Conference on Computing and Communication Networks, A. K. Bashir, G. Fortino, A. Khanna, and D. Gupta, Eds., Lecture Notes in Networks and Systems, vol. 394, Singapore: Springer, 2022, pp. 93–111. https://doi.org/10.1007/978-981-19-0604-6_9

[34] A. Selim, S. Kamel, G. Murtaza, and F. Jurado, ""Optimal placement of DGS in distribution system using an improved Harris Hawks optimizer based on single- and multi-objective approaches," *IEEE Access*, vol. 8, pp. 52815-52829, 2020. https://doi.org/10.1109/ACCESS.2020.2980245.

[35] F. Soro, M. Allegretta, M. Mellia, I. Drago, and L. Bertholdo, "Sensing the noise: uncovering communities in darknet traffic," *Proceedings of the 2020 Mediterranean Communication and Computer Networking Conference (MedComNet)*, Arona, Italy, 2020, pp. 1-8. https://doi.org/10.1109/MedComNet49392.2020.9191555.

[36] P. Wang, E. Fan, and P. Wang, "Comparative analysis of image classification algorithms based on traditional machine learning and deep learning," *Pattern Recognition Letters*, vol. 141, pp. 61-67, 2021. https://doi.org/10.1016/j.patrec.2020.07.042.

[37] Z. Wu, L. Zhang, and M. Yue, "Low-rate DOS attacks detection based on network multifractal," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 5, pp. 559-567, 2016. https://doi.org/10.1109/TDSC.2015.2443807.

[38] Y. Zeng, H. Gu, W. Wei, and Y. Guo, "$deep-full-range$: A deep learning based network encrypted traffic classification and intrusion detection framework," *IEEE Access*, vol. 7, pp. 45182-45190, 2019. https://doi.org/10.1109/ACCESS.2019.2908225.

[39] C. Zhong, M. Wang, C. Dang, W. Ke, and S. Guo, "First-order reliability method based on Harris Hawks optimization for high-dimensional reliability analysis," *Structural and Multidisciplinary Optimization*, vol. 62, no. 4, pp. 1951-1968, 2020. https://doi.org/10.1007/s00158-020-02587-3.

[40] M. Coutinho Marim, P. V. Ramos, A. B. Vieira, A. Galletta, M. Villari, R. M. de Oliveira, and E. F. Silva, "Darknet traffic detection and characterization with models based on decision trees and neural networks," *Intelligent Systems with Applications*, vol. 18, p. 200199, 2023. https://doi.org/10.1016/j.iswa.2023.200199.

[41] L. Ye, Y. Yimeng, and C. Wei, "Analyzing public perception of educational books via text mining of online reviews," *Procedia Computer Science*, vol. 221, pp. 617-625, 2023. https://doi.org/10.1016/j.procs.2023.08.030.

[42] M. Bachmann, J. Beermann, T. Brey, H. J. de Boer, J. Dannheim, B. Edvardsen, P. G. Ericson, K. C. Holston, V. A. Johansson, P. Kloss, R. Konijnenberg, K. J. Osborn, P. Pappalardo, P. H. Pehlke, D. Piepenburg, T. H. Struck, P. Sundberg, S. S. Markussen, K. Teschke, and M. P. Vanhove, "The role of systematics for understanding ecosystem functions: Proceedings of the zoologica scripta symposium, Oslo, Norway, 25 August 2022," *Zoologica Scripta*, vol. 52, no. 3, pp. 187-214, 2023. https://doi.org/10.1111/zsc.12593.

[43] J. Ahmed, H. H. Gharakheili, C. Russell, and V. Sivaraman, "Automatic detection of DGA-enabled malware using SDN and traffic behavioral modeling," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 4, pp. 2922-2939, 2022. https://doi.org/10.1109/TNSE.2022.3173591.

[44] J. Jaafari, S. Douzi, K. Douzi, and B. Hssina, "The impact of ensemble learning on surgical tools classification during laparoscopic cholecystectomy," *Journal of Big Data*, vol. 9, no. 1, article 49, 2022. https://doi.org/10.1186/s40537-022-00602-6.

[45] F. Pouromran, Y. Lin, and S. Kamarthi, "Personalized deep BI-LSTM RNN based model for pain intensity classification using EDA Signal," *Sensors*, vol. 22, no. 21, p. 8087, 2022. https://doi.org/10.3390/s22218087.

[46] A. Kaveh and Y. Gholipour, "Prediction of strength for concrete specimens using artificial neural network," *Asian Journal of Civil Engineering*, vol. 2, no. 2, pp. 1-13, 1998.

[47] A. Kaveh, Y. Gholipour, and H. Rahami, "Optimal design of transmission towers using genetic algorithm and neural networks," *International Journal of Space Structures*, vol. 23, no. 1, pp. 1-19, 2008. https://doi.org/10.1260/026635108785342073.

[48] A. Kaveh and N. Khavaninzadeh, "Efficient training of two ANNs using four meta-heuristic algorithms for predicting the FRP strength," *Structures*, vol. 52, pp. 256-272, 2023. https://doi.org/10.1016/j.istruc.2023.03.178.

[49] M. Koc, Ö. Ekmekcioğlu, and A. P. Gurgun, "Developing a national data-driven construction safety management framework with interpretable fatal accident prediction," *Journal of Construction Engineering and Management*, vol. 149, no. 4, p. 04023010, 2023. https://doi.org/10.1061/JCEMD4.COENG-12848.

[50] M. Hasan Ghodusinejad, A. Ghodrati, R. Zahedi, and H. Yousefi, "Multi-criteria modeling and assessment of PV system performance in different climate areas of Iran," *Sustainable Energy Technologies and Assessments*, vol. 53, p. 102520, 2022. https://doi.org/10.1016/j.seta.2022.102520.

[51] S. Karimzadeh, M. Ghasemi, M. Matsuoka, K. Yagi, and A. Banihashemi, "Experimental investigation and numerical simulation of strain-induced crystallization in glassy polymers during uniaxial tensile loading," *International Journal of Mechanical Sciences*, vol. 108, pp. 169-181, 2016. https://doi.org/10.1016/j.ijmecsci.2016.02.012.

[52] H. Jolani and A. Kaveh, "Application of modified teaching-learning algorithm in civil engineering optimization problems," *Journal of the*

Franklin Institute, vol. 352, no. 11, pp. 4458-4473, 2015. https://doi.org/10.1016/j.jfranklin.2015.08.012.

[53] M. M. Islam, M. R. Rahman, and A. Kaveh, "Performance analysis of back-propagation neural networks in predicting compressive strength of high-performance concrete incorporating metakaolin," *Advances in Engineering Software*, vol. 55, pp. 19-29, 2013. https://doi.org/10.1016/j.advengsoft.2012.12.010.

[54] H. M. Balaha and A. E. S. Hassan, "Skin cancer diagnosis based on deep transfer learning and sparrow search algorithm," *Neural Computing and Applications*, vol. 35, no. 1, 2023, pp. 815-853. https://doi.org/10.1007/s00521-022-07762-9.

[55] B. A. Taha, Y. A. Mashhadany, A. H. Al-Jumaily, M. S. D. B. Zan, and N. Arsad, "SARS-CoV-2 morphometry analysis and prediction of real virus levels based on full recurrent neural network using TEM images," *Viruses*, vol. 14, no. 11, pp. 2386, 2022. https://doi.org/10.3390/v14112386.

[56] K. Koc, Ö. Ekmekcioğlu, and A. P. Gurgun, "Developing a national data-driven construction safety management framework with interpretable fatal accident prediction," *Journal of Construction Engineering and Management*, vol. 149, no. 4, p. 04023010, 2023. https://doi.org/10.1061/JCEMD4.COENG-12848.

[57] M. C. Marim, P. V. B. Ramos, A. B. Vieira, A. Galletta, M. Villari, R. M. de Oliveira, and E. F. Silva, "Darknet traffic detection and characterization with models based on decision trees and neural networks," Intelligent Systems with Applications, vol. 18, p. 200199, 2023, https://doi.org/10.1016/j.iswa.2023.200199.

[58] S. Karimzadeh, M. Ghasemi, M. Matsuoka, K. Yagi, and A. C. Zulfikar, "A deep learning model for road damage detection after an earthquake based on synthetic aperture radar (SAR) and field datasets," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 15, pp. 5753-5765, 2022. https://doi.org/10.1109/JSTARS.2022.3189875.

[59] M. Lübbering, M. Gebauer, R. Ramamurthy, C. Bauckhage, and R. Sifa, "Bounding open space risk with decoupling autoencoders in open set recognition," *International Journal of Data Science and Analytics*, vol. 14, no. 4, pp. 351-373, 2022. https://doi.org/10.1007/s41060-022-00342-z.

[60] S. Liu, L. Liu, E. Kozan, P. Corry, M. Masoud, and X. Li, "Machine learning for open-pit mining: A systematic review," Available at SSRN 4540535.

[61] M. Al-Fayoumi, M. Al-Fawa'reh, and S. Nashwan, "VPN and Non-VPN network traffic classification using time-related features," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 3091-3111, 2022. https://doi.org/10.32604/cmc.2022.025103.

[62] A. Ishtaiwi, J. Petra, A. Ali, A. Al-Qerem, Y. Alsmadi, A. Aldweesh, M. Alauthman, O. Alzubi, S. Nashwan, A. Ramadan, and M. Al-Zghoul, "Impact of data-augmentation on brain tumor detection using different YOLO versions models," *International Arab Journal of Information Technology*, vol. 21, no. 3, pp. 466–482, 2024. https://doi.org/10.34028/iajit/21/3/10.

[63] A. Al-Qerem, A. M. Ali, I. Jebreen, A. Nabot, S. Nashwan, A. Aldweesh, and M. Alzgol, "Enhancing stroke prediction using generative adversarial networks for intelligent medical care," *International Journal of Crowd Science*, 2024. [Online]. Available at: https://www.sciopen.com/article/10.26599/IJCS.2023.9100034.

[64] A. Al-Qerem, A. M. Ali, S. Nashwan, M. Alauthman, A. Hamarsheh, A. Nabot, and I. Jibreen, "Transactional services for concurrent mobile agents over edge/cloud computing-assisted social Internet of Things," *ACM Journal of Data and Information Quality*, vol. 15, no. 3, pp. 1–20, 2023. https://doi.org/10.1145/3603714.

***AHMED HASSAN** received a M.Sc. degree in Computer Information Systems and a Ph.D. in Information Security from MEDIU University in Malaysia. He previously served as the Head of the Cybersecurity and Software Engineering Departments at Ajloun National University. He is currently the Head of the Cybersecurity Department at Middle East University in Amman, Jordan.*

His research interests include Cybersecurity, Software Engineering, AI, and Networks.