Cloud Security Based Malware and Ransomware Detection Model Using Supervised Machine Learning Techniques

Raed Alharthi

Department of Computer Science and Engineering, University of Hafr Albatin, Saudi Arabia
https://orcid.org/0000-0001-6182-7923

Abstract
Cloud computing offers several kinds of computer services via the Internet. Instead of utilizing their local storage, many consumers and enterprises are adopting the cloud to store their data remotely in data centers. This allows access to data from any device, at any time, and from any location. Protecting privacy and dealing with malware threats are two of the main issues facing cloud computing. Ransomware attacks have seen hackers take important data hostage in exchange for financial gain. The encrypted nature of ransomware-infected files makes it challenging to retrieve original data from them without special keys. The accuracy of malware detection has been the subject of several research, but the privacy protection of cloud tenants has not received enough attention. This research presents a novel feature extraction, selection, and detection approach for cloud-based semi-supervised transfer learning (SSTL) malware and ransomware detection. CatBoost classifiers are intended to identify malware and ransomware files to protect tenants' privacy in public cloud environments. Temporal Convolution Networks (TCNs) are used in this phase to calculate features, feature action kinds, and path scores. First, each property's frequency is computed. The Sand Cat Swarm Optimization technique is utilized to select features based on path scores and action states once the frequency computation is complete. Following feature selection, we categorize malware and ransomware attacks using the CatBoost algorithm. In terms of detecting and categorizing attacks, the CatBoost method performs better than other machine learning classifiers.

Keywords:
Malware detection; Ransomware detection; Temporal Convolution Networks; Machine learning.

1. Introduction

The fast increase of attacks like malware and ransomware has come up as an emerging threat to cybersecurity. Nowadays, malware and ransomware are very famous tools with these cybercriminals force the wounded person for money by doing encryption on their original data and demand money for the key to decryption. The ransomware and malware attack impact are identified in all industries, from healthcare to government and finance to education. The most attractive area is education. Malware and ransomware attack nature, how they were spread, and the significant consequences of wounded people. The most important concept of a survey regarding this topic cannot be overplayed. Because of these increasing malware and ransomware attacks, there is a strong essential need to create a technology to mitigate and prevent the attacks for practitioners and scholars. This research paper provides the malware and ransomware threat overview, investigating the concepts that contribute to the malware and ransomware spread and ransomware spread and prevent the way to protect the files and resources by using technology semi-supervised transfer learning (SSTL). CatBoost or Categorical Boost is used for regression purposes which increases the quality of classification compared to other approaches in the domain of malware and ransomware attack. The Temporal convolution network (TCN) framework is used to find the features and translate the raw data into numerical features. Finally, the optimization algorithmic SCSO is utilized for optimization.

The key contributions of the research are:

- Two datasets (malware and ransomware) are used, which contain benign and malicious programs
- Utilizing the concept of Temporal Convolution Networks (TCN) the feature will be extracted. Also, it can increase the speed of execution.
- By utilizing the concept of the Sand Cat Optimization Algorithm, the feature selection will be done
- With the help of the CatBoost classifier, malware and ransomware attacks will be detected

This article is structured as mentioned below, section 2 explains the details of the literature review, and section 3 explains the new methodology utilized in this article, section 4 explains the experimental results of the newly developed system.

2. Literature Review

The process of collecting the data was done by choosing up-to-date and relevant conference and journal articles from good quality databases, namely archives. Org, IET, Elsevier, MDPI, Springer, and IEEE, also some other sources like dissertations /theses journals from universities, and companies namely Techspot, Symantec, crowd strike and Microsoft published blogs. The gathered details were divided into technical and non-technical sources. The

Manuscript received April 5, 2025
Manuscript revised April 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.4.22

technical research paper proposes a way to the problems of malware and ransomware attacks [1].

The non-technical research paper contains common details about malware and ransomware, and this can be used to give proper information while writing the introduction about malware and ransomware [2]. The technical research papers are divided into two groups, namely Artificial Intelligence based, non-artificial Intelligence; also, the AI-based methodologies were categorized into ANN (Artificial Neural Networks), ML, and DL. In the same way, the non-AI-based methodologies were categorized into traffic and packet investigation [3].

The process of data collection summarizes each article by analyzing the issues, objectives, and approaches/ techniques utilized. The success of the articles in terms of results created and the limitations of the research. Synthesis of information was utilized to determine the relationship or similarities among the articles in every group [4]. Protecting from malware and ransomware is very difficult for many reasons. The function of ransomware is similar to the software benign. Malware and ransomware can be available in different methodologies and tools.

An approach related to the analysis of static decomposes the source code without executing the source code [5]. The attackers continuously develop different variations of code and modify their source code by utilizing different packaging approaches. To overcome these problems, the research scholar utilizes the analysis of dynamic behaviors that notice the interactions between the virtual environment and executed code.

Machine learning is one of the best approaches to finding malware and ransomware because it efficiently learns the anomalies and patterns in big datasets, which may be very difficult for human beings to identify [6]. In – this context the machine learning approach is trained on big datasets of benign and malicious software to train the characteristics of behavior that differentiates malware and ransomware from normal software [7].

To differentiate the malware and ransomware attacks that have not yet been recognized by seeing an application or file's access permissions and memory area it leads to access. Analyzing the ascertaining and behavior of lawful purposes, applications, and files before running is acceptable and beneficial [8].

Numerous efficient machine learning approaches are utilized for more efficient and accurate malware and ransomware identification tools. The malware and ransomware prevention and detection approach were developed for an unstructured dataset obtained from Ecuadorian Control and Regulating Institution (EcuCERT) logs [9]. This approach utilizes musing to pin special patterns joined to Windows ransomware and malware. A selection of features is supplied to the data to filter the common discriminating and beneficial information that specifies an attack of ransomware. The filtered data presents that the algorithm of learning in malware and ransomware is precisely and swiftly determined using the features of the input algorithm and set that duplicates the abnormal patterns of behavior [10].

3. Proposed System

Nowadays cyber security is a most interesting and demanding topic in the research area. Big organizations and educational institutions are using cloud methodology to store their data, files, and applications. The benefit of storing these files in the cloud is that the user can view their files on any device, at anytime and anywhere in the world. This is very helpful for the consumer to see their files. By this, the consumer can do any work at any time without any intervention. But the problem here is safety; the cybercriminals attack the files and change their data. Protecting the files and applications from cybercriminals is very risky. Many researchers developed many applications to overcome this problem, but the accuracy and efficiency are low. A new technology was developed to safeguard files against malware and ransomware threats. The following diagram in Figure 1 ("General structure of the proposed system") represents the general structure of the newly developed system to protect the files and applications from unauthorized persons or devices.

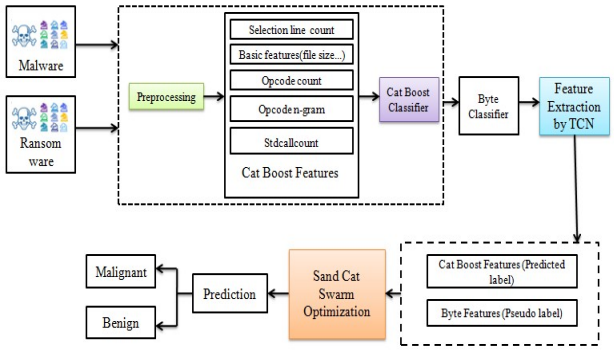


Fig 1: General structure of the proposed system

In the proposed system we utilized two sets of datasets: malware and ransomware. These two datasets may contain benign and malicious applications and files. To select the features, we used the Temporal Convolution Network. This convolution network is similar to common convolution networks, but the speed of execution is high compared to other convolution networks.

For selecting the features, we choose the Sand Cat Swarm Optimization algorithm, because, detecting the malware and ransomware this optimization algorithm is well suited compared to other optimization algorithms. The CatBoost algorithm is utilized to detect malware and ransomware attacks.

3.1 Dataset Description

In this research, we used malware and ransomware datasets to detect whether the application or file was affected by malware or ransomware [13]. We used malignant and benign data to identify the affected files.

3.2 Processing of Data

Processing data is the way of interchanging raw data into a useful or understandable structure. This may have a couple of steps, the first one is an accusation of data, which refers to changing misplacement values, outlier removal, and removing repeated values, and the second one is validation of data to assure consistency and completeness [14]. In our research, we identified that the dataset does not contain any duplicate value, as the row number is equal to the column number [15]. The features are continuous numerical variables except for status. The status may contain a binary variable; it may be 0 or 1.

3.3 Temporal Convolution Network

Temporal Convolution Network is a structure that employs normal dilations and convolutions, because of that this can be suitable for sequential data with its huge fields of receptivity and temporality. Here we chose TCN for calculating the features because it is faster than RNN and LSTM. Consequently, the computations are performed more efficiently and at a faster manner [16]. To train our convolution network, to detect malware and ransomware, the training set may contain the details of the input sequence and target sequence. TCN can take a series of any length as input and produce the same length of output. Out of other convolution networks, TCN performs well in prediction tasks in the time series. We selected TCN for our research and implemented it accordingly. This approach resulted in a significant improvement in the prediction accuracy for malware and ransomware detection.

3.4. Classification

During the classification phase, the feature selection process was done. With the help of the ordered encoding technique, the CatBoost algorithm encodes the features of categories. The ordered encoding considers the statistics of the target from all rows before the data point to compute the values and replaces the features of categories. Also, the CatBoost algorithm has a unique characteristic that it utilizes the concept of a symmetric tree. This shows that at every level of depth, all the nodes of the decision tree use the unique split situation. Because of this unique character, it detects malware and ransomware quickly and accurately compared to other techniques. The researchers employed the CatBoost algorithm in their study, which enabled them to achieve high accuracy results within a short time frame.

3.5 Sand Cat Swarm Optimization Algorithm

i. Population Initialization

Every cat in the sand has a 1^{x} dime array in the dimension of dime issues of optimization. The following diagram in figure 2 shows the problem solution. Every Pos (Pos_1, Pos_2 ..... Pos_{dime}) lies in between the limits to the top and bottom. In the algorithm of initialization, the matrix of initialization is developed based on the length of the problem which may be (N^{x} dime) [17]. Additionally, the corresponding solution is the result in every iteration. In every iteration the present result is better than the previous results, and then the present detail is stored, otherwise, it will be neglected [18].

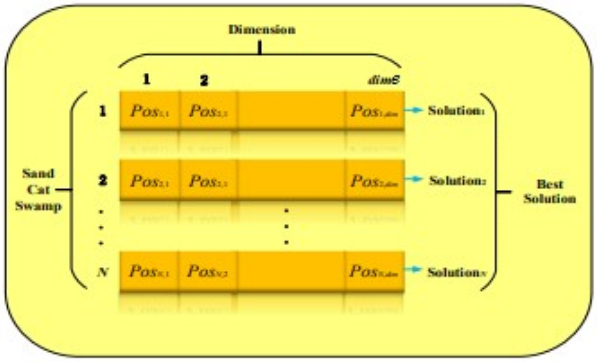


Fig 2. Structure of the problem solution

ii. Prey Searching (Stage of exploration)

The sand cat position can be represented as Pos. The benefit of using the algorithm of Sand Cat Swarm Optimization methodology is that it has the capacity of hearing at very low detection frequency [19]. Every cat in the sand can identify the very low frequency that may be below 2 KHz. The following equation 1 represents the mathematical formula of sensitivity y_H.

Here the range of sensitivity is from 2 to 0 KHz. Additionally, the parameter value of B is created based on mathematical expression 2; also, the methodology of exploitation and exploration ability is controlled [20].

$$Y_H = S_M - \left(\frac{S_M \times l}{T}\right) \quad (1)$$

$$B = 2^{x} Y_H \times \text{rand}(0,1) - Y_H \quad (2)$$

Here, S_M is 2, l is the present iteration, and T represents the maximum iteration. Every cat in the sand chooses a completely new area within its range of sensitivity while prey searching. This will be very conducive for the algorithm's exploitation. The following formula represents the sensitivity range ($\mathbf{Y}$) of every sand cat [21].

$$Y = Y_H + \text{rand}(0,1) \quad (3)$$

Here γ_H is utilized for the parameter of guidance γ. Every sand cat will identify the prey position based on the optimal position of the candidate (Pos_{BC}), range of sensitivity (γ), and the present position ($Pos_{PC}(t)$) [22]. The following mathematical expression represents the prey position.

$$Pos(l+1) = \gamma^{x}\left(Pos_{BC}(t) - rand\,(0,1)^{x} Pos_{PC}(t)\right) \quad (4)$$

iii. Prey attack (Stage of exploitation)

The following mathematical expression 5 represents the sand and prey distance (Pos_{rmd}). Considering the sand cat range of sensitivity is circle and movement direction utilizes the selection methodology of Roulette Wheel, to choose an angle of random (α). The random angle is between 0° to 360°, it's maybe -1 to 1 [23]. In this manner, every cat in the sand can move forward in several distance circumferences in the search reference area. The following diagram in figure 3 shows the mechanism of area update and sand cat position of the current and previous iterations. The following mathematical expression 6 shows the pray attack in the search area.

$$Pos_{ruv} = |rand\,(0,1)^{x} Pos_{B}(t) - Posc(l)| \quad (5)$$

$$Pos(l+1) = Pos_{B}(l) - \gamma^{x} Pos_{ruv}{}^{x} \cos(\alpha) \quad (6)$$

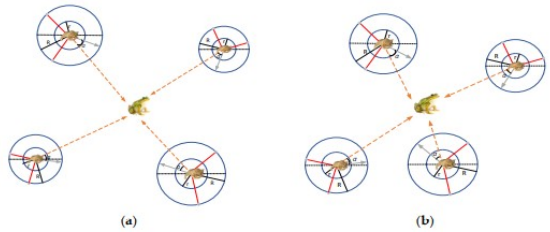


Fig 3: The mechanism of area update and sand cat position of current and previous iteration

iv. Algorithm of Sand Cat Swarm Optimization Algorithm (SCSO)

The algorithm of SCSO regulates both the exploration and exploitation of the methodology based on the parameter values γ_H and B. The parameter value is between 2 and 0. So, the adaptive parameter B is [-4, 4] random parameter value. While the random parameter value B is low i.e. γbelow the value of 1, then the cat in the sand will attack the prey [24]. When the value of parameter B is greater than one, then the cat in the sand will search for the prey. The following equation 7 represents the prey attack and prey search.

$$Pos(l+1)\begin{cases} \gamma^{x}(Pos_{BC}(l) - rand\,(0,1)^{x} Posc\,(l)) & |B| > 1; exploration \\ Pos_{B}(l) - Pos_{ruv}{}^{x} \cos(\alpha)^{x} \gamma & |B| < 1; exploitation \end{cases} \quad (7)$$

v. Sand Cat Swarm Optimization Algorithm Pseudo Code

Population is initialized

The fitness function is computed related to the function of the objective

γ, н, and B are initialized

While (l ≤ highest value of iteration)

For every agent of search obtain an angle of random related to the algorithm Roulette wheel (0° ≤ α ≤ 360°)

If (also (B)>t)

Change the position of the searching agent related to the mathematical equation (4)

Else

Search agent position update by using the formula (6)

End

T= l +1

End

3.6. Updated Sand Cat Swarm Optimization (USCSO)

i. Phase of initialization

During the initialization phase, the population size is assigned as M, dimension dime, and number of iterations T. The population initialization is done by using the following mathematical expression 8 [25].

$$Pos_{\chi,\gamma} = (ul_{\chi} - ll_{\chi})^{x} rand + lb_{\chi} \quad (8)$$

Here ul_{χ} represents the upper limit of x identity in the y dimension, ll_{χ} represents the upper bound of x identity in the y dimension and the value of rand represents the numbers in between 0 and 1.

ii. Prey search

The behavior of hunting sand cats is based on the adaptive parameter B. If the value of parameter B is less than one, then the cat in the sand attacks the prey. If the value of parameter B is greater than one, then the cat in the sand will search for the prey [26].

iii. Strategy of Triangle Search (STS)

While penetrating for prey the sand cat, the sand cat cannot only search for its range of sensitivity. By using the strategy of triangle search, the cat in the sand can select the angle of walking to get a new location [27]. The strategy of triangle search will be computed by utilizing the following mathematical equation 9.

$$Pos_{new} = Pos_{a}(t) = r \times P \quad (9)$$

iv. Prey attack

Considering the sand cat range of sensitivity is circle and movement direction utilizes the selection methodology of Roulette Wheel, to choose an angle of random (α). The angle of random is between 0° to 360°, it's maybe -1 to 1 [28]. In this manner, every cat in the sand could move forward in several distance circumferences in the search area.

v. The strategy of levy flight search (SLFS)

While attacking the prey, the solution is very close to the sand cat, which leads to concentrating on the low optimum solution and it is not possible to get good results. So, the strategy of levy flight search can present a method of walking that conform the distribution of levy and creates the sand cat high mobile [29]. The strategy of levy flight search will be computed by utilizing the following mathematical equation 10.

$$Pos_{ted} = pos_a(\quad) + (pos_a(\quad) - pos_a(\quad)) \times D \times \text{Levy} \quad (10)$$

vi. Opposition of Lens Related to Learning (OLRL)

To augment the competence of exploration of USCSO methodology, OLRL is included to enhance the common competence of exploration methodology while changing the area, as described in equation 9. The following diagram in figure 4 represents the range of search extended by creating a reverse position related to the present coordinates. While considering the 2D coordinates, the range of search will be (a, b) on the x-axis, and the convex lens is represented by the y-axis. If the object projection A is x on the x-axis and *h* is height [30].

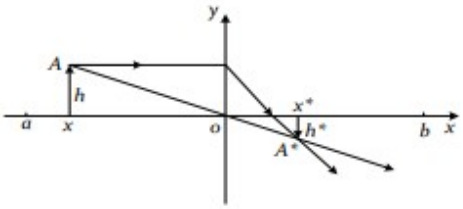


Fig 4: Opposition of Lens Related to Learning Algorithm

In figure 4, x takes the value of 0 as the point of base to get the related reverse point $_{\chi}\star$, which can be created from the principle called lens imaging.

$$K_{\chi}\star = \frac{a_{\chi} + b_{\chi}}{2} + \frac{a_{\chi} + b_{\chi}}{2t} - \frac{K_{\chi}}{t} \quad (11)$$

vii. Changing the position of the population

Based on the value of fitness the area is updated. While the value of fitness is good then the individual of the original will be changed. If the value of the fitness is bad, then the individual of the original will not be changed [31]. The following diagram in figure 5 represents the flow diagram of Updated SCSO.

viii. Updated Sand Cat Swarm Optimization Algorithm Pseudo Code

Population is initialized based on the formula (8)
The function of fitness is calculated based on the function of objective
Y, R and B are initialized
While (≤ highest value of iteration)
For every agent of search
Obtaining angle of random related to algorithm
Roulette wheel (0° ≤ α ≤ 360°)
If (abs (B)>t)
Change the position of search agent related to the mathematical equation (4)
Using the formula (9) to get a new position
Else
Search agent position update by using the formula (6)
Using the mathematical equation (10) to get a new position
End
Computing the Opposition of Lens Related to Learning by using the formula (11)
T= +1
End

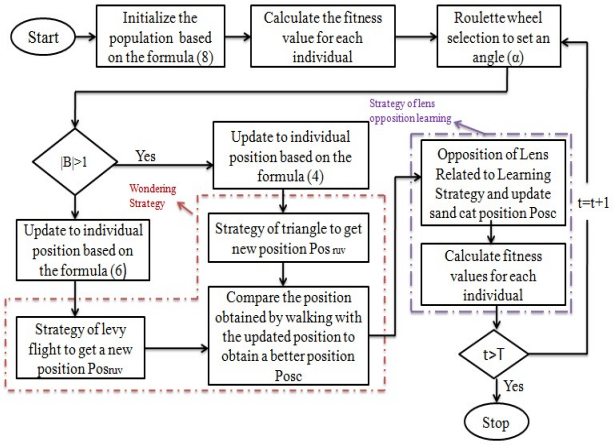


Fig 5: Updated Sand Cat Swarm Optimization Algorithm

4. Experimental Results

We conducted many experiments to check the efficiency of our system with the existing system. While doing experiments on our system we found that our system is more accurate and easier to implement. The important thing here is we found that our system is well-suited for practical use. The values of accuracy, recall, f1-score, and precision are high compared to other existing systems [32]. The following table shows the values of accuracy, recall, f1-score, precision, and support during the experiment.

Table 1: Accuracy, recall, f1-score, precision, and support factors

	Precision	Recall	F1- Score	Support	Accuracy
0	0.96	0.97	0.92	17096	0.98
1	0.97	0.98	0.95	15201	0.99

The following diagram in figure 6 represents the confusion matrix of the experiment. Here we used the 17097 malware dataset, because of the high accuracy of the suggested system it predicted 17096 datasets correctly. Only one is a wrong prediction. For ransomware we used 15403 datasets, because of the high prediction capacity of the newly developed system, this system predicted 15401 samples correctly only two were the wrong predictions. The following figure 7 represents the Performance Matrix competition of the suggested system; here the performance of the proposed system is high compared to other existing systems. The following diagram in figure 8 represents the TPR and FPR Comparison of the proposed system. Here the TPR and FPR results are high in the proposed system when compared to other existing systems. The following figure 9 represents the ROC curve with the Accuracy Point of the proposed system. In our proposed system the false positive rate is low compared to another system. If the system produces high accuracy in true positive, this means that the system produces good quality output. We already saw in the confusion matrix that the false positive rate is low and the true positive rate is high.

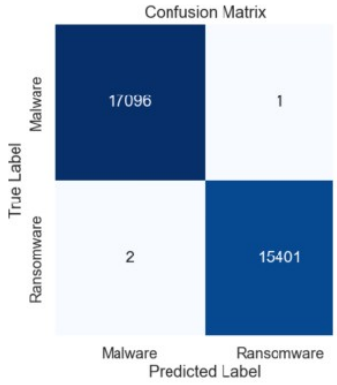


Fig 6: Confusion Matrix of the newly developed system

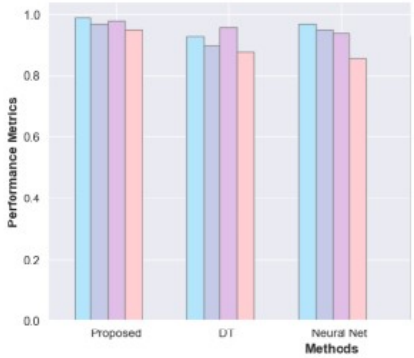


Fig 7: Performance Matrix competition of the proposed system

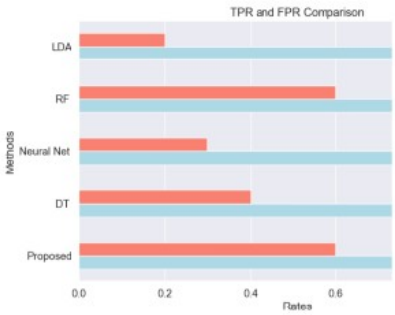


Fig 8: TPR and FPR Comparison of the proposed system

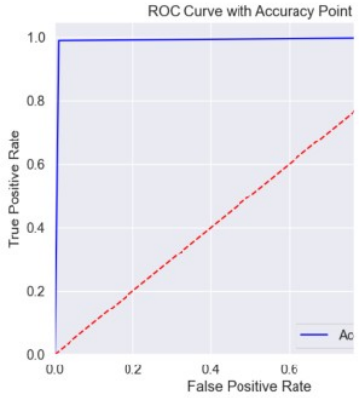


Fig 9: ROC curve with Accuracy Point of the proposed system

The proposed system was compared with existing approaches, and the results demonstrated that it consistently outperformed them, achieving excellent performance. The following diagram figure 10 represents the comparison result of the existing system and the proposed system. While calculating the values of sensitivity, precision, and accuracy, some existing systems were best in any one of the mentioned categories. However, the proposed system produced good results in all categories.

The temporal convolution network is the common convolution network, but the speed of execution is high when comparing other convolution networks. So, the proposed system is fast compared to other existing systems. Also, we used SCSO, and for optimization purposes, the accuracy of the system was increased. We got good accuracy in a very short time. Here we received 99 % accuracy while executing our system. The false positive rate is very low compared to other existing systems. Some existing systems may produce 85% of accuracy and also the false positive rate is high. Also, we found that our system is well suited for practical use.

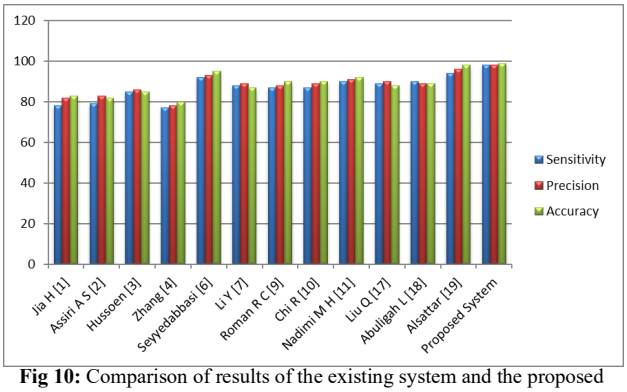
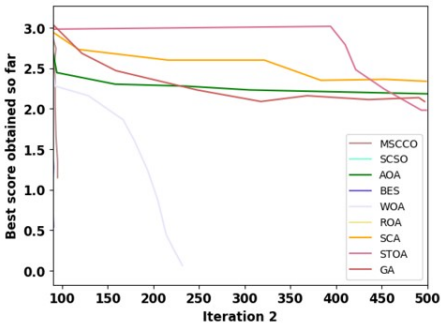
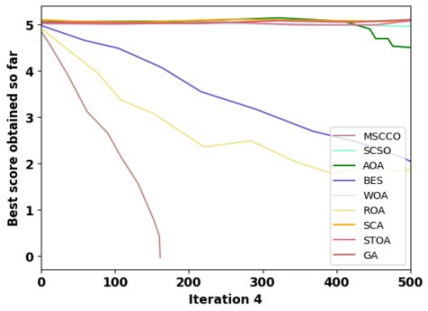
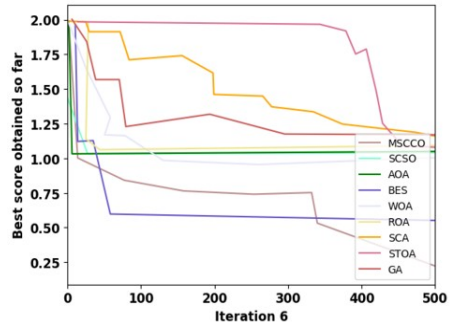


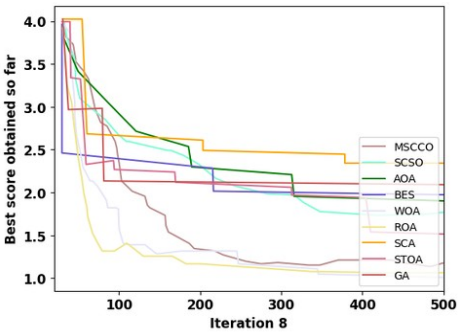
Fig 10: Comparison of results of the existing system and the proposed system.

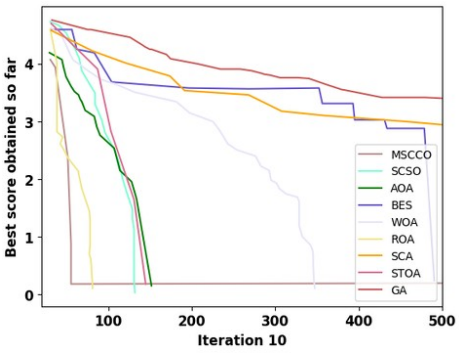
While doing optimization we used the SCSO algorithm, in the detection of malware and ransomware, the SCSO is best and well-suited compared to other optimization algorithms. The SCSO algorithm was compared with several existing optimization algorithms, and it achieved competitive results within a significantly shorter time frame. In every iteration, the score of SCSO is high compared to other optimization algorithms. The following diagram figure 11 represents the curves of convergence for the algorithm of SCSO for ordinary benchmark functions (F1-F12) with dim=500.











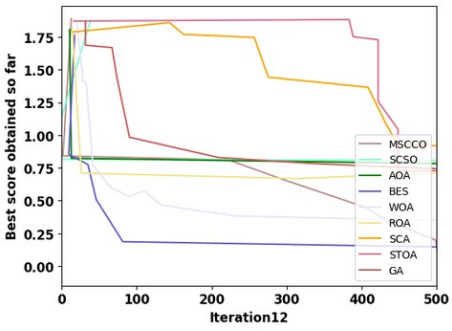


Fig 11: Convergence curves for the typical benchmark functions (F1–F12) method with dim=500

The CatBoost-based classification approach was compared with several existing methodologies, and it demonstrated superior performance across the evaluated metrics. CatBoost methodology has a unique feature called ordered encoding which increases the accuracy and other

quality checking parameters. Also, the CatBoost algorithm has a unique characteristic that it utilizes the concept of a symmetric tree. This shows that at each level of depth, all the nodes of the decision tree use the unique split situation. Because of this unique character, it detects malware and ransomware quickly and accurately compared to other techniques. The following table shows the comparison results of CatBoost and some other existing technologies.

Table 2: Comparison with some other existing methodologies

Approaches	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
MCFT and CNN	96.54	95.01	95.59	97.02
RMVC	96	-	-	-
ML and VT	95.68	-	-	-
MDMC	96.58	-	-	-
SERLA	98.91	94.78	96.65	97.59
RCNF	98.28	-	-	97.46
XGBoost	95.57	96.24	95.89	95.28
LightGBM	98.26	98.65	97.26	95.38
ACO-DT	99.12	-	-	-
CNN and BILSTM	98.24	-	-	97.59
XGBoost and RNN	95.48	-	-	-
HYDRA	96.24	-	-	97.25
CatBoost	99.56	99.24	99.89	99.86

5. Conclusion

The massive growth and development of malware and ransomware methodologies have established the categorization of malware and ransomware as a prominent topic. Many currently active malware and ransomware methodologies are a prominent topic. Many currently active malware and ransomware methodologies are there, which may concentrate on redundancy and may lead to maximum overhead of memory and complexity of computation. Also, many existing models of classification are not interpretable highly; they are not practical for the research and analysis of ransomware and malware.

A novel approach was developed by integrating the Sand Cat Optimization Algorithm, the CatBoost algorithm for classification, and a Temporal Convolutional Network (TCN) for feature extraction. Two distinct datasets were utilized—one for malware and the other for ransomware. This hybrid model enables the system to achieve high processing speed and strong interpretability, effectively identifying both ransomware and malware threats. Future research will focus on further enhancing the model by balancing the trade-off between accuracy and computational efficiency.

References

[1] Jia, H.; Peng, X.; Lang, C. Remora optimization algorithm. Expert Syst.Appl.2021,185,115665.
[2] Assiri, A.S.; Hussien, A.G.; Amin, M. Ant lion optimization: Variants, hybrids, and applications. IEEE Access 2020, 8, 77746–77764.
[3] Hussien, A.G.; Amin, M.; Abd El Aziz, M. A comprehensive review of moth-flame optimisation: Variants, hybrids, and applications. J. Exp. Theor. Artif. Intell. 2020, 32, 705–725.
[4] Hatamlou, A. Black hole: A new heuristic optimization approach for data clustering. Inform. Sci. 2013, 222, 175–184.
[5] Zhang, Y.; Jin, Z. Group teaching optimization algorithm: A novel metaheuristic method for solving global optimization problems. Expert Syst. Appl. 2020, 148, 113246.
[6] Seyyedabbasi, A.; Kiani, F. Sand Cat swarm optimization: A nature-inspired algorithm to solve global optimization problems. Eng. Comput. 2022, 1–25.
[7] Li, Y.; Wang, G. Sand Cat Swarm Optimization Based on Stochastic Variation With Elite Collaboration. IEEE Access 2022, 10, 89989–90003.
[8] Jovanovic, D.; Marjanovic, M.; Antonijevic, M.; Zivkovic, M.; Budimirovic, N.; Bacanin, N. Feature Selection by Improved Sand Cat Swarm Optimizer for Intrusion Detection. In Proceedings of the 2022 International Conference on Artificial Intelligence in Everything (AIE), Lefkosa, Cyprus, 2–4 August 2022; pp. 685–690. Mathematics 2022, 10, 4350 40 of 41
[9] Roman, R.C.; Precup, R.E.; Petriu, E.M. Hybrid data-driven fuzzy active disturbance rejection control for tower crane systems. Eur. J. Control 2021, 58, 373–387.
[10] Chi, R.; Li, H.; Shen, D.; Hou, Z.; Huang, B. Enhanced P-type Control: Indirect Adaptive Learning from Set-point Updates. IEEE Trans. Autom. Control 2022.
[11] Nadimi-Shahraki, M.H.; Taghian, S.; Mirjalili, S.; Faris, H. MTDE: An effective multi-trial vector-based differential evolution algorithm and its applications for engineering design problems. Appl. Soft Comput. 2020, 97, 106761.
[12] Hussien, A.G. An enhanced opposition-based salp swarm algorithm for global optimization and engineering problems. J. Ambient. Intell. Humaniz. Comput. 2022, 13, 129–150.
[13] Zhang, H.; Wang, Z.; Chen, W.; Heidari, A.A.; Wang, M.; Zhao, X.; Liang, G.; Chen, H.; Zhang, X. Ensemble mutation-driven salp swarm algorithm with restart mechanism: Framework and fundamental analysis. Expert Syst. Appl. 2021, 165, 113897.
[14] Nadimi-Shahraki, M.H.; Taghian, S.; Mirjalili, S. An improved grey wolf optimizer for solving engineering problems. Expert Syst. Appl. 2021, 166, 113917.
[15] Zheng, R.; Jia, H.; Abualigah, L.; Wang, S.; Wu, D. An improved remora optimization algorithm with autonomous

foraging mechanism for global optimization problems. Math. Biosci. Eng. 2022, 19, 3994–4037.
[16] Nadimi-Shahraki, M.H.; Taghian, S.; Mirjalili, S.; Ewees, A.A.; Abualigah, L.; AbdElaziz, M. MTV-MFO: Multi-Trial Vector-Based Moth-Flame Optimization Algorithm. Symmetry 2021, 13, 2388.
[17] Liu, Q.; Li, N.; Jia, H.; Qi, Q.; Abualigah, L. Modified remora optimization algorithm for global optimization and multilevel thresholding image segmentation. Mathematics 2022, 10, 1014.
[18] Abualigah, L.; Diabat, A.; Mirjalili, S.; Elaziz, M.A.; Gandomi, A.H. The arithmetic optimization algorithm. Comput. Methods Appl. Mech. Eng. 2021, 376, 113609.
[19] Alsattar, H.A.; Zaidan, A.A.; Zaidan, B.B. Novel meta-heuristic bald eagle search optimisation algorithm. Artif. Intell. Rev. 2020, 53, 2237–2264.
[20] Rao, H.; Jia, H.; Wu, D.; Wen, C.; Liu, Q.; Abualigah, L. A Modified Group Teaching Optimization Algorithm for Solving Constrained Engineering Optimization Problems. Mathematics 2022, 10, 3765.
[21] Laith, A.; Dalia, Y.; Mohamed, A.E.; Ahmed, A.E.; Mohammed, A.A.A.; Amir, H.G. Aquila Optimizer: A novel meta-heuristic optimization algorithm. Comput. Ind. Eng. 2021, 157, 107250.
[22] Abualigah, L.; Elaziz, M.A.; Sumari, P.; Zong, W.G.; Gandomi, A.H. Reptile search algorithm (RSA): A nature-inspired metaheuristic optimizer. Expert Syst. Appl. 2021, 191, 116158.
[23] Wen, C.; Jia, H.; Wu, D.; Rao, H.; Li, S.; Liu, Q.; Abualigah, L. Modified Remora Optimization Algorithm with Multistrategies for Global Optimization Problem. Mathematics 2022, 10, 3604.
[24] Hayyolalam, V.; Kazem, A.A.P. Black widow optimization algorithm: A novel meta-heuristic approach for solving engineering optimization problems. Eng. Appl. Artif. Intell. 2020, 87, 103249.
[25] Song, M.; Jia, H.; Abualigah, L.; Liu, Q.; Lin, Z.; Wu, D.; Altalhi, M. Modified Harris Hawks Optimization Algorithm with Exploration Factor and Random Walk Strategy. Comput. Intell. Neurosci. 2022, 2022, 23.
[26] Faramarzi, A.; Heidarinejad, M.; Mirjalili, S.; Gandomi, A.H. Marine predators algorithm: A nature-inspired metaheuristic. Expert Syst. Appl. 2020, 152, 113377. Mathematics 2022, 10, 4350 41 of 41
[27] Houssein, E.H.; Neggaz, N.; Hosney, M.E.; Mohamed, W.M.; Hassaballah, M. Enhanced Harris hawks optimization with genetic operators for selection chemical descriptors and compounds activities. Neural Comput. Appl. 2021, 33, 13601–13618.
[28] Wang, S.; Sun, K.; Zhang, W.; Jia, H. Multilevel thresholding using a modified ant lion optimizer with opposition-based learning for color image segmentation. Math. Biosci. Eng. 2021, 18, 3092–3143.
[29] Said, V.; Eelly, E.; Zag, E.; Murat, O. The Dangerous Combo: Fileless Malware and Cryptojacking. J. SoutheastCon 2022, 125–132.
[30] Rizvi, S.K.J.; Aslam, W.; Shahzad, M.; Saleem, S.; Fraz, M. PROUD-MAL: Static analysis-based progressive framework for deep unsupervised malware classification of windows portable executable. Complex Intell. Syst. 2022, 8, 673–685.
[31] Johnson, S.; Gowtham, R.; Nair, A.R. Ensemble Model Ransomware Classification: A Static Analysis-based Approach. Inventive Comput. Inf. Technol. 2022, 336, 153–167.
[32] Loi, N.; Borile, C.; Ucci, D. Towards an Automated Pipeline for Detecting and Classifying Malware through Machine Learning. 2021. Available online: https://arxiv.org/abs/2106.05625 (accessed on 5 December 2022).