Complex Proportional Assessment Based Neutrosophic Approach for Ransomware Detection in Cybersecurity IoT System

Louai A. Maghrabi[1,*]

[1]Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia
Email: l.maghrabi@ubt.edu.sa

Abstract

A neutrosophic set (NS) is an advanced computational technique that accesses uncertain information via three membership functions. A soft expert set (SES) is derived from the hypothesis of a "soft set" with computer technology. Currently, this method is utilized in various domains such as intelligent systems, measurement theory, probability theory, cybernetics, game theory, and so on. Internet user faces a myriad of risks with the development of malware worldwide. The most prominent type of malware, Ransomware, encrypts confidential data without releasing the files until the user makes a ransom payment. Internet of Things (IoT) framework is a wide region of Internet-related devices with further computation capacities with storage capabilities that can be damaged by malware creators. Ransomware is a cruel and new malware on Internet with increasing attack levels. Ransomware encrypts the whole information to make users incapable of accessing important information and their files. In this article, we propose a Complex Proportional Assessment Based Neutrosophic Approach for Ransomware Detection in Cybersecurity (CPABNA-RDCS) methodology in IoT environment. The objective of the CPABNA-RDCS approach is to identify and categorize the ransomware to accomplish cybersecurity in the IoT network. Primarily, the CPABNA-RDCS method exploits min-max normalization for scaling the input dataset into relevant format. Meanwhile, the ransomware classification takes place via Complex Proportional Assessment Based Neutrosophic (CPABN) method. Finally, grey wolf optimizer (GWO) is employed for optimum hyperparameter choice of the CPABN system. The experimental results of the CPABNA-RDCS method are inspected on benchmark data. The simulation analysis emphasized the developments of the CPABNA-RDCS method over other existing techniques.

Keywords: Ransomware Detection; Grey Wolf Optimizer; Neutrosophic Set; Complex Proportional Assessment; Cybersecurity; Soft Expert Set

1. Introduction

Neutrosophic Logic (NL) is a bairn training field in that all proposition is valued to have the proportions (percentage) of fact considering sub-set T, percentage of uncertainty with a sub-set I, and percentage of falseness with a sub-set F [1]. Neutrosophic set (NS) is successfully applied for data processing and determines benefits for dealing with the uncertain evidence of data, also still requires a method encouraged for data scrutiny and classification applications. NS delivers a well-organized and precise way to describe unbalanced data based on the features of the data [2]. The Internet of Things (IoT) is designed to connect the manual device. The IoT device contains normal objects from day-to-day life that communicate with one another to make it easier for human life. Owing to botnet, DDoS, ransomware, and malware attacks on IoT devices, the security of IoT has been in the news in recent times [3]. The latest editions of ransomware have been everywhere for two years and recently have posed a large risk for IoT too. Ransomware is a mixture of ransom and malware. It encodes the private records of victims and marks those useless, allowing them to decrypt and deliver the documents once a ransom is compensated to the ransomware creators [4]. The invader via credit card or crypto-currency requests for the compensation of ransom. Ransomware assaults have become more powerful and it is tough to develop prohibition methods. IoT devices, that previously had weak safety profiles, are simple goals for ransomware invaders. It enters into targets via phishing, spam, malware, or social engineering [5].

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

Meanwhile, Ransomware assaults are unalterable once they reach a deadline, this may outcomes in higher losses in systems consisting of laptops and computers [6]. The smooth health of IoT is also the critical goal of ransomware, any delays in the payments of ransom may outcomes in the loss of human lives while the attackers take control of some devices. Similarly, ransomware could strike IoT devices related to each other fields and force the victims to pay fees on time [7]. Machine learning (ML) and deep learning (DL) have impacted all sides of life. These techniques have many uses in each area due to the capability of decision-making. This too finds many applications in computing and development in cybersecurity [8]. Advanced assaults and risk recognition have become simple in less time because of the use of these particular possible techniques. DL is the topmost for detecting the designs of an enduring tool [9]. Due to its pattern acknowledgment capability, it discovers applications in various fields, i.e., security, medical, entertainment, and AI. ML and DL techniques are successful methods and are extremely applied in the progressive study of cyber security. These techniques are applied in the area of ransomware recognition [10].

In this article, we propose a Complex Proportional Assessment Based Neutrosophic Approach for Ransomware Detection in Cybersecurity (CPABNA-RDCS) method in IoT environment. The objective of CPABNA-RDCS approach is to identify and categorize the ransomware to accomplish cybersecurity in IoT network. Primarily, the CPABNA-RDCS method exploits min-max normalization for scaling the input dataset into relevant format. Meanwhile, the ransomware classification takes place via Complex Proportional Assessment Based Neutrosophic (CPABN) method. Finally, grey wolf optimizer (GWO) is employed for optimum hyperparameter choice of the CPABN system. The experimental results of the CPABNA-RDCS method are inspected on benchmark data.

2. Literature Review

Mofidi et al. [11] proposed a lightweight IDS (L-IDS). While combining multi-layer control, hardware-improved TEE namely TrustZone, by ML Methods. L-IDS could effectually identify to reduce ransomware attacks in internal IoT models with lower resources related to conventional security scan techniques. By combining the TEE, and L-IDS improves the protection and security of IoT devices, whereas ML methods aid in identifying ransomware attacks accurately and effectively. The authors [12] introduced an Optimum Graph CNN Ransomware Detection (OG-CNNRWD) approach for cybersecurity in IoT. The GCNN method is utilized for the ransomware identification and its parameters are selected by the harmony search algorithm (HSA) method. Singh et al. [13] develop a novel methodology for RaaS attack recognition that utilizes the ensemble of DL methods. In the early stage, exponential linear unit-, scaled, and the ReLU-based 3 single MLP methods are improved. Then, utilizing the integrated predicting power of these 3 MLPs, the RansoDetect Fusion ensemble method is proposed in the recommended method.

Ahanger et al. [14] utilized the ML methods to improve ransomware defense in IoT devices operating on the Pure OS. The method also established a ransomware detection method through ML that integrates the ElasticNet and XGBoost methods in a fusion method. The implementation and design of the method are based on the estimations for several current ML methods. Gazzan and Sheldon [15] proposed an Uncertainty-Aware Dynamic Early Stopping (UA-DES) method for enhancing DBN in ransomware recognition. UA-DES levers an active learning methods, dropout methods, and Bayesian techniques for adjusting the dynamical amount of epochs through the training of the recognition method. The technique combines calibration quality measures and uncertainty, by improving the training method for well-precise ransomware recognition. Zewdie et al. [16] researched in what way malware attack, particularly ransomware attacks, uses IoT devices. The method also highly surveys various ML outcomes. The technique also concentrated on what way the ML results identify the malicious events, for example, a ransomware attacks on IoT-connected networks. The method used RF and DT classification methods.at last, an ML recognition method is presented.

3. The Proposed Model

In this study, we have developed a CPABNA-RDCS methodology in IoT environment. The CPABNA-RDCS methodology purposes to identify and categorize the ransomware to achieve cybersecurity in the IoT network. The CPABNA-RDCS method comprises min-max normalization, CPABN-based classification, and GWO-based hyperparameter tuning processes as demonstrated in Figure 1.

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

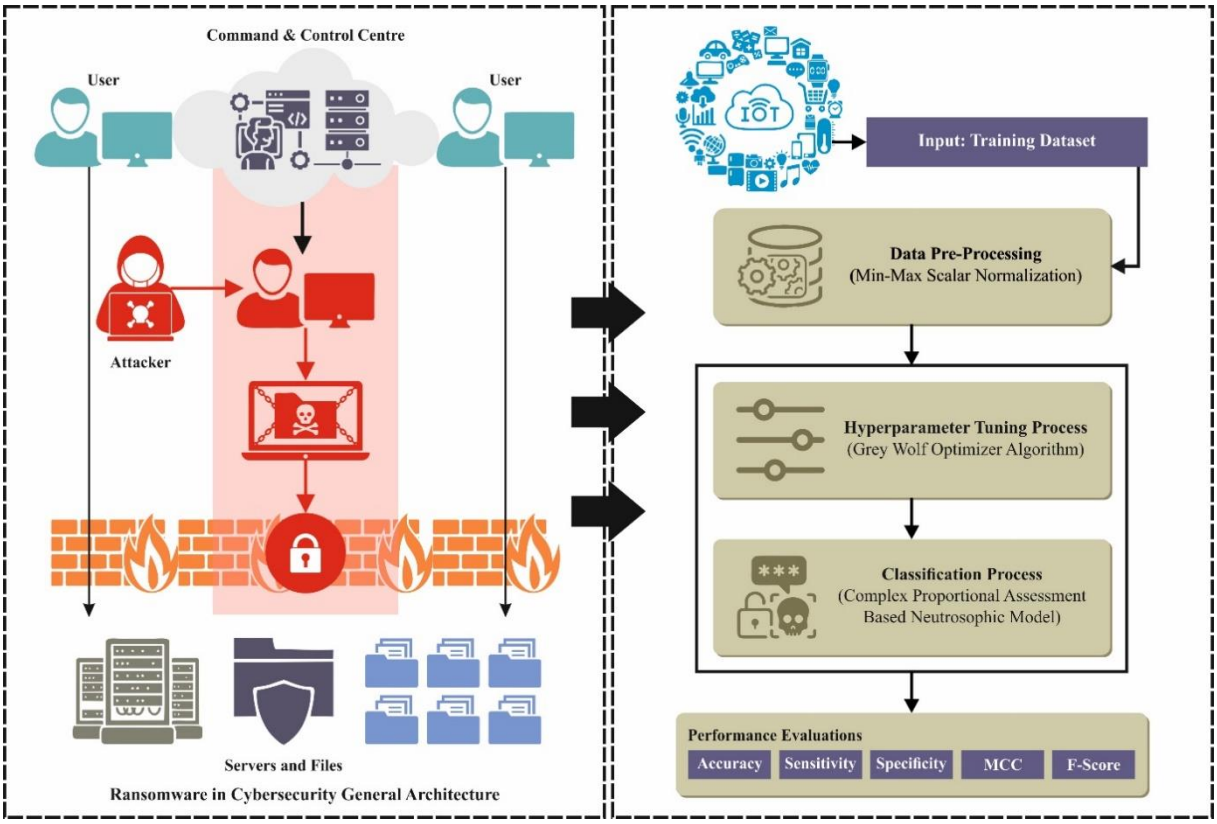

Figure 1. Overall process of CPABNA-RDCS technique

A. Data Normalization

Primarily, the CPABNA-RDCS method exploits min-max normalization for scaling the input dataset into relevant format. Min-max normalization is a data preprocessing method deployed in ransomware recognition for cybersecurity IoT networks to measure features between a maximum and minimum interval of 0 and 1 [17]. This technique improves the machine learning performance by ensuring that the feature equally contributes towards the examination, which prevents features with large range from controlling the outcomes. By normalizing information, the model can more efficiently recognize abnormal behaviors symptomatic of ransomware attacks, optimizing the performance and effectiveness of risk identification in IoT networks.

B. Ransomware Detection using CPABN Model

Meanwhile, the ransomware classification takes place via CPABN method. Before analyzing the neutrosophic decision matrix, it is necessary to determine the NS being examined [18]. The NS is defined in the following: truth ϑ, indeterminacy η, and falsity (δ) of x in Q, correspondingly, and the images constitute a non-standard or standard subset [0,1]. The single value NS Q over X is given as $l = \{\langle x, \vartheta_A(x), \eta_A(x), \delta_A(x)\rangle : x\varepsilon X\}$.

Where $\vartheta_A(x), \vartheta_A, \eta_A(x)$ meet the conditions $\eta_A(x), \delta_A(x)0 \leq, , \delta_A(x) \leq 3$ for $x \in X$. Thus, h, i, and j are the neutrosophic values for modeling the CPABN method. $h = \vartheta_A(x)$ for truth degree, where $\in \{0,1\}$.

$i = \eta_A(x)$ for indeterminacy degree, where $\in \{0,1\}$.

$j = \delta_A(x)$ for falsity degree, where $\in \{0,1\}$.

Therefore, the neutrosophic values are defined as $= (h, \mathrm{i}, j)$, where $h, \mathrm{i}, j \in \{0,1\}$ and meets the criteria $0 \leq h + i + j \leq 3$. Hence, the score function B can be determined.

CPA is a Complex Proportional Assessment of System" and a mathematical model is applied in decision-making, where the weights are assigned to classify and rank additional choices. It assesses and chooses probabilities in complex situations where the factors and criteria must be taken into account. To determine the decision component within the NS, the CPABN method can be chosen to enable the evaluation and selection of another possibility in uncertain and more complex conditions. Consequently, it measures which decision is the better and envisages the relationship with dependence on other selections.

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

The modeling of CPABN technique is given below:

Define another possibility and conditions: Define the relative alternates and the benchmark that is evaluated and compared.

Allocate weight to the conditions: Detect the applicable criterion weights to reflect the importance of the making decisions.

Alternative assessments: The alternatives are evaluated for each condition and a scores are estimated.

Score normalization: The scores are normalized to ensure all the alternatives are similar.

Calculation of the relationship rules: It fuses the normalized scores and the weights of the condition to calculate the final score for each alternative.

Rank the alternative: The alternatives are ranked based on the last score to determine the best option.

The CPABN method selects the best alternatives by considering the better and worst solutions, in a step-by-step assessment and computation of the alternatives for the importance, indeterminacy, dependence, and degree of utility. The steps of CPABN technique are as follows:

Step 1: Calculation of the regularized decision matrix l_{ij}^{*}, based on the following equation.

$$l_{ij}^{*} = \frac{l_{ij}}{\sum_{i=1}^{m} l_{ij}} \tag{1}$$

Step 2: Determine the weight decision matrix D_{hij}:

$$D_{hij} = x_{hij}^{*} \cdot w_{hj}$$

$$= [w_{h1}l_{11}w_{h2}l_{12}, \dots, w_{h1}l_{1n}w_{h1}l_{21}w_{h2}l_{22}, \dots, w_{h2}l_{2n} \vdots \ddots \vdots w_{h1}l_{m1}w_{h2}l_{m2}, \dots, w_{hn}l_{mn}] \tag{2}$$

Where l_{ij}^{*} is the normalized neutrosophic value of i_{th} alternatives in j_{th} condition and w_{hj} shows the weight associated with the j_{th} criterion.

Step 3: S_{i+} and S_{i-} sum of the weight values assessed for non-beneficial (NB) and beneficial (B) conditions.

$$S_{i_{i+}} = \sum_{k=1}^{k} D_{hij} \tag{3}$$

$$S_{i_{i-}} = \sum_{k=1}^{k} D_{hij} \tag{4}$$

Step 4: Define the comparative prominence of Q_i alternative as follows.

$$Q_i = S_i + \frac{\Sigma_{j=1}^{m} S_i}{s_{i-} \Sigma_{j=1}^{m} \frac{-1}{s_{i-}}} \tag{5}$$

The Q_i of alternative shows the satisfaction degree attained.

Step 5: Assessment of the assessment matrix P_i:

$$P_i = \frac{Q_i}{Q_{\max}} \cdot 100 \tag{6}$$

In Eq. (6), Q_{max} is the high value of relation significance. P_{hi} attains a comprehensive ranks of the candidate alternatives. Temporarily, the CPABN technique fuses criteria and weights to evaluate and select another possibility in multifaceted decision-making conditions.

C. Hyperparameter Tuning using GWO

Finally, GWO is employed for optimum hyperparameter choice of the CPABN method. GWO is a new metaheuristic optimization technique stimulated by the natural behavior of grey wolves for improving ML algorithm [19]. The GWO follows the hunting activities and hierarchy power of wolf. Especially, a swarm of grey wolves is split into alphas (α), beta (β), delta (δ), and omega (ω) where responsibility and power of all the groups are not similar. $\alpha, \beta,$ and δ are the three better solutions for modelling the social nature of wolves, correspondingly.

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

The searching, encircling, and attacking prey are the three different strategies of GWO. The hunting strategy is led by α, β, and δ. Prey encirclement was implemented by upgrading the wolf location. Three of them were used for predicting the prey position whereas the omega location is randomly updated surrounding the three optimum wolves as follows:

$$\vec{X}(t+1) = \vec{X}(t) - \vec{A} \cdot \left|\vec{C} \cdot \vec{X}_p(t) - \vec{X}(t)\right| \quad (7)$$

$$\vec{A} = 2\vec{a} \cdot \vec{r}_1 - \vec{a} \; and \; \vec{C} = 2 \cdot \vec{r}_2 \quad (8)$$

$$\vec{X}_1 = \vec{X}_\alpha - \vec{A}_1 \cdot \vec{D}_\alpha, \vec{D}_\alpha = \left|\vec{C}_1 \cdot \vec{X}_\alpha - \vec{X}\right| \quad (9)$$

$$\vec{X}_2 = \vec{X}_\beta - \vec{A}_2 \cdot \vec{D}_\beta, \vec{D}_\beta = \left|\vec{C}_2 \cdot \vec{X}_\beta - \vec{X}\right| \quad (10)$$

$$\vec{X}_3 = \vec{X}_\delta - \vec{A}_3 \cdot \vec{D}_\delta, \vec{D}_\delta = \left|\vec{C}_3 \cdot \vec{X}_\delta - \vec{X}\right| \quad (11)$$

$$\vec{X}(t+1) = \frac{\vec{X}_1 + \vec{X}_2 + \vec{X}_3}{3} \quad (12)$$

Whereas, $\overrightarrow{A}$ and $\vec{C}$ defines the coefficient vectors; the location vector of wolf at $(t+1)$ iteration is $\vec{X}(t+1)$; a position vector of prey at t iteration is $\vec{X}_p(t)$; $\vec{a}$ are dropped from 2 to 0; $\vec{r}_1$ and $\vec{r}_2$ are random vectors of [0,1].

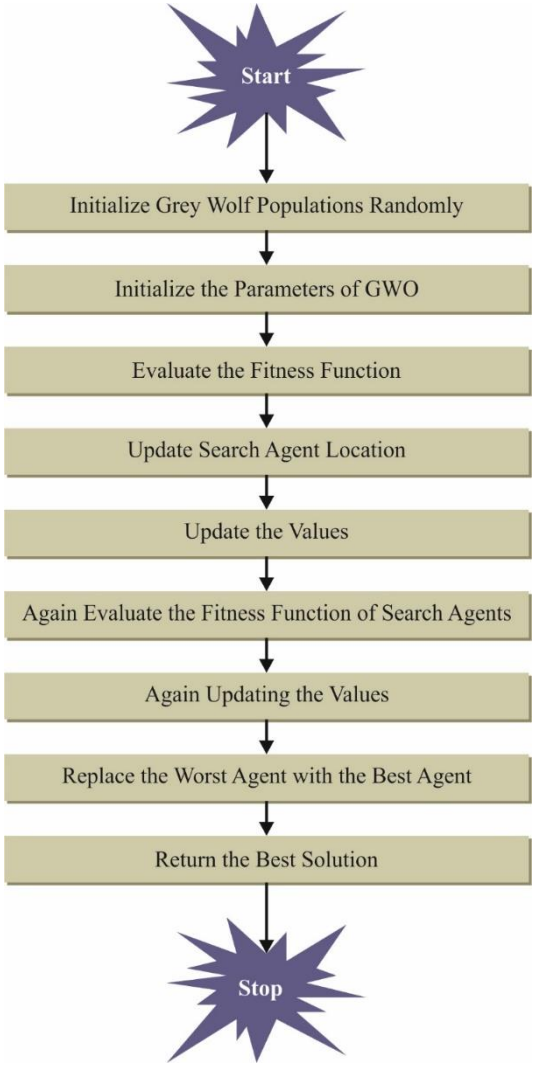

Figure 2. Flowchart of GWO

In the GWO, the exploitation and exploration of diversity were controlled by $\vec{A}$vector. If $|A| < 1$, then wolf gets closer to the target because the next position of wolf is within the region between the present and the prey positions 26

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

confirming the exploitation of GWO. If $|A| > 1$, then the wolf deviate from the target. This conforms the global exploration. In addition, the vector $\vec{C}$ influence on the exploitation and exploration of GWO since it is arbitrary weight that impact the wolf position update. This assists the GWO in resolving the local optima problems. Fig. 2 illustrates the flowchart of GWO.

The appropriateness of selections is a significant factors that impact the presentation of the GWO technique. The hyper-parameter selection procedure includes the solutions encrypting model to estimate the efficiency of the candidate solution. Considering this work, the GWO algorithms consider precision as the main benchmark for designing the fitness function (FF), which may expressed as mentioned below.

$$Fitness = \max(P) \tag{13}$$

$$P = \frac{TP}{TP + FP} \tag{14}$$

Deriving from the term, TP denotes the truth positive and FP represents the falsity positive values.

4. Experimental Validation

The simulation analysis of the CPABNA-RDCS method has been detected on a database containing 840 samples as signified in Table 1.

Table 1: Details on Dataset

Classes	No. of samples
Goodware	420
Ransomware	420
Total Samples	840

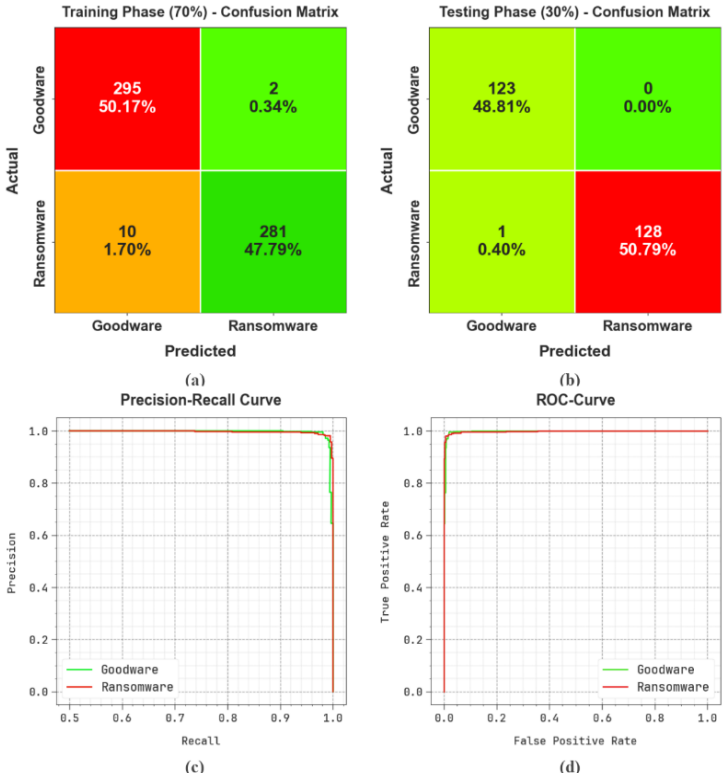

Figure 3. Classifier outcome of (a-b) 70: 30 of TRAP/TESP of confusion matrices and (c-d) PR and ROC curves

Figure 3 shows the performance of the CPABNA-RDCS technique. Figs. 3a-3b depicts the confusion matrices existing by the CPABNA-RDCS approach on 70%TRAP:30%TESP. The outcome indicated that the CPABNA-

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

RDCS method has detected and categorized different classes. As well, Fig. 3c authorizes the PR study of the CPABNA-RDCS model. The outcome defined that the CPABNA-RDCS model has increased greatest PR efficiency under each class. To conclude, Fig. 3d depicts the ROC curve of the CPABNA-RDCS approach. The outcomes indicated that the CPABNA-RDCS system led to skilled performances with maximum values of ROC at each class.

In Table 2 and Figure 4, the overall ransomware detection outcome of the CPABNA-RDCS system are examined in 70%TRAP and 30%TESP. The table values stated that the CPABNA-RDCS technique properly recognized two classes. With 70%TRAP, the CPABNA-RDCS model gains average $accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 97.95%, 97.95%, 97.95%, 97.96%, and 95.95%, respectively. Moreover, With 30%TESP, the CPABNA-RDCS technique gains average $accu_y$, $sens_y$, $spec_y$, F_{score}, and MCC of 99.61%, 99.61%, 99.61%, 99.60%, and 99.21%, respectively.

Table 2: Ransomware detection of CPABNA-RDCS methodology under 70:30 of TRAP/TESP

Class	$Accu_y$	$Sens_y$	$Spec_y$	$F1_{Score}$	MCC
TRAP (70%)					
Goodware	99.33	99.33	96.56	98.01	95.95
Ransomware	96.56	96.56	99.33	97.91	95.95
Average	97.95	97.95	97.95	97.96	95.95
TESP (30%)					
Goodware	100.00	100.00	99.22	99.60	99.21
Ransomware	99.22	99.22	100.00	99.61	99.21
Average	99.61	99.61	99.61	99.60	99.21

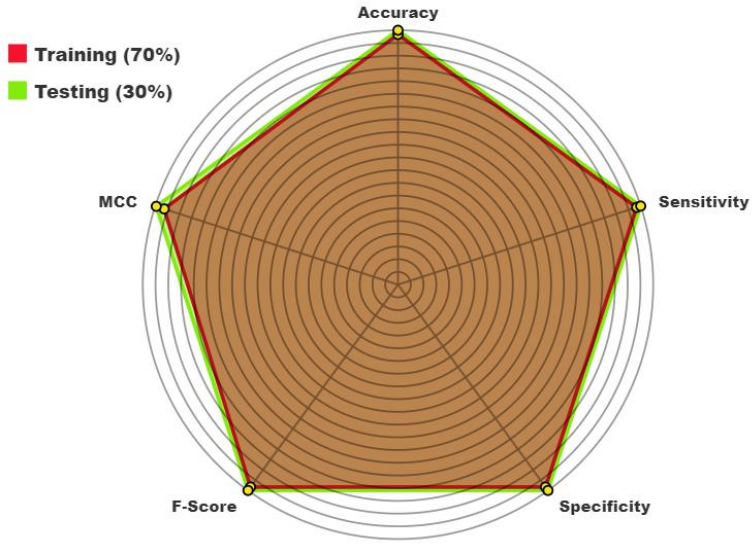

Figure 4. Average outcome of CPABNA-RDCS method under 70:30 of TRAP/TESP

In Figure 5, the training and validation accuracy outcomes of the CPABNA-RDCS method are established. The accuracy values are calculated over a range of 0-25 epochs. The outcome emphasized that the training and validation accuracy values display a rising tendency which notified the skill of the CPABNA-RDCS system with enhanced performance over numerous iterations. Moreover, the training and validation accuracy remains nearer over the epochs, which designates lowest minimal overfitting and exhibits improved performance of the CPABNA-RDCS system, assuring consistent prediction on unseen samples.

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

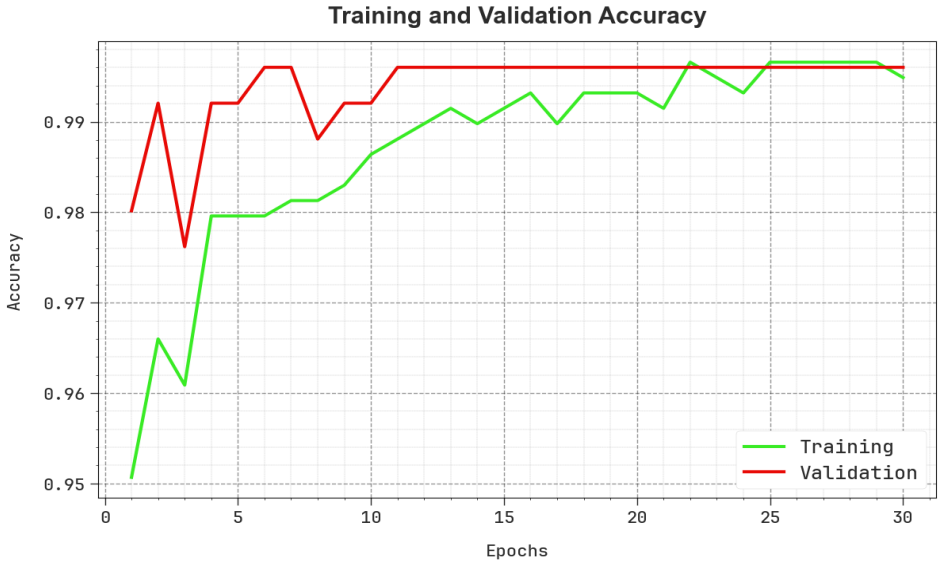

Figure 5. $Accu_y$ curve of CPABNA-RDCS technique

Figure 6. Loss curve of CPABNA-RDCS technique

In Figure 6, the training and validation loss graph of the CPABNA-RDCS method is displayed. The loss values are calculated throughout 0-25 epochs. It is embodied that the training and validation accuracy values demonstrate a decreasing tendency, which alerted the ability of the CPABNA-RDCS model to balance a trade-off between data fitting and generalization. The continual decrease in loss values furthermore guarantees the enhanced performance of the CPABNA-RDCS system and tunes the prediction outcomes over time.

To establish the proficiency of the CPABNA-RDCS approach, a comprehensive comparison study is prepared in Table 3 [12]. In Figure 7, a comparative $accu_y$ result of the CPABNA-RDCS system is provided. The results indicate that the CPABNA-RDCS methodology has exhibited optimum performances compared with other methods. Based on $accu_y$, the CPABNA-RDCS system has obtained higher $accu_y$ of 99.61% whereas the OG-CNNRWD, DWO-ML, Bagging, AdaBoostM1, ROF, DT, and RF approaches have gained lesser $accu_y$ of 99.54%, 99.09%, 98.47%, 96.13%, 95.79%, 97.63%, and 98.83%.

In Figure 8, a comparative $sens_y$ and $spec_y$ result of the CPABNA-RDCS method is provided. The outcomes show that the CPABNA-RDCS model has exhibited optimum performances compared with other techniques. Based on $sens_y$, the CPABNA-RDCS method has gotten higher $sens_y$ of 99.61% but the OG-CNNRWD, DWO-ML, Bagging, AdaBoostM1, ROF, DT, and RF systems have gained smaller $sens_y$ of 99.54%, 99.43%, 93.66%,

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

94.50%, 96.77%, 97.82%, and 98.79%. Based on $spec_y$, the CPABNA-RDCS method has gotten higher $spec_y$ of 99.61% where the OG-CNNRWD, DWO-ML, Bagging, AdaBoostM1, ROF, DT, and RF methodologies have gained smaller $sens_y$ of 99.54%, 99.17%, 96.06%, 94.60%, 97.38%, 98.12%, and 98.26%.

Table 3: Comparative outcome of CPABNA-RDCS technique with other models

Methods	$Accu_y$	$Sens_y$	$Spec_y$
CPABNA-RDCS	99.61	99.61	99.61
OG-CNNRWD	99.54	99.54	99.54
DWO-ML	99.09	99.43	99.17
Bagging	98.47	93.66	96.06
AdaBoostM1	96.13	94.50	94.60
ROOF	95.79	96.77	97.38
DT	97.63	97.82	98.12
RF	98.83	98.79	98.26

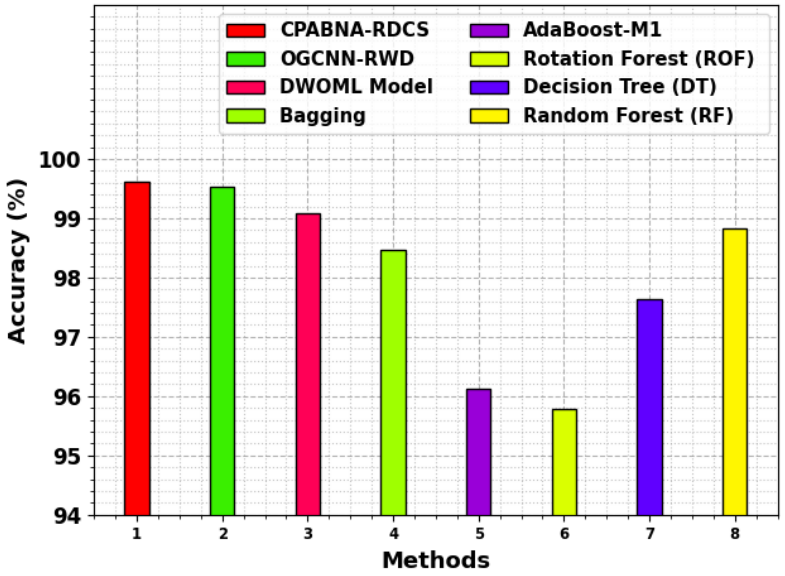

Figure 7. $Accu_y$ outcome of CPABNA-RDCS technique with other models

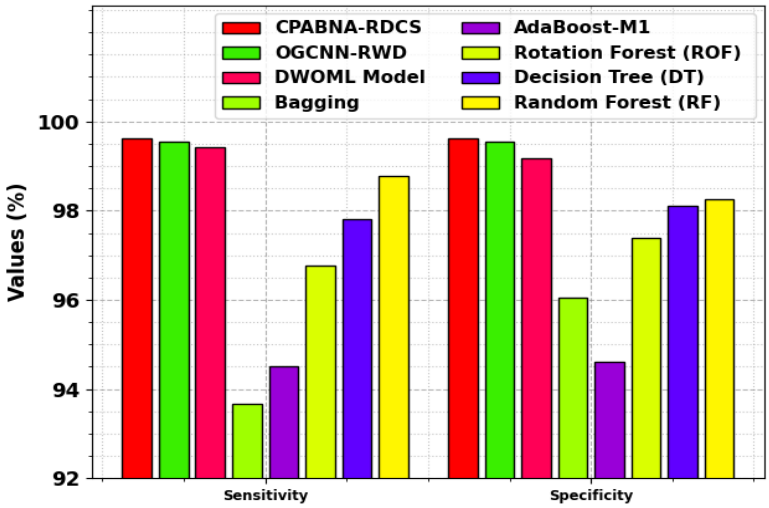

Figure 8. $Sens_y and\ Spec_y$ outcome of CPABNA-RDCS technique with other models

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

5. Conclusion

In this article, we have introduced a novel CPABNA-RDCS methodology in IoT environment. The objective of the CPABNA-RDCS model is to identify and categorize the ransomware to accomplish cybersecurity in the IoT network. To accomplish that, the CPABNA-RDCS method comprises min-max normalization, CPABN-based detection, and GWO-based hyperparameter tuning processes. Initially, the CPABNA-RDCS method exploits min-max normalization for scaling the input dataset into relevant format. Meanwhile, the ransomware classification takes place via CPABN method. Finally, GWO is employed for optimum hyperparameter choice of the CPABN method. The experimental results of the CPABNA-RDCS method are inspected on benchmark data. The simulation analysis emphasized the developments of the CPABNA-RDCS method over other existing techniques.

Funding: "The author gratefully acknowledges the invaluable support provided by the Department of Software Engineering, College of Engineering, University of Business and Technology, Jeddah, Saudi Arabia"

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

References

[1] Saheb, A.H. and Buti, R.H., 2024. A Specific Category of Harmonic Functions Characterized By A Generalized Komatsu Operator in Conjunction With The (RK) Integral Operator and Applications to Neutrosophic Complex Field. Full-Length Article, 23(3), pp.44-4.

[2] Mathew, L.P., Sebastian, L. and Thankachan, B., 2024. Some Operations on Trapezoidal Single Valued Neutrosophic Fuzzy Numbers. International Journal of Neutrosophic Science, 23(3), pp.29-9.

[3] Noaman, I.A.R., Hasan, A.H. and Ahmed, S.M., 2024. Optimizing Weibull Distribution Parameters for Improved Earthquake Modeling in Japan: A Comparative Approach. International Journal of Neutrosophic Science, 24(1), pp.65-5.

[4] Doaa Nihad Tomma, L. A. A. Al-Swidi. "Necessary and Sufficient Conditions for a Stability of the Concepts of Stable Interior and Stable Exterior via Neutrosophic Crisp Sets." International Journal of Neutrosophic Science, Vol. 24, No. 1, 2024, PP. 87-93

[5] Mathews, P., Sebastian, L. and Thankachan, B., 2024. Neutrosophic Fuzzy Score Matrices: A Robust Framework for Advancing Medical Diagnostics. International Journal of Neutrosophic Science, 23(3), pp.08-8.

[6] Al-Hawawreh, M.; Sitnikova, E. Leveraging deep learning models for ransomware detection in the industrial Internet of things environment. In Proceedings of the 2019 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 12–14 November 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–6.

[7] Al-Hawawreh, M.; Sitnikova, E. Industrial Internet of Things-based ransomware detection using stacked variational neural network. In Proceedings of the 3rd International Conference on Big Data and Internet of Things, Melbourn, VIC, Australia, 22–24 August 2019; pp. 126–130.

[8] Sharma, S.; Krishna, C.R.; Kumar, R. Android Ransomware Detection using Machine Learning Techniques: A Comparative Analysis on GPU and CPU. In Proceedings of the 2020 21st International Arab Conference on Information Technology (ACIT), Giza, Egypt, 28–30 November 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1–6.

[9] Dion, Y.; Brohi, S.N. An experimental study to evaluate the performance of machine learning algorithms in ransomware detection. J. Eng. Sci. Technol. 2020, 15, 967–981.

[10] Al-Hawawreh, M.; Sitnikova, E.; Aboutorab, N. Asynchronous Peer-to-Peer Federated Capability-Based Targeted Ransomware Detection Model for Industrial IoT. IEEE Access 2021, 9, 148738–148755.

[11] Mofidi, F., Hounsinou, S.G. and Bloom, G., 2024, January. L-IDS: A Multi-Layered Approach to Ransomware Detection in IoT. In 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0387-0396). IEEE.

[12] Khalid Alkahtani, H., Mahmood, K., Khalid, M., Othman, M., Al Duhayyim, M., Osman, A.E., Alneil, A.A. and Zamani, A.S., 2023. optimal graph convolutional neural network-based ransomware detection for cybersecurity in IoT environment. Applied Sciences, 13(8), p.5167.

[13] Singh, A., Abosaq, H.A., Arif, S., Mushtaq, Z., Irfan, M., Abbas, G., Ali, A. and Al Mazroa, A., 2024. Securing Cloud-Encrypted Data: Detecting Ransomware-as-a-Service (RaaS) Attacks through Deep Learning Ensemble. Computers, Materials & Continua, 79(1).

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024

[14] Ahanger, T.A., Tariq, U., Dahan, F., Chaudhry, S.A. and Malik, Y., 2023. Securing IoT devices running PureOS from ransomware attacks: leveraging hybrid machine learning techniques. Mathematics, 11(11), p.2481.

[15] Gazzan, M. and Sheldon, F.T., 2024. Novel Ransomware Detection Exploiting Uncertainty and Calibration Quality Measures Using Deep Learning. Information, 15(5), p.262.

[16] Zewdie, T.G., Girma, A. and Cotae, P., 2022, June. Ransomware Attack Detection on the Internet of Things Using Machine Learning Algorithm. In International Conference on Human-Computer Interaction (pp. 598-613). Cham: Springer Nature Switzerland.

[17] Ali, P.J.M., 2022. Investigating the Impact of min-max data normalization on the regression performance of K-nearest neighbor with different similarity measurements. ARO-The Scientific Journal of Koya University, 10(1), pp.85-91.

[18] Mohamed, Adam. COPRAS Neutrosophic Approach with Big Data Analytics for Enhancing Multi-Dimensional Customer Churn Prediction on Corporate Performance Assessment. Journal of International Journal of Neutrosophic Science, vol. 24, no. 3, 2024, pp. 127-137.

[19] Ngo, N.T., Truong, T.T.H., Truong, N.S., Pham, A.D., Huynh, N.T., Pham, T.M. and Pham, V.H.S., 2022. Proposing a hybrid metaheuristic optimization algorithm and machine learning model for energy use forecast in non-residential buildings. Scientific Reports, 12(1), p.1065.

DOI: https://doi.org/10.54216/IJNS.250203
Received: April 26, 2024 Revised: June 30, 2024 Accepted: July 22, 2024