[1]Yashwant Aditya
[2]Dr. Priyank Jain
[3]Dr. Ritu Tiwari

# Improved Cyber-Security Mechanism Using Integration of OD-DRUNN and XAI-BASED Proactive Defense for Organizations

Journal of Electrical Systems

***Abstract:*** - Today, cyber-attacks have become more severe and frequent, which calls for a new line of security defenses to protect against them. So, to preserve the organizations' details from cyber threats, many research works use different proactive defense mechanisms. But the attacks that are present in the machine learning (ML) model provide misclassification results. So, this research methodology proposed an integration of Explainable Artificial Intelligence (XAI) with Ordinary Differential Deep Recurrent Unit Neural Network (OD-DRUNN) for a proactive defense mechanism in cyber-security for organizations. Initially, the input data is pre-processed and the features are extracted. From the extracted features, the traffic pattern and user behaviors are analyzed using the Minimum Parameterized Muller Spanning Tree (MPMST) approach. Then, the obtained traffic pattern, user behavior, and the extracted features are given as input to the OD-DRUNN classifier. Then, the output is displayed with XAI. With the help of XAI output, the attack in the ML model is neglected. After that, the severity is assessed for the abnormal types using the potential level score. If the severity level is high and moderate, then security is ensured by the Cycloid Curved Optimized Cryptography (2COC) algorithm and stored in the blockchain. Otherwise, it follows normal security procedures for storage. The proposed methodology achieves 99.2% accuracy in potential vulnerability detection.

***Keywords:*** Ordinary Differential Deep Recurrent Unit Neural Network (OD-DRUNN), Cycloid Curved Optimized Cryptography (2COC), Minimum Parameterized Muller Spanning Tree (MPMST), Explainable Artificial Intelligence (XAI), Proactive defense mechanism, Cyber-security, and Cyber threats.

## I. INTRODUCTION

In this world, innovations are increasing in the digitalization of the organization. But digitalization poses a challenge related to cyber threats in organizational security [15]. So, several organizations, such as banks, customer services, and so on are considered cyber-security services. Cybersecurity has become a priority on the agenda of the leadership of public and private organizations [6, 7]. However, cyber threats are continuously increasing in the cyber security service. So, it is crucial to continuously enhance cyber security networks to stay ahead of potential attackers [12]. Cyber-attacks and defense frameworks offer numerous ways to protect systems and networks from threats [11]. The threats mainly originated from online sources, including viruses, Trojans, worms, spam, and botnets [1]. For protection, two different mechanisms are used, such as protective and active mechanisms. Proactive defense can predict potential vulnerabilities and threats, and active mechanisms detect the presented vulnerabilities [5]. Organizations severely need a proactive defense mechanism because if the attack is influenced in the organizations' network, then the attack is spread all over the network [13]. Various Artificial Intelligence (AI) and Machine Learning (ML) techniques have been explored for the proactive defense mechanism of organizations [13]. Also, existing methodologies also presented different defense mechanisms but those were inadequate to prevent various types of attacks [20]. So, this research methodology presented the integration of XAI with OD-DRUNN for proactive defense mechanisms in cyber-security.

### *A. Problem statement*

- None of the existing research explained the vulnerability detection description process for the attack in ML of cybersecurity for organizations.
- The existing [3] might provide inaccurate results during the dynamic behavior of the user.
- The existing [8] was lacking in the extraction of features of encrypted data in potential vulnerability prediction.

[1, 2, 3] *Department of Computer Science and Engineering,

[1, 2, 3] Indian Institute of Information Technology, Pune, India

*Corresponding author's E-mail id: yashwant.aditya23@iiitp.ac.in, [2]priyank@iiitp.ac.in , [3]ritu@iiitp.ac.in

- Existing [18] failed to assess the potential of attack severity level assessment-based data preservation for organizations.

### *B. Objectives*

- The XAI is used with the OD-DRUNN for assessment of attack in ML.
- The user's dynamic and static patterns are analyzed by utilizing MPMST.
- The features are also extracted from encrypted data.
- To predict the severity level by potential level score and preserved by utilizing 2COC.

The structure of the paper is organized as follows, in section 2, the existing works are explained, in section 3, the proposed research is explained, and in sections 4 and 5, the result and conclusion phase is given.

## II. RELATED WORK

Almahmoud et al.[3] introduced a Machine Learning (ML)-based model for cyber-attack detection. The framework was completely automated and quantitative using the ML model. In experimental assessment, the presented research framework achieved higher performance than the conventional model.

Alevizos et al.[2] recommended the Cyber Resilience Index (CRI), a TTP-based probabilistic approach to quantify an organization's defense effectiveness against cyber-attacks (campaigns). The result showed that the model achieved better performance than the conventional model.

Xing et al.[18] presented a hierarchical network security measurement and optimal active defense in the cloud computing environment. The hierarchical analysis calculated the relative importance weights of similar evaluation factors. Experimental results showed that the security of the network was increased than the conventional model.

Dekker et al.[8] developed a Threat-Intelligence (TI) driven methodology for cyber security analysis. The quality of the decision-making process was enhanced by utilizing casual graphs. The presented methodology achieved higher performance than the conventional methods. However, it didn't ensure the security of the data within organizations. So, it might affect the performance of the framework.

Rehman et al.[14] suggested a proactive defense framework for security analysis. The framework was a combination of Moving Target Defense techniques with cyber deception. The simulation result demonstrated the approach to mitigate the impact of attacks while maintaining high-performance levels in IoT networks. However, the scalability wasn't flexible.

## III. **TABLE 1**: ANALYSIS OF STATE-OF-THE-ART WORKS

| Author's name | Paper title | Contribution | Technique used | Limitations | Remark |
|---|---|---|---|---|---|
| Almahmoud et al.[3] | A holistic and proactive approach to forecasting cyber threats | The study presents a machine learning-based approach for long-term prediction of cyber-attacks, enabling proactive planning and resource allocation for cybersecurity agencies. | The research employs a Bayesian Long Short-Term Memory (B-LSTM) model with an encoder-decoder architecture. It utilizes multiple data sources, including incident reports, scientific literature mentions, social media data on armed conflicts, and public holiday information. | The model's accuracy may be affected by the quality and availability of input data.<br><br>It may struggle with predicting entirely new, zero-day attacks.<br><br>The approach relies on historical data and patterns, which may not always reflect future trends. | This proactive approach to cyber threat prediction offers valuable insights for cybersecurity planning, allowing agencies to prioritize resources and develop defensive measures against potential future attacks. However, it should be used in conjunction with other security measures and expert knowledge for comprehensive cybersecurity strategies. |
| Alevizos et al.[2] | TTP-Based Cyber Resilience Index: A Probabilistic | The study introduces a Cyber Resilience Index (CRI) framework that quantitatively | The research employs a Partially Observable Markov Decision Process (POMDP) approach, incorporating MITRE ATT&CK framework and threat intelligence | The model's accuracy depends on the quality and availability of threat intelligence data. | The CRI framework offers a dynamic, quantifiable metric for assessing cyber resilience, providing organizations |

| | | | | | |
|---|---|---|---|---|---|
| | Quantitative Approach to Measure Defence Effectiveness Against Cyber Attacks | measures an organization's defense effectiveness against cyber attacks using threat intelligence and probabilistic modeling. | to model attack flows and calculate the CRI. | It may require significant computational resources for practical implementation.<br><br>The approach focuses on known attack patterns and may not fully account for novel or zero-day attacks. | with actionable insights for improving their security posture. It addresses limitations of existing methodologies by integrating threat intelligence and probabilistic modeling, offering a more comprehensive and adaptable approach to cybersecurity assessment. |
| Xing et al.[18] | Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments | The study introduces a hierarchical network security measurement and optimal proactive defense system for cloud computing environments, using risk values as indicators to evaluate security situations. | The research employs a combination of methods, including:<br><br>•A Partially Observable Markov Decision Process (POMDP) approach<br>• Fuzzy logic for risk assessment<br>•Hierarchical analysis for calculating importance weights of evaluation factors<br>•A cloud platform posture fusion algorithm for multi-region cloud platforms | The model's accuracy depends on the quality of input data and expert judgments.<br><br>It may require significant computational resources for large-scale networks.<br><br>The approach primarily focuses on known vulnerabilities and threats. | This hierarchical approach to network security measurement in cloud computing environments offers a comprehensive and adaptable framework for assessing and improving cybersecurity posture. It integrates multiple techniques to provide a more nuanced understanding of security risks, enabling proactive defense strategies. However, its effectiveness relies heavily on accurate input data and expert knowledge. |
| Dekker et al.[8] | A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making | The study introduces a threat intelligence-driven methodology called TIBSA (Threat Intelligence Based Security Assessment) to incorporate uncertainty in cyber risk analysis and enhance decision-making. | The research employs a combination of methods, including:<br>• Partially Observable Markov Decision Process (POMDP) approach<br>• Benefit-cost analysis (BCA) for evaluating security control effectiveness<br>• Scoring models for assessing Tactics, Techniques, and Procedures (TTPs)<br>• Integration of threat intelligence data | 1. The model's accuracy depends on the quality and availability of threat intelligence data.<br>2. Significant expertise may be required to interpret results accurately and effectively.<br>3. The approach primarily focuses on known threats and TTPs, potentially overlooking novel attack vectors. | TIBSA offers a comprehensive framework for assessing cybersecurity risks by incorporating threat intelligence and uncertainty factors. It provides a more nuanced understanding of an organization's security posture, enabling better-informed decision-making. However, its effectiveness relies heavily on the quality of input data and expert knowledge in interpreting the results. |
| Rehman et al.[14] | Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception | The study introduces a proactive defense mechanism for IoT security, combining diversity-based Moving Target Defense (MTD) and cyber deception techniques within an SDN-based IoT framework. | The research employs:<br>• Diversity-based MTD to periodically change system components<br>• Cyber deception using decoy nodes<br>• Hierarchical Attack Representation Model (HARM) for scalable security modeling<br>• Novel security metrics including Attack Cost (AC), Return on Attack (RoA), and Risk (R) | The effectiveness may depend on the quality of diversity implementation and decoy design. Frequent adaptations could potentially impact network performance and service quality. The approach may require significant computational resources for large-scale IoT networks. | This integrated approach offers a promising solution for enhancing IoT network security by combining MTD and cyber deception techniques. It provides a comprehensive framework for assessing and improving security posture while addressing scalability issues. However, careful consideration must be given to balancing |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | security improvements with potential performance impacts. |

## IV. Proposed OD-DRUNN-Based Proactive Defense Mechanism For Cyber-Security

In this paper, the proactive defense mechanism is derived by using OD-DRUNN with an XAI approach for the cyber-security of organizations. The structural design of the proposed research framework is displayed in Fig. 1.

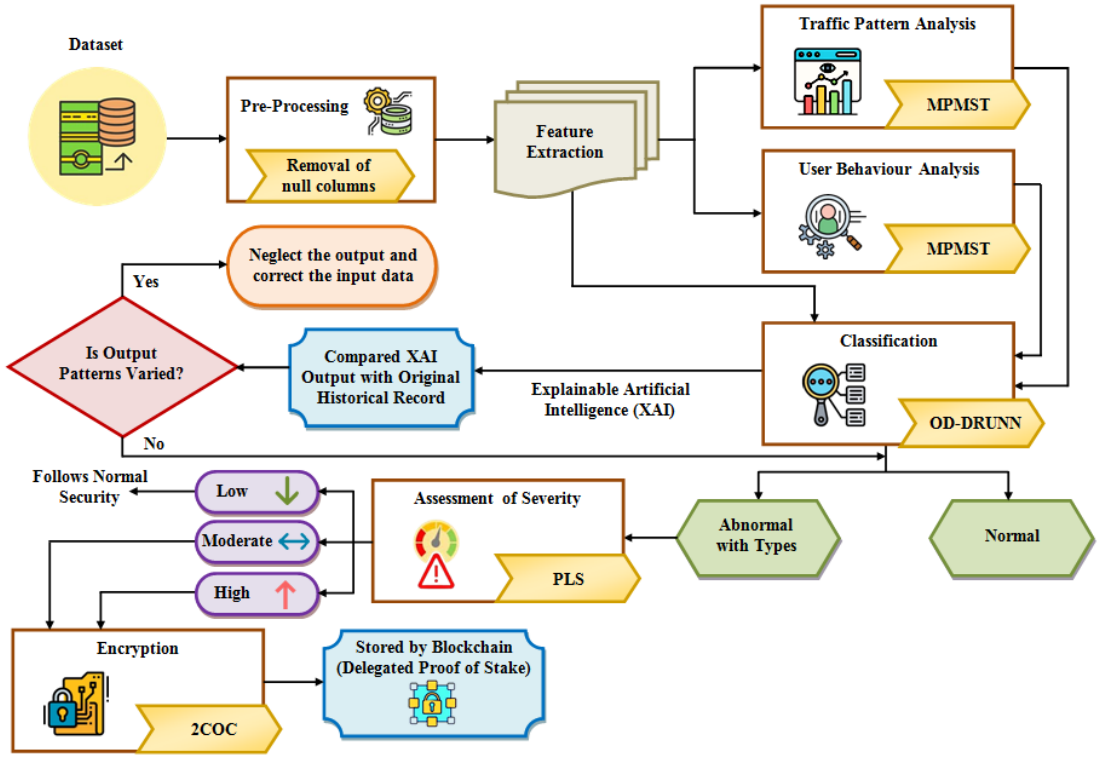



**Fig.1**: Structural Design of the Proposed Framework

### *A. Dataset*

Initially, the input data is obtained from the dataset. The dataset contains user device details and packet details. The initial input data is denoted as $\wp_z$.

### *B. Pre-processing*

In this section, the null columns of the input data files are removed for reducing the training time of the threat detection process. The null value removed data is represented as $\kappa_j$.

### *C. Feature extraction*

Here, from $\kappa_j$, the features, such as user id, original host, response host, flow duration, forward packets total, backward packets total, forward header size maximum, and so on are extracted.

$$\varpi_e = \{\varpi_1, \varpi_2, \ldots\ldots, \varpi_n\} \tag{1}$$

Where, $\varpi_e$ indicates the extracted feature set and $\varpi_n$ defines the n-number of extracted features.

*D.* ***Traffic Pattern Analysis***

In this section, the traffic pattern of the data transfer is assessed in $\varpi_e$ using the MPMST to improve the proactive defence mechanism. The conventional MST model is a cost-effective approach. However, the complexity is very high because the cycle in the graph and the edges are with the same weight. So, this research methodology uses the Parameterized Muller function for the weight initialization for graph construction. At first, the graph $\delta_g$ is constructed by considering vertex $V_x$ and edges $E_d$.

$$\delta_g(\varpi_e) = (E_d, V_x) \tag{2}$$

Then, the weight $\omega_t$ value for the edges is assigned using the parameterized Muller function, which is derived in equation (3),

$$\omega_t = \frac{E_d - E_{d-1}}{E_{d-1} - E_{d-2}} \tag{3}$$

According to the $\omega_t$, graph is restructured. Then, whether the tree is formed or not is checked, and the checking condition is presented in equation (4),

$$\begin{cases} A_l & if\ \ tree == formed \\ N_l & otherwise \end{cases} \tag{4}$$

Here, $A_l$ denotes the formed tree for further process and $N_l$ specifies the discarded tree. The pseudocode of MPMST is given below,

**Pseudocode for MPMST**

---

**Input:** $\varpi_e$

**Output:** $W_{tf}$

---

**Begin**

**Initialize** $V_x$, $E_d$ and $\omega_t$

**For** each $\varpi_e$ **do**

**Construct** $\delta_g(\varpi_e)$

**Estimate** $\omega_t = \frac{E_d - E_{d-1}}{E_{d-1} - E_{d-2}}$

*#constructed graph checking*

**if** $(tree == formed)${

$A_l$

**} else {**

$N_l$

**} end if**

**End for**

**Return** $W_{tf}$

**End**

---

By utilizing the connected edges of the tree, the traffic behavior is taken and it is denoted as $W_{tf}$ .

### *E. User Behavior Analysis*

Here, from $\varpi_e$, the user behavior is also analyzed to enhance the proactive defense mechanism using MPMST, which is explained in section D above. The obtained user behavior is denoted as $\beta_{ur}$ .

### *F. Classification*

In this section, the potential vulnerability threats are detected to preserve the cyber-security of organizations using OD-DRUNN with the XAI approach. For detection of vulnerabilities, the combination of $\varpi_e$, $W_{tf}$ , and $\beta_{ur}$ are considered as input, which is denoted as $\Im_x$. The conventional DRNN remembers important things about the input they received. But, DRNN has a vanishing gradient problem. So, this research methodology uses the Unit vector function. Also, the conventional DRNN was challenging for large sequences. Therefore, this research methodology uses the Ordinary Differential Equation based isolation of some repeated parameters stored in the memory. The structure of the OD-DRUNN is shown in Figure 2.

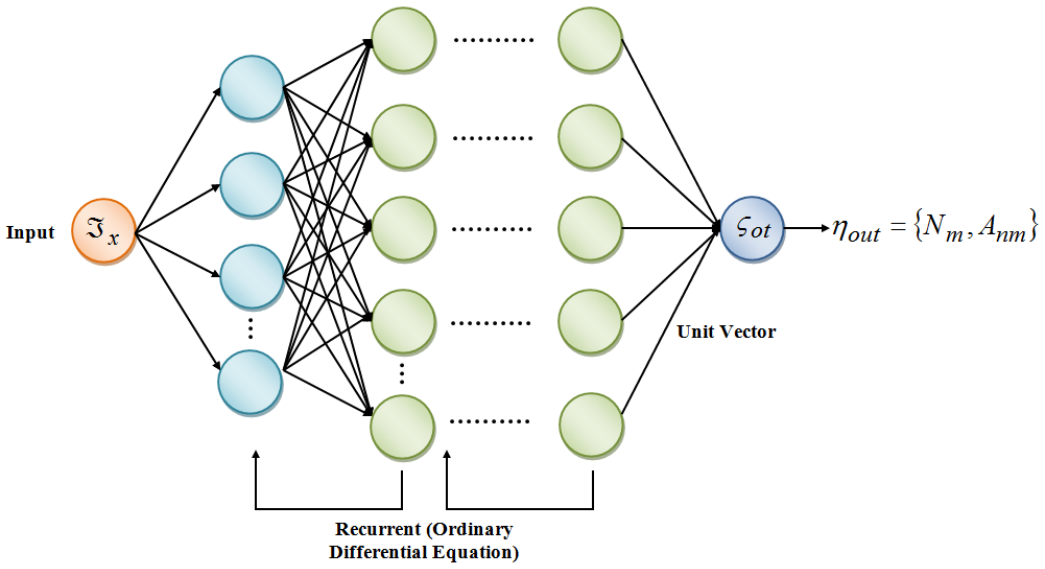



**FIG.2:** STRUCTURE OF OD-DRUNN

Originally, $\Im_x$ is given to the input layer. Then, the output of the input layer $\varsigma_{oi}$ is given to the hidden layer. In the hidden layer, the recurrent connection of the previously hidden outcome is passed to the current hidden layer. Before that, the previous connection parameters are isolated using an ordinary differential equation, which is derived in equation (5),

$$\frac{dj^{j+1}}{dj^{i}} = \alpha j^{j} + \alpha = \ell^{t} \tag{5}$$

Here, $j^{j}$ indicates the previous stored parameters and $\alpha$ denotes the constant value. The final obtained parameter is denoted as $\ell^{t}$ . Then, the derivation of hidden layer $B_d$ and output layer $\varsigma_{ot}$ are given in equation (6), (7), and (8),

$$B_d = \lambda\left(\varphi.\varsigma_{oi} + \varphi.B_{d-1} + \varepsilon\right) \quad (6)$$

$$\upsilon_t = B_d.\varphi + \varepsilon \quad (7)$$

$$\varsigma_{ot} = soft_{\max}\left(\upsilon_t\right) \quad (8)$$

Where, $\lambda$ defines the activation function, $\varphi$ and $\varepsilon$ represent the weight and bias value, $\upsilon_t$ defines the function of the output layer, and $soft_{\max}$ indicates the softmax activation function. Finally, the gradient of the direction $\nabla G(\varsigma_{ot})$ is analyzed by unit vector, which is derived in equation (9),

$$\nabla G(\varsigma_{ot}) = \begin{cases} \chi \dfrac{G}{\|G\|}, & if\ G \geq \chi \\ C_l, & else \end{cases} \quad (9)$$

Where, $\nabla G(\varsigma_{ot})$ denotes the gradient value of the functions, $\chi$ defines the hyper-parameter, and $C_l$ indicates the normal gradient function. The final outcome $\eta_{out}$ is expressed in equation (10),

$$\eta_{out} = \{N_m, A_{nm}\} \quad (10)$$

Here, $N_m$ denotes the normal class and $A_{nm}$ defines abnormal types, such as Bruteforce, Bruteforce-XML, Probing, and XMRIGCC CryptoMiner. The pseudocode for the OD-DRUNN is given below,

**Pseudocode for OD-DRUNN**

---

**Input:** $\Im_x$

**Output:** $\eta_{out} = \{N_m, A_{nm}\}$

---

**Begin**

**Initialize** $\varsigma_{oi}$, $B_d$ and $\varsigma_{ot}$

**For** each $\Im_x$ **do**

**Derive** $\dfrac{dj^{j+1}}{dj^i} = \alpha j^j + \alpha = \ell^t$

**Estimate** $B_d = \lambda\left(\varphi.\varsigma_{oi} + \varphi.B_{d-1} + \varepsilon\right)$

**Perform** output layer $\varsigma_{ot}$

**Derive** $\nabla G(\varsigma_{ot})$

**if** $(G \geq \chi)$ **{**

$$\nabla G(\varsigma_{ot}) = \chi \frac{G}{\|G\|}$$

**} else {**

$$\nabla G\left(\varsigma_{ot}\right) = C_l$$

**} end if**

**End for**

**Return** $\eta_{out} = \left\{N_m, A_{nm}\right\}$

**End**

---

The XAI output is also obtained and the obtained output pattern is compared with the historical data pattern. If it is varied, then the output is neglected and the input pattern is corrected; otherwise, the obtained output is considered as final output.

*G.* ***Assessment of Severity***

Here, the severity level of the obtained class is assessed using the polarity score $\aleph_{scr}$, which is expressed in equation (11),

$$\aleph_{scr} = 1 - \sum_{f=0}^{r} \frac{\psi^f e^{-\psi}}{f!} \left\{1 - \left(\frac{X\left(A_{nm}\right)}{Y\left(A_{nm}\right)}\right)^{r-f}\right\} \tag{11}$$

Where, $\psi$ denotes the combination of the total number of output classes and probability of obtained output, $X\left(A_{nm}\right)$ and $Y\left(A_{nm}\right)$ indicate the probability functions, $r$ defines the total number of output classes. According to the $\aleph_{scr}$, abnormal class is defined as low $L_w$, high $H_g$, and moderate $M_e$. If $L_w$ is obtained, then normal security is followed; otherwise, security is ensured by encryption with blockchain concept-based data storage.

*H.* ***Encryption***

Here, $H_g$ and $M_e$ classes of potential vulnerability threats related to input data $\wp_z$ are encrypted to ensure security using 2COC. But signing with a broken random number generator compromises the key. So, this research methodology uses the Tuna Swarm Optimization (TSO) algorithm for private key generation. It has unique and efficient features. But the optimizer is affected by the pre-mature convergence problem. So, this research uses the Bernoulli Distribution (BD) function for the determination of optimal individual selection in the updation process. Also, in ECC, the same curve points are repeatedly generated for the different users. So, this research methodology uses the Cycloid Curve.

$$C_{rv} = \begin{cases} co_1 = \iota\left(\tau - \sin\left(\tau\right)\right) \\ co_2 = \iota\left(1 - \cos\left(\tau\right)\right) \end{cases} \tag{12}$$

Here, $C_{rv}$ defines the curve plot, $co_1$ and $co_2$ indicate the co-ordinates 1 and 2, $\iota$ defines the radius, $\tau$ is the radius angle. The public key $\xi^{pc}$ generation is displayed in equation (13),

$$\xi^{pc} = \xi^{pr} \bullet o \tag{13}$$

Where, $o$ denotes the point on the curve value, and $\xi^{pr}$ indicates the private key, which is generated using the BD-TSO algorithm. First, the tuna are considered as the generated numbers. Then, the position of the initialized population is derived, and it is denoted as $\sigma_\rho$. Then, the fitness is evaluated. Here, a higher security level is considered a fitness function $\lambda_{fit}$. Then, updation derivation in spiral foraging is derived in equation (14),

$$\sigma_{\rho+1}=\begin{cases} V_1\cdot(\sigma_\rho^{best}+U\cdot\left|\sigma_\rho^{best}-\sigma_\rho\right|)+V_2\cdot\sigma_\rho \\ V_1\cdot(\sigma_\rho^{best}+U\cdot\left|\sigma_\rho^{best}-\sigma_\rho\right|)+V_2\cdot\sigma_{\rho-1}^{best} \end{cases} \quad (14)$$

$$V_1=V+(1-V)\cdot\frac{\rho}{\rho_{Max}} \quad (15)$$

$$V_2=(1-V)-(1-V)\cdot\frac{\rho}{\rho_{Max}} \quad (16)$$

Where, $\sigma_{\rho+1}$ signifies individual population of $\rho+1$ iteration, the current optimal individual is specified as $\sigma_\rho^{best}$, $V_1$ and $V_2$ are weight coefficients, $U$ specifies the distance parameter, $\rho$ denotes the current iteration, $\rho_{Max}$ is the maximum iteration, and $V$ defines the constant value. Then, the population position is updated in the parabolic foraging mechanism, which is derived in equation (17),

$$\sigma_{\rho+1}=\begin{cases} \sigma_\rho^{best}+l_r\cdot(\sigma_\rho^{best}-\sigma_\rho)+\Psi_\omega\cdot l_r\cdot(\sigma_\rho^{best}-\sigma_\rho), & if\ l_r<0.5 \\ \Psi_\omega\cdot l_r\cdot\sigma_\rho, & if\ l_r\geq 0.5 \end{cases} \quad (17)$$

$$\Psi_\omega=p_b^{(t_c)}*(1-p_b)^{1-t_c} \quad (18)$$

Here, $l_r$ specifies the random number, $p_b^{(t_c)}$ specifies the probability parameter for the initialized population $t_c$, and $\Psi_\omega$ defines the Bernoulli distribution function. Then, the input data is encrypted using equations (19) and (20),

$$Q_1=rand*o \quad (19)$$

$$Q_2=\wp_z\left(H_g,M_e\right)+rand*\xi^{pc} \quad (20)$$

Where, $Q_1$ and $Q_2$ specify the ciphertext 1 and 2, and the random number is denoted as $rand$. The encrypted data is securely stored in blockchain with delegate proof of stake concept. During data access by the authorized person, the data is decrypted. The decryption process is expressed as,

$$\wp_z\left(H_g,M_e\right)=Q_2-\xi^{pr}*Q_1 \quad (21)$$

The performance of the research approaches is analyzed in the further section.

## V. RESULT AND DISCUSSION

Here, the performance of the proposed methodologies is evaluated, and the proposed framework is implemented in the working platform of Python.

### *A. Dataset description*

For the performance assessment, the research work uses the HIKARI-2021 datasets, which are publically available, and the source link is provided under the reference section. Here, 80% of the data is used for training purposes, and the remaining 20% is used for testing purposes.

### *B. Performance analysis*

#### *1) Performance analysis of behavior and traffic pattern analysis*

Here, the performance of the proposed MPMST is compared with the existing MST, B-Tree, Splay tree, and block tree.

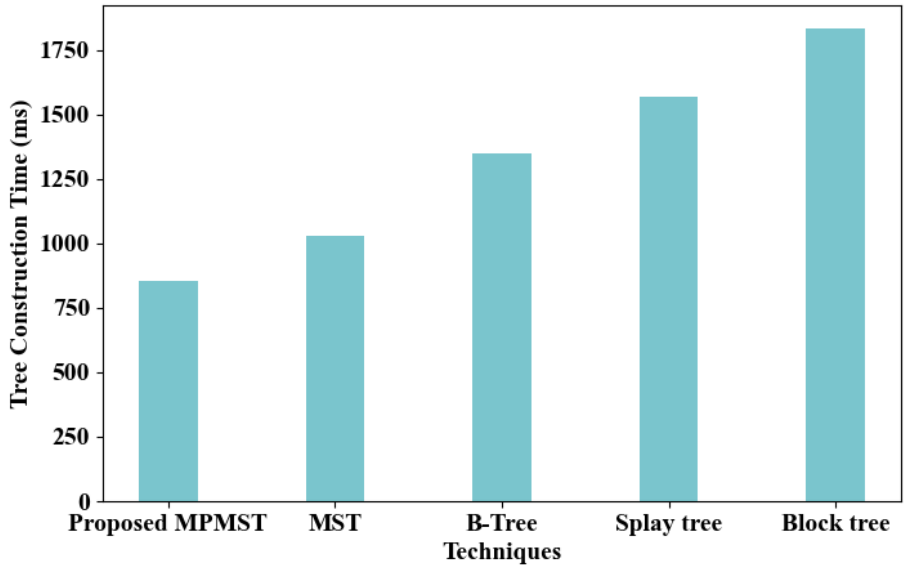



**FIG.3:** TREE CONSTRUCTION TIME ANALYSIS

The tree construction time of the proposed and existing methodology is graphically displayed in Figure 3. The tree construction time of MPMST is 856ms, which is lower than the conventional model because the weight is initialized by the Parameterized Muller function.

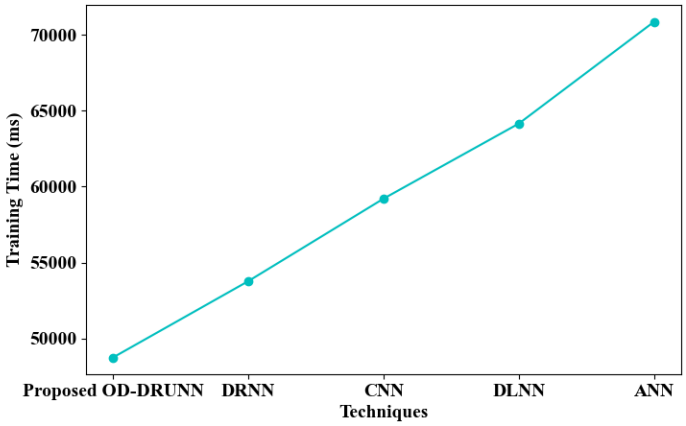
*2) Performance analysis of classification*

In this subsection, the performance of the proposed OD-DRUNN is analyzed with the existing Deep Recurrent Neural Network (DRNN), Convolutional Neural Network (CNN), Deep Learning Neural Network (DLNN), and Artificial Neural Network (ANN).

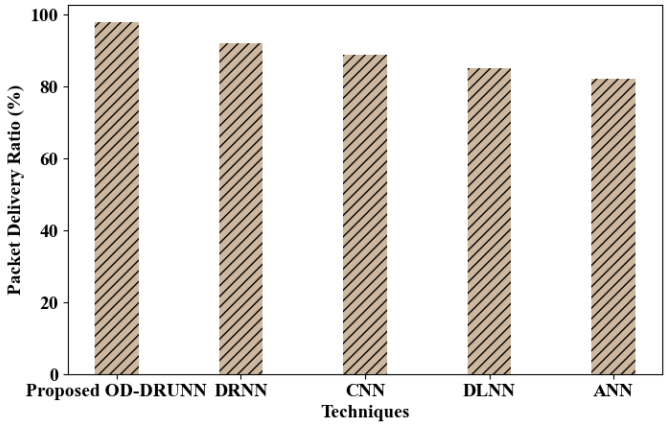
**TABLE 2**: PERFORMANCE ANALYSIS OF PROPOSED AND EXISTING CLASSIFIERS BASED ON STATISTICAL METRICS

| Metrics | Proposed OD-DRUNN | DRNN | CNN | DLNN | ANN |
|---|---|---|---|---|---|
| Precision | 98 | 95.9 | 92 | 90 | 89.6 |
| Recall | 97.9 | 94.6 | 92.2 | 89.7 | 87 |
| F-measure | 98.4 | 95.6 | 92.1 | 90.3 | 88.3 |
| Accuracy | 99.2 | 97 | 95.3 | 92 | 88.3 |
| MCC | 98.1 | 96 | 93.3 | 91 | 89.3 |
| FNR | 0.0591 | 0.0854 | 0.1078 | 0.1248 | 0.1305 |
| FPR | 0.0624 | 0.0962 | 0.1145 | 0.1296 | 0.1452 |

Table 2 shows the classification performance of the proposed and existing classifiers in terms of precision, recall, F-measure, accuracy, Mathew's Correlation Coefficient (MCC), False Negative Rate (FNR), and False Positive Rate (FPR). Here, the accuracy of OD-DRUNN is 99.2%, which is higher than the existing research methodologies because the vanishing gradient and long sequence challenges are solved by unit vector function and ordinary differential equation. For the remaining metrics, the OD-DRUNN also achieved higher performance.




**(a)**




**(b)**

**FIG.4:** GRAPHICAL PLOT FOR (A) TRAINING TIME, AND (B) PACKET DELIVERY RATIO ANALYSIS

Figure 4 displays the graphical plot for training time and packet delivery ratio. Here, the training time of the OD-DRUNN is 48762ms, which is lower than the existing methodologies. The packet delivery ratio of the proposed approach is 97.8%, which is higher than the existing methodologies.

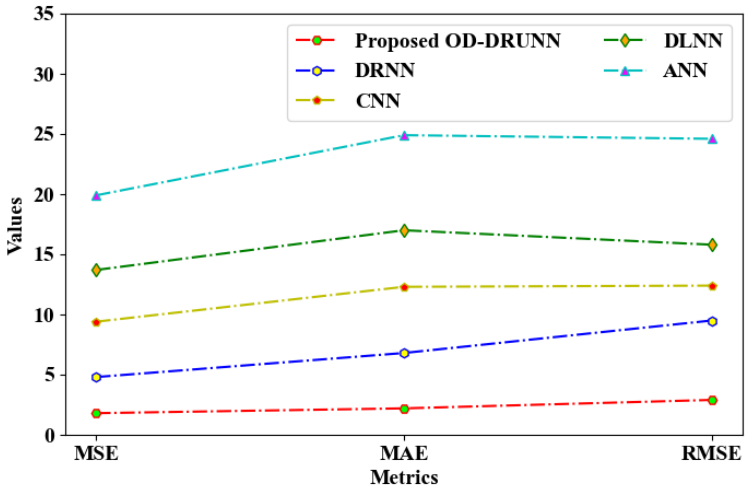



**FIG.5:** PICTORIAL REPRESENTATION OF ERROR ANALYSIS

The error value of the proposed OD-DRUNN is analyzed with the existing classifiers based on Mean Square Error (MSE), Mean Absolute Error (MAE), and Root MSE (RMSE). The OD-DRUNN has 1.8 MSE, 2.2 MAE, and 2.9 RMSE, which is lower than the existing research methods.

*3) Performance analysis of security*

Here, 2COC is analyzed with the Elliptic Curve Cryptography (ECC), Rivest Shamir Adleman (RSA), Data Encryption Standard (DES), and ElGamal approaches.

**TABLE 3**: SECURITY ANALYSIS

| **Methods** | **Security level (%)** |
|---|---|
| Proposed 2COC | 98.8 |
| ECC | 95 |
| RSA | 93.2 |
| DES | 90.3 |
| ElGamal | 88 |

The security level of the proposed and existing research methodologies is shown in Table 3. The security level of the 2COC is 98.8%, which is higher than the existing methods. Because, the key compromising problem is solved by using the BD-TSO, and the curve is plotted by utilizing a cycloid curve. The average security level of the existing research methods is 73.3%, which is lower than the proposed methodology.

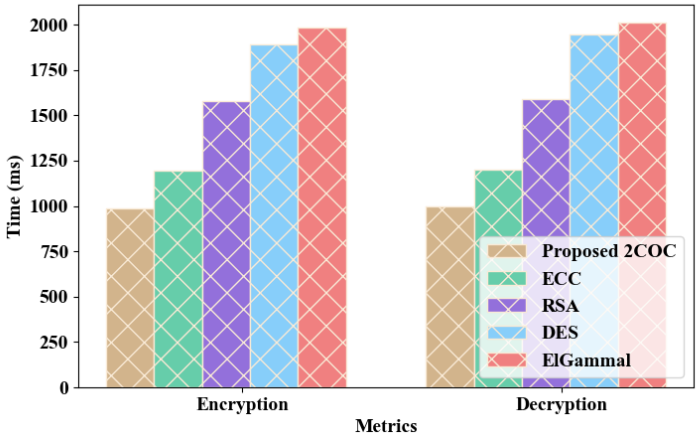



**FIG.6:** ENCRYPTION AND DECRYPTION TIME ANALYSIS

Figure 6 displays the encryption and decryption time analysis. The time taken for the encryption and decryption by 2COC is 986ms and 997ms, which is lower than the existing research methods. The average encryption and decryption time for the existing methodologies are 1662ms and 1686.5ms, respectively.

## *C. Comparative analysis*

**TABLE 4**: COMPARATIVE ANALYSIS OF PROPOSED AND STATE-OF-ART WORKS

| **Author's name** | **Methods** | **Accuracy** | **Precision** | **Recall** | **F-Measure** |
|---|---|---|---|---|---|
| Kure et al.[10] | Decision Tree (DT) | 93% | - | - | - |
| Alqudhaibi et al.[4] | Linear classifier | 66.25% | 18.25% | 36% | 13% |
| Yeboah-Ofori et al.[19] | ML model | 66% | - | - | - |

| | | | | | |
|---|---|---|---|---|---|
| Kim et al.[9] | System-independent data-driven approach | - | - | - | 0.628 |
| Thapa et al.[16] | Deep Learning (DL) based Ensemble models | 96.62% | 0.93 | 0.93 | 0.93 |
| Proposed model | XAI with OD-DRUNN | 99.2% | 98% | 97.9% | 98.4% |

Table 4 shows the comparative analysis of the proposed and existing research frameworks based on precision, recall, F-measure, and accuracy metrics. Based on all the metrics, the proposed methodology achieved higher performance than the existing methods because it preserves the data by XAI and improves the DRNN. The existing DL-based ensemble model achieved 96.62%, which is higher than the other existing methods but is also lower when compared with the proposed model.

## VI. Conclusion

This paper proposed an OD-DRUNN with XAI of proactive defense mechanism in the cyber-security of organizations. Here, the performance of the proposed methodology was assessed with the existing conventional methods and state-of-art works. Based on both comparisons, the proposed approaches achieved higher performance. The accuracy, packet delivery ratio and training time of the OD-DRUNN were 99.2%, 97.8%, and 48762ms, respectively. Also, the error value was also lower for the proposed methodology. Hence, it showed that the research was highly helpful for real-time potential cyber threat detection.

**Future scope:** However, the framework concentrates on specific threats only. In the future, the proposed research will be enhanced by considering various potential threats in proactive defense mechanisms.

## Conflict of intrest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

All authors have participated in (a) conception and design, or analysis and interpretation of the data; (b) drafting the article or revising it critically for important intellectual content; and (c) approval of the final version.

This manuscript has not been submitted to, nor is under review at, another journal or other publishing venue.

The authors have no affiliation with any organization with a direct or indirect financial interest in the subject matter discussed in the manuscript.

## Dataset Availability

The publicly available dataset [21] used in this research work are already cited in reference section.

## References

[1] Aiyanyo, I. D., Samuel, H., & Lim, H. (2020). A systematic review of defensive and offensive cybersecurity with machine learning. Applied Sciences (Switzerland), 10(17), 1–26. https://doi.org/10.3390/app10175811

[2] Alevizos, L., & Ta, V. (2024). TTP-Based Cyber Resilience Index: A Probabilistic Quantitative Approach to Measure Defence Effectiveness Against Cyber Attacks. ArXiv Preprint ArXiv:2406.19374., 1–11.

[3] Almahmoud, Z., Yoo, P. D., Alhussein, O., Farhat, I., & Damiani, E. (2023). A holistic and proactive approach to forecasting cyber threats. Scientific Reports, 13(1), 1–15. https://doi.org/10.1038/s41598-023-35198-1

[4] Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting cybersecurity threats in critical infrastructure for industry 4.0: a proactive approach based on attacker motivations. Sensors, 23(9), 1–17. https://doi.org/10.3390/s23094539

[5] Apruzzese, G., Laskov, P., Montes De Oca, E., Mallouli, W., Brdalo Rapa, L., Grammatopoulos, A. V., & Di Franco, F. (2023). The Role of Machine Learning in Cybersecurity. Digital Threats: Research and Practice, 4(1), 1–38. https://doi.org/10.1145/3545574

[6] Creado, Y., & Ramteke, V. (2020). Active cyber defence strategies and techniques for banks and financial institutions. Journal of Financial Crime, 27(3), 771–780. https://doi.org/10.1108/JFC-01-2020-0008

[7] De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0—A Survey. Electronics (Switzerland), 12(8), 1–18. https://doi.org/10.3390/electronics12081920

[8] Dekker, M., & Alevizos, L. (2024). A threat‐intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision‐making. Security and Privacy, 7(1), 1‐18. https://doi.org/10.1002/spy2.333

[9] Kim, Y., Lee, I., Kwon, H., Lee, K., & Yoon, J. (2023). BAN: Predicting APT Attack Based on Bayesian Network With MITRE ATT&CK Framework. IEEE Access, 11(August), 91949–91968. https://doi.org/10.1109/ACCESS.2023.3306593

[10] Kure, H. I., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2022). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. Neural Computing and Applications, 34(1), 493–514. https://doi.org/10.1007/s00521-021-06400-0

[11] Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G (2020). Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. Resilience Week (RWS), 75, 106–112. https://doi.org/10.1109/RWS50334.2020.9241271

[12] Naseer, I. (2020). Cyber Defense for Data Protection and Enhancing Cyber Security Networks for Military and Government Organizations. MZ Computing Journal, 1(2), 1–8. https://mzjournal.com/index.php/MZCJ/article/view/8

[13] Nassar, A., & Kamal, M. (2021). Traditional rule-based security systems, while effective to some extent, are insufficient to combat the dynamic and evolving strategies employed by cybercriminals. 5(1), 51–62.

[14] Rehman, Z., Gondal, I., Ge, M., Dong, H., Gregory, M., & Tari, Z. (2024). Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception. Computers and Security, 139(December 2023), 103685. https://doi.org/10.1016/j.cose.2023.103685

[15] Tahmasebi, M. (2024). Beyond Defense: Proactive Approaches to Disaster Recovery and Threat Intelligence in Modern Enterprises. Journal of Information Security, 15(02), 106–133. https://doi.org/10.4236/jis.2024.152008

[16] Thapa, N., Liu, Z., Shaver, A., Esterline, A., Gokaraju, B., & Roy, K. (2021). Secure cyber defense: An analysis of network intrusion-based dataset ccd-idsv1 with machine learning and deep learning models. Electronics (Switzerland), 10(15), 1–13. https://doi.org/10.3390/electronics10151747

[17] Trim, P. R. J., & Lee, Y. I. (2022). Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience. Big Data and Cognitive Computing, 6(4), 1–20. https://doi.org/10.3390/bdcc6040110

[18] Xing, J., & Zhang, Z. (2022). Hierarchical Network Security Measurement and Optimal Proactive Defense in Cloud Computing Environments. Security and Communication Networks, 2022(1), 1–12. https://doi.org/10.1155/2022/6783223

[19] Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. IEEE Access, 9, 94318–94337. https://doi.org/10.1109/ACCESS.2021.3087109

[20] Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. Digital Communications and Networks, 8(4), 422–435. https://doi.org/10.1016/j.dcan.2021.07.006

[21] GitHub Dataset: https://github.com/gfek/Real-CyberSecurity-Datasets#-Hikari-2021-Datasets