Enhancing Cybersecurity in Financial Services using Single Value Neutrosophic Fuzzy Soft Expert Set

Alsadig Ahmed[*1]

[1]Applied Management Program, Applied College at Muhyle, King Khalid University, Saudi Arabia
Emails: mamoustafa@kku.edu.sa

Abstract

Cybersecurity has become a primary concern as the financial sectors generally handle increasing cyber-attacks and an increasing danger of financial crime. Recently, ransomware attacks have intensified, affecting enterprises, and crucial infrastructure worldwide. Ransomware employs sophisticated encryption techniques to encrypt data on the targeted device, then requests payment for decrypting the data. Artificial intelligence (AI) approaches involving ML were progressively employed in the domain of cybersecurity and significantly subsidized to preventing and detecting variety of threats. On the other hand, the several researchers that employed ML to identify ransomware are still constrained by the accuracy of models, the complication of malware, the high false-positive rate, and the lack of setting up the appropriate analysis environment. Therefore, there is a need to design efficient ransomware detection based on ML algorithms. This work introduces a modified Single Value Neutrosophic Fuzzy Soft Expert Set (M-SVNFSES) technique for cyberattack detection. The main purpose of the M-SVNFSES system is to detect and recognize the existence of cyberattacks in the financial sectors. In the M-SVNFSES technique, min-max normalization is used as an initial pre-processing stage. For the identification of cyberattacks in the financial sectors, the M-SVNFSES technique uses the SVNFSES model. To enhance its performance, the M-SVNFSES technique makes use of a bat optimization algorithm (BOA). The performance of the M-SVNFSES methodology was extensively studied using financial datasets. The experimental outcomes depicted that the M-SVNFSES method reaches optimal detection performance in attack detection process

Keywords: Ransomware; Cyberattack Detection; Bat Optimization Algorithm; Neutrosophic Fuzzy Soft Expert Set; Machine Learning

1. Introduction

Economic services include an extensive assortment of businesses that handle money, with banks, credit unions, investment funds, insurance businesses, user finance companies, credit card companies, and few government-sponsored companies [1]. These organizations play a vital part in facilitating transactions, global economy, providing credit, and permitting entities and individuals to invest and develop wealth. The initiation of technology has carried about online investment platforms, electronic payment methods, digital banking, and other internet-based economic services [2]. This digital transformation has made economic services more available and useful. However, the alteration to digital platforms has also presented novel tasks, mainly in terms of cyber-security [3].

Economic organizations handle a huge quantity of sensitive and money data, creating them an attractive objective for cyber criminals [4]. Cybercriminals use a range of strategies to affect online money affording organizations utilizing fraudulent mail in order to generate faults in consumers' methods like key loggers, drive-through transferring, phishing emails, and contaminating targets with automatic and trojanized malware with the goal of leading financial fraud by taking consumer accounts [5]. A financial botnet is a system of diseased computers that is handled and established by command and control servers (CCS) to object monetary users. Money-lending Trojans are considered the most overwhelming hazard to economic companies and the main drivers of malignant and botnet congestion actions [6]. Malware, with ransomware, is another general cybersecurity hazard in the economic services sector. Malware is malicious software that can interrupt computer processes, collect sensitive

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

data, or gain illegal access to computer systems [7]. Ransomware is also a kind of malware, that encodes files on a method and demands a payment for their decryption. These threats can be addressed by strong malware protection [8]. This often upgrading and patching methods to fix exposures, installing and upgrading antivirus software, observing network traffic for malware signals, and frequently backing up data to diminish the effect of ransomware attacks [9]. Monetary ransomware is very challenging to classify, recognize, and examine in an automated method owing to its silent feature [10]. A well-recognized model for identifying deviations in system congestion is ML-based classification. The prevention and recognition of system congestion were generally completed utilizing the signature-based models.

This work introduces a modified Single Value Neutrosophic Fuzzy Soft Expert Set (M-SVNFSES) technique for cyberattack recognition. The main objective of the M-SVNFSES algorithm is to identify and recognize the presence of cyberattacks in the financial sectors. In the M-SVNFSES technique, min-max normalization is used as an initial pre-processing stage. For the identification of cyberattacks in the financial sectors, the M-SVNFSES technique uses the SVNFSES model. To enhance its performance, the M-SVNFSES technique makes use of bat optimization algorithm (BOA). The performance of the M-SVNFSES methodology was extensively studied using financial database.

2. Literature Works

Gong et al. [11] utilize DL for innovative threat recognition to enhance defensive measures in the economic industry. The recognition technology mostly utilizes statistical ML models - gathering usual program and network behaviour data, removing multi-dimensional features, and training decision ML methods on this foundation. The authors [12] projected a Rock Hyrax Swarm Optimizer with DL-based Android malware detection (RHSODL-AMD) system. The model projected contains discovering the API and the most major approvals that outcomes in effectual perception among the decent ware and malware users. So, an RHSO-FS model was resultant to enhance the outcomes of classification.

The author [13] presented advanced features personalized to seizure of distinct features of ransomware activity within the crypto-currency network. The paper used a multi-faceted study to explore ransomware-related data covering transaction meta-data, ransom analysis, and economic features. Musonda et al. [14] main goal is to attain numerous objectives linked to Crypto-Ransomware detection. At first, it involved an inspection of present ML structures used in this area and the classification of related tasks. Then, the research concentrated on the establishment of a novel ML method intended for the recognition and investigation of Crypto-Ransomware. At last, the proposed model's efficiency in classifying Crypto-Ransomware was measured.

In [15], an ML classification technique is projected in order to classify ransomware families. The projected research uses numerous ML systems to generate extremely precise methods for categorizing ransomware families. In [16], a Kernel-based Ensemble Meta Classifier (KEMC) Approach is recommended. The PSO and GA intellectual optimizer models were employed in order to initiate the perfect order. The technique protected has been used to estimate Internet cyber security conditions. The Binary Cross-Entropy (loss), GA-PSO, Softsign activation functions, and ensembles can be employed in this research.

3. The Proposed Methodology

In this work, we have introduced an M-SVNFSES technique for cyberattack detection. The major purpose of the M-SVNFSES algorithm is to detect and recognize the presence of cyberattacks in the financial sectors. It contains three different processes such as preprocessing, cyberattack detection using SVNFSES, and BOA-based hyperparameter tuning. Fig. 1 signifies the entire procedure of M-SVNFSES technique.

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

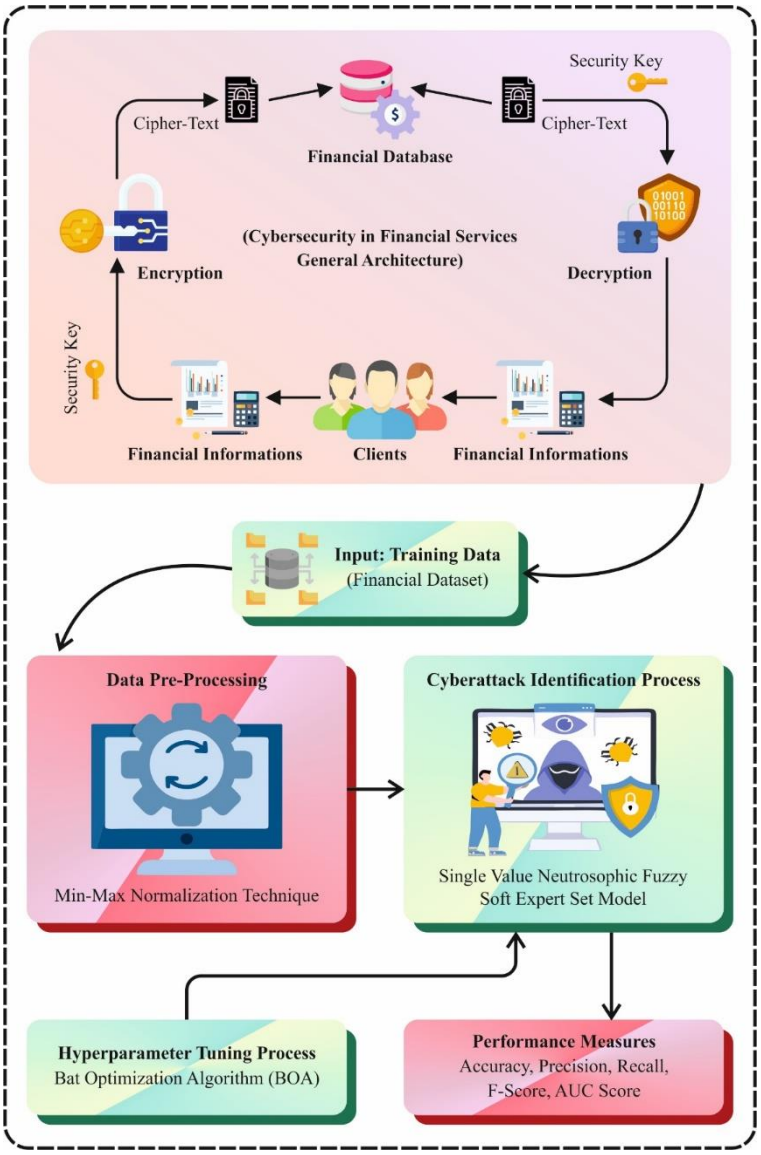

Figure 1: Overall process of M-SVNFSES technique

A. Preprocessing

At initial pre-processing stage, the M-SVNFSES technique, min-max normalization is used. Min-max normalization is popular way for data normalization [17]. For all the features, the least value is rehabilitated to 0, the highest value is renovated to 1, and all the other values get converted into a decimal within [0,1].

B. Cyberattack Detection using SVNFSES

For the identification of cyberattacks in the financial sectors, the M-SVNFSES utilizes the SVNFSES model. The study presents the concept of SVNFES and determines certain properties such as a subset of SVNFES, the null of SVNFES, the equality of SVNFES, and the complete of SVNFES [18].

The well-arranged pair (H, O) is indicative of SNFSESS proceeding U. If

The mapping H: $O \rightarrow SVNFN^U$ but $O \subseteq Z = MxNxY$, thus $z \in Z$ then $z = (m \times n \times y = 0 \; or \; 1)$

$U = \{u_1, u_2, u_3, \ldots, u_s\}, M = \{m_1, m_2, m_3, \ldots, m_s\}, N = \{n_1, n_2, n_3, \ldots, n_s\}$ are reference set (RS), attribute set, and expert sets correspondingly and $Y = \{0,1\}$.

PIVNSS $\mathcal{H}$ on $\widehat{U}$ has the structure:

$$\mathcal{H}^{svnfses} = \{(u, \langle \ddot{\partial}^t_{\mathcal{H}}(z_i)(u_j), \ddot{\partial}^i_{\mathcal{H}}(z_i)(u_j), \ddot{\partial}^f_{\mathcal{H}}(z_i)(u_j)\rangle | u \in \widehat{U}, z \in \widehat{\mathbb{Z}}\}$$

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

Let $\widehat{U}$ has three hotels $\{u_1, u_2, u_3\}$, and the object is estimated by two experts $N = \{n_1, n_2\}$, and the criteria is denoted as $M = \{m_1, m_2, m_3\}$ such that $m_1 = Food\ services, m_2 = Staff, m_3 = Number\ of\ rooms$. Now for $O \subseteq Z = M \times N \times Y$,

$$\mathcal{H}(z_1 = (m_1, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

$$\mathcal{H}(z_2 = (m_1, n_2, 1)) = \left\{\left(\frac{u_1}{\langle 0.5,0.4,0.2\rangle}\right), \left(\frac{u_2}{\langle 0.1,0.5,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.2,0,0.8\rangle}\right)\right\}.$$

$$\mathcal{H}(z_3 = (m_2, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.7,0.6,0.2\rangle}\right), \left(\frac{u_2}{\langle 0.6,0.3,0.1\rangle}\right), \left(\frac{u_3}{\langle 0.2,0.3,0.5\rangle}\right)\right\}.$$

$$\mathcal{H}(z_4 = (m_2, n_2, 1)) = \left\{\left(\frac{u_1}{\langle 0.5,0.3,0.2\rangle}\right), \left(\frac{u_2}{\langle 0.6,0.4,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.5,0.4,0.3\rangle}\right)\right\}.$$

$$\mathcal{H}(z_5 = (m_3, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.7,0.5,0.9\rangle}\right), \left(\frac{u_2}{\langle 0.2,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.3,0.4,0.6\rangle}\right)\right\}.$$

$$\mathcal{H}(z_6 = (m_3, n_2, 1)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

$$\mathcal{H}(z_7 = (m_1, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

$$\mathcal{H}(z_8 = (m_1, n_2, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.6,0.2\rangle}\right), \left(\frac{u_2}{\langle 0.7,0.2,0.5\rangle}\right), \left(\frac{u_3}{\langle 0.1,0.1,0.3\rangle}\right)\right\}.$$

$$\mathcal{H}(z_9 = (m_2, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.5,0.8\rangle}\right), \left(\frac{u_2}{\langle 0.9,0.8,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.1,0.6,0.9\rangle}\right)\right\}.$$

$$\mathcal{H}(z_{10} = (m_2, n_2, 0)) = \left\{\left(\frac{u_1}{\langle 0.3,0.4,0.7\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.4,0.2\rangle}\right), \left(\frac{u_3}{\langle 0.6,0.6,0.2\rangle}\right)\right\}.$$

$$\mathcal{H}(z_{11} = (m_3, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.5,0.6\rangle}\right), \left(\frac{u_2}{\langle 0.1,0.2,0.8\rangle}\right), \left(\frac{u_3}{\langle 0.2,0.4,0.7\rangle}\right)\right\}.$$

$$\mathcal{H}(z_{12} = (m_3, n_2, 0)) = \left\{\left(\frac{u_1}{\langle 0.6,0.8,0.6\rangle}\right), \left(\frac{u_2}{\langle 0.2,0.5,0.6\rangle}\right), \left(\frac{u_3}{\langle 0.4,0.9,0.9\rangle}\right)\right\}.$$

$\mathcal{H}(z_i)$ represents the matrix as follows:

$$\mathcal{H}(z_i) = \begin{pmatrix} ((0.2,0.5,0.3)) & ((0.3,0.6,0.7)) & ((0.8,0.1,0.6)) \\ ((0.5,0.4,0.2)) & ((0.1,0.5,0.7)) & ((0.2,0.0,0.8)) \\ ((0.7,0.6,0.2)) & ((0.6,0.3,0.1)) & ((0.2,0.3,0.5)) \\ ((0.5,0.3,0.2)) & ((0.6,0.4,0.7)) & ((0.5,0.4,0.3)) \\ ((0.7,0.5,0.9)) & ((0.2,0.6,0.7)) & ((0.3,0.4,0.6)) \\ ((0.2,0.5,0.3)) & ((0.3,0.6,0.7)) & ((0.8,0.1,0.6)) \\ ((0.4,0.6,0.2)) & ((0.7,0.2,0.5)) & ((0.1,0.1,0.3)) \\ ((0.4,0.5,0.8)) & ((0.9,0.8,0.7)) & ((0.1,0.6,0.9)) \\ ((0.3,0.4,0.7)) & ((0.3,0.4,0.2)) & ((0.6,0.6,0.2)) \\ ((0.4,0.5,0.6)) & ((0.1,0.2,0.8)) & ((0.2,0.4,0.7)) \\ ((0.6,0.8,0.6)) & ((0.2,0.5,0.6)) & ((0.4,0.9,0.9)) \end{pmatrix}$$

Agree SVNFSES $\mathcal{H}_1$ denotes the agreement of expert's opinion.

$$\mathcal{H}_O = \{H_O(z_i) : z_i \in M\text{x}N\text{x}\{1\}\}$$

$$\mathcal{K}(z_1 = (m_1, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

Disagree SVNFSES $\mathcal{H}_0$ signifies disagreement of expert's opinion.

$$\mathcal{H}_O = \{H_O(z_i) : z_i \in M \times N \times \{0\}\}$$

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

$$\mathcal{K}(z_9 = (m_2, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.5,0.8\rangle}\right), \left(\frac{u_2}{\langle 0.9,0.8,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.1,0.6,0.9\rangle}\right)\right\}.$$

(SVNFSE-subset): Assume $\mathcal{H}_O = (\mathcal{H}, O \subseteq \mathcal{Z})$ and $\mathcal{K}_P = (\mathcal{H}, O \subseteq \mathcal{Z})$ as SVNFSE set on RS $\widehat{U}$. At that time $\mathcal{H}_O$ is SVNFSE-set of $\mathcal{K}_P$ and defined as $\mathcal{H}_O \subseteq \mathcal{K}_P$:

$\mathcal{H}_O(u)$ is SVNFSE-subset of $\mathcal{K}_P(u_i)$, $\forall u_i \in \widehat{U}$.

$$O \subseteq P.$$

$$\mathcal{K}(z_1 = (m_1, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

$$\mathcal{K}(z_9 = (m_2, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.5,0.8\rangle}\right), \left(\frac{u_2}{\langle 0.9,0.8,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.1,0.6,0.9\rangle}\right)\right\}.$$

(Equivalence of SVNFSE-set): Assume $\mathcal{H}_O = (\mathcal{H}, O \subseteq \mathcal{Z})$ and $\mathcal{K}_P = (\mathcal{H}, O \subseteq \mathcal{Z})$ as SVNFSE-set on RS $\widehat{U}$. Then $\mathcal{H}_O = (\mathcal{H}, O \subseteq \mathcal{Z})$ was equal of $\mathcal{K}_P = (\mathcal{H}, O \subseteq \mathcal{Z})$ and illustrated as $\mathcal{H}_O = \mathcal{K}_P$ if:

$\mathcal{H}(u_i)$ refers to SVNFSE-set of $\mathcal{K}(u_i)$ and $\mathcal{K}(u_i)$ refers to SVNFSE-set of $\mathcal{H}(u_i)$, $\forall u_i \in \widehat{U}$.

O is subset of $\mathcal{P}$ and $\mathcal{P}$ is subset of O, $\forall u_i \in \widehat{U}$.

$$\mathcal{H}_O = \begin{pmatrix} (0.2,0503) & (0.3,0.6,0.8) & (0.8,0.1,0.6) \\ (0.5,0802) & (0.2,0.4,0.8) & (0.8,0,0.2) \\ (0.4,0.50.3) & (0.9,0.6,0.8) & (0.8,0.7,0.7) \end{pmatrix}$$

and

$$\mathcal{G}c = \begin{pmatrix} (0.1,0.30.3) & (0.6,0.8,0.8) & (0.8,0.1,0.1) \\ (0.5,0.80.2) & (0.2,0.4,0.8) & (0.8,0,0.2) \\ (0.4,0.7,0.8) & (0.4,0.6,0.8) & (0.8,0.5,0.4) \end{pmatrix}$$

and

$$\mathcal{K}_P = \begin{pmatrix} (0.2,0503) & (0.3,0.6,0.8) & (0.8,0.1,0.6) \\ (0.5,0802) & (0.2,0.4,0.8) & (0.8,0,0.2) \\ (0.4,0.50.3) & (0.9,0.6,0.8) & (0.8,0.7,0.7) \end{pmatrix}$$

Now $\mathcal{H}_O = \mathcal{K}_P$ and $\mathcal{H}_O \neq \mathcal{G}c$.

Next, complement operation of PIVNS-set is given below:

$$\mathcal{H}_O^c = \{(u, \langle \ddot{\partial}_{\mathcal{H}}^f(z_i)(u_j), 1 - \ddot{\partial}_{\mathcal{H}}^i(z_i)(u_j), \ddot{\partial}_{\mathcal{H}}^t(z_i)(u_j)\rangle | u \in \widehat{U}, z \in \widehat{\mathbb{Z}}\}$$

$$\mathcal{H}(z_1 = (m_1, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.2,0.5,0.3\rangle}\right), \left(\frac{u_2}{\langle 0.3,0.6,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.8,0.1,0.6\rangle}\right)\right\}.$$

$$\mathcal{H}(z_9 = (m_2, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.4,0.5,0.8\rangle}\right), \left(\frac{u_2}{\langle 0.9,0.8,0.7\rangle}\right), \left(\frac{u_3}{\langle 0.1,0.6,0.9\rangle}\right)\right\}.$$

$$\mathcal{H}^c(z_1 = (m_1, n_1, 1)) = \left\{\left(\frac{u_1}{\langle 0.3,0.5,0.2\rangle}\right), \left(\frac{u_2}{\langle 0.7,0.4,0.3\rangle}\right), \left(\frac{u_3}{\langle 0.6,0.9,0.8\rangle}\right)\right\}.$$

$$\mathcal{H}^c(z_9 = (m_2, n_1, 0)) = \left\{\left(\frac{u_1}{\langle 0.8,0.5,0.4\rangle}\right), \left(\frac{u_2}{\langle 0.7,0.2,0.9\rangle}\right), \left(\frac{u_3}{\langle 0.9,0.4,0.1\rangle}\right)\right\}.$$

C. Hyperparameter Tuning

Eventually, the M-SVNFSES technique makes use of BOA. The BOA was projected and improved by Yang in 2010 and is often utilized in resolving global optimizer issues [19]. This metaheuristic approach depends on *bi*-sonar or echolocation signals created by the microbats with distinct pulse emission values and loudness. The BOA is exposed in three major principles:

The bat utilizes the echolocation signal for estimating the better distance to the prey or food.

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

For searching for the prey or food, the bat at certain place flies arbitrarily with a specific velocity and set wavelength where the changing frequency and loudness. The bat automatically changes the frequency of its produced pulses and the pulse emission value depends on its nearby prey or food.

The bat linearly reduces its loudness from a huge to a minimal constant rate.

The BOA parameters are the size of population represented as (N), the maximal iteration counts are defined as $iter$, the minimal frequency (f_{min}), the maximal frequency (f_{max}) the initial velocity of bats the initial value of Pulse emission (ro), the problem dimensional $(dims)$, the bat pulse emission rate (γ), and bat loudness (A_l). The initial bat positions are arbitrarily created in Eq. (1). Based on this formula, the position of all the bats defines a possible result.

$$xp_{ij} = xp_j^l + rand( ) * \left(xp_j^u - xp_j^l\right) \tag{1}$$

whereas $i = 1, \dots, N,\ N$ implies the size of populations, $j = 1, \dots, dims$, and x_j^u and x_j^l signifies the up and low position bounds of bat with j dimensional, correspondingly.

The Mean Squared Error (MSE) objective function has been measured as:

$$MSE(i) = \frac{1}{K}\sum_{kk=1}^{K}\left(V_{ref}(kk) - V_o(kk)\right)^2 \tag{2}$$

In which, $i = 1, \dots, N, N$ implies the size of populations, kk denotes the existing instance, K stands for the maximal instance counts, V_{ref} defines the reference voltage, and V_o signifies the actual resultant voltage.

The bat with minimal MSE rate among each bat takes the optimum position (xp^*). The MSE rate of this bat is located as $(f_{\min})$. Accordingly, the frequency, velocity, and position of bats have been upgraded as shown in Eqs. (3)-(5), correspondingly.

$$f_i = f_{\min} + (f_{\max} - f_{\min}) * rand( ) \tag{3}$$

$$v_i^{ii} = v_i^{ii-1} + \left(x_i^{ii-1} - x^*\right) * f_i \tag{4}$$

$$xp_i^{ii} = xp_i^{ii-1} + v_i^{ii} \tag{5}$$

whereas $ii = 1, \dots, Iter$.

For all the bats, when the pulse emission value (γ_i) is lesser than an arbitrary number, a local search has been executed, and an original solution can generated by a random walk for all the bats. This new solution can be employed to improve the variety of the performances as expressed in Eq. (6).

$$xp_i^{new} = xp^* + eps * < A_l >^{ii} \tag{6}$$

In which, eps demonstrates the scaling factor created randomly within range of [-1, 1], and $< A_l >^{ii}$ signifies the average loudness at ii iteration for every bat.

The loudness and Pulse values can be upgraded based on Eqs. (7) and (8), correspondingly.

$$A_{l_i} = \theta * A_{l_i} \tag{7}$$

$$\gamma_i = ro * \left(1 - exp(-\delta * ii)\right) \tag{8}$$

whereas θ and δ indicate the bat parameters within range of zero and one. Fig. 2 represents the steps involved in BOA.

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

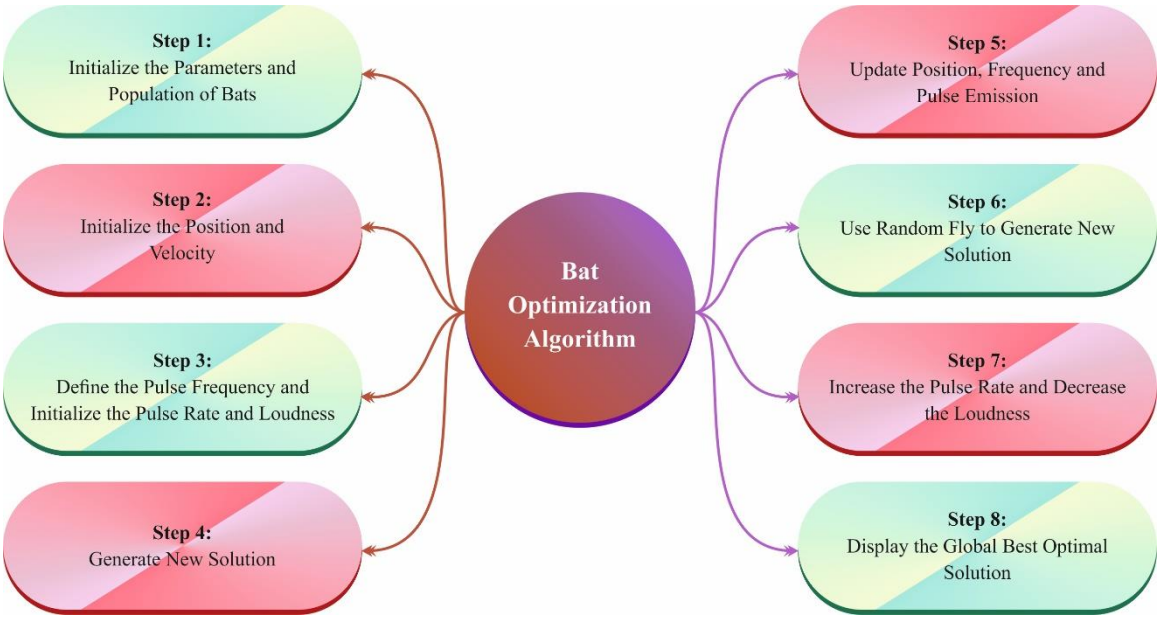

Figure 2. Steps involved in BOA

The BOA develops an FF to reach a superior classifier solution. It resolves a positive integer to define the optimal solution of candidate outcomes. During this case, the decreasing of the classifier error value has been assumed that FF, as provided in Eq. (9).

$$fitness(x_i) = ClassifierErrorRate(x_i)$$
$$= \frac{No.of\ misclassified\ instances}{Total\ no.of\ instances} * 100 \quad (9)$$

4. Experimental Validation

The results of the M-SVNFSES methodology were studied using the ransomware dataset, encompassing 200 instances with 2 classes as illustrated in Table 1.

Table 1: Details of dataset

Classes	No. of instances
Benign	100
Ransomware	100
Total instances	200

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

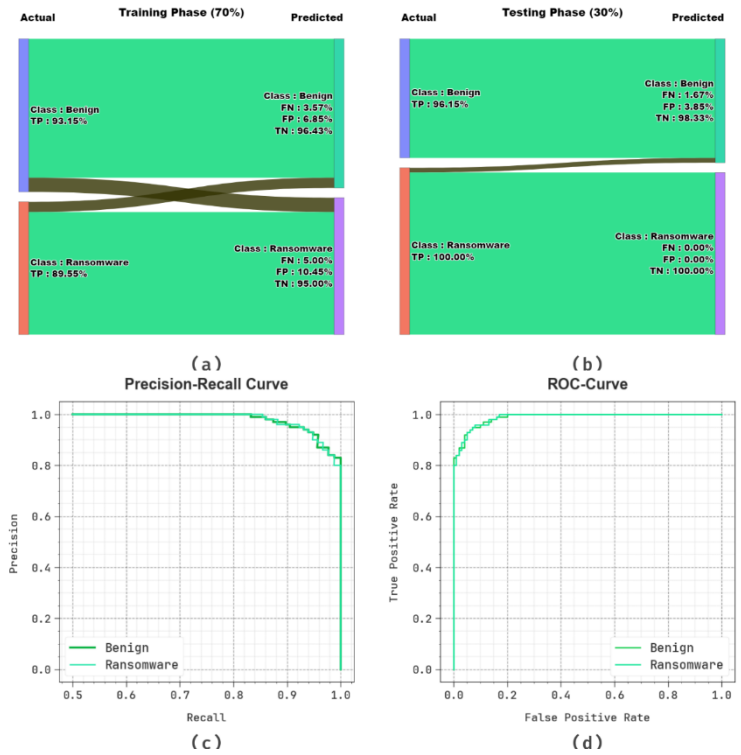

Figure 3: Classifier outcomes of (a-b) 70% and 30% of confusion matrices and (c-d) PR and ROC curves

Fig. 3 portrays the classifier solution of the M-SVNFSES algorithm at test database. Figs. 3a-3b reveals the confusion matrices achieved by the M-SVNFSES methodology on 70%TRAS and 30%TESS. The simulation value defined that the M-SVNFSES technique has classified and detected two classes. Then, Fig. 3c exposes the PR outcome of M-SVNFSES algorithm. The experimental value stated that the M-SVNFSES system takes accomplished highest rates of PR at 2 classes. However, Fig. 3d reveals the ROC curve of M-SVNFSES technique. The experimental value demonstrated that M-SVNFSES system led to capable performances with higher value of ROC at 2 classes.

The ransomware detection results of the M-SVNFSES technique are provided in Table 2 and Fig. 4. The results highlighted that the M-SVNFSES technique appropriately identified the samples. On 70%TRAS, the M-SVNFSES technique offers average $accu_y$ of 91.43%, $prec_n$ of 91.35%, $reca_l$ of 91.49%, F_{score} of 91.40%, and AUC_{score} of 91.49%. Also, on 30%TESS, the M-SVNFSES methodology attains average $accu_y$ of 98.33%, $prec_n$ of 98.08%, $reca_l$ of 98.57%, F_{score} of 98.29%, and AUC_{score} of 98.57%.

Table 2: Ransomware detection outcome of M-SVNFSES technique under 70%TRAS and 30%TESS

Classes	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}	AUC_{Score}
TRAS (70%)					
Benign	91.43	93.15	90.67	91.89	91.49
Ransomware	91.43	89.55	92.31	90.91	91.49
Average	91.43	91.35	91.49	91.40	91.49
TESS (30%)					
Benign	98.33	96.15	100.00	98.04	98.57
Ransomware	98.33	100.00	97.14	98.55	98.57
Average	98.33	98.08	98.57	98.29	98.57

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

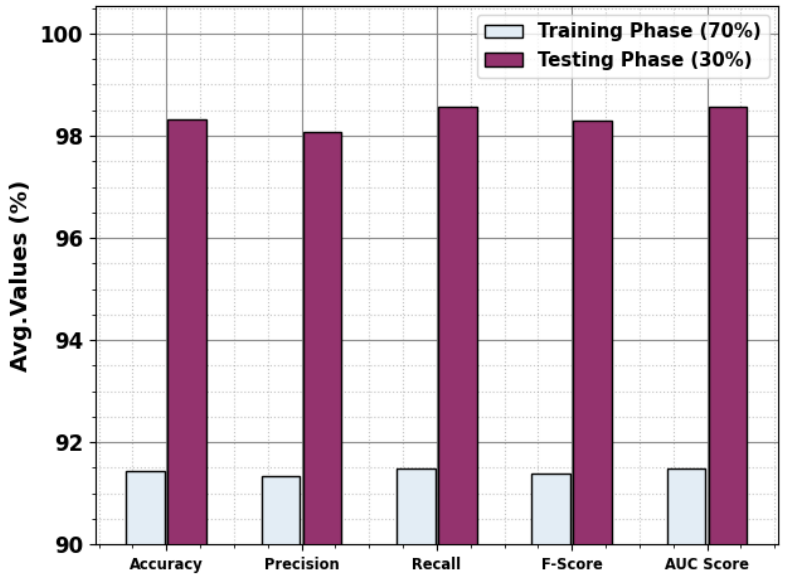

Figure 4: Average of M-SVNFSES technique under 70%TRAS and 30%TESS

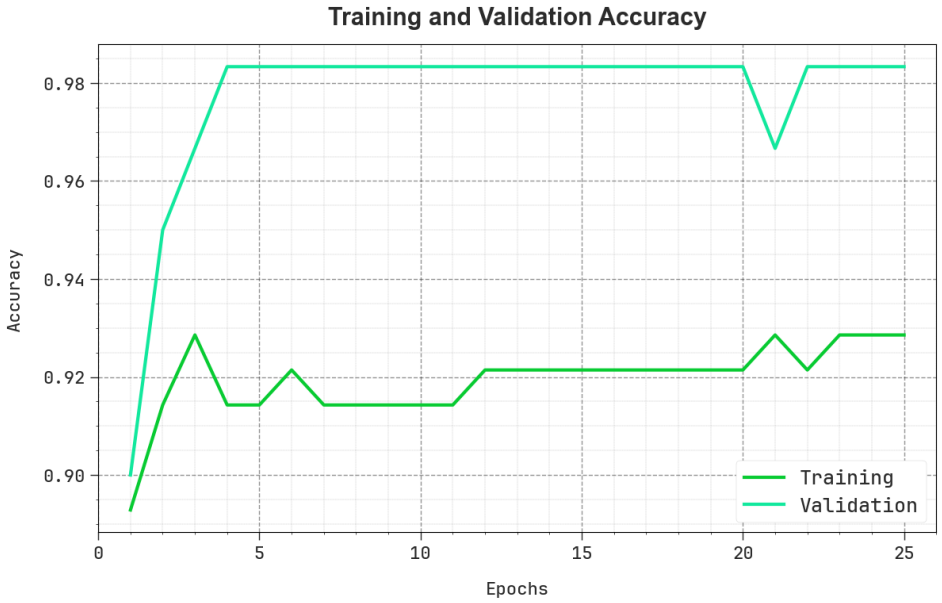

Figure 5: $Accu_y$ curve of M-SVNFSES system

The performance of M-SVNFSES model is graphically projected in Fig. 5 in the procedure of training accuracy (TRAA) and validation accuracy (VALA) outcomes. The outcomes exhibit beneficial interpretation of M-SVNFSES algorithm at various epoch counts, demonstrating its learning method and generalization proficiencies. Noticeably, the outcome supposes a steady improvement from TRAA and VALA with evolvement in epochs. It guarantees the adaptive nature of the M-SVNFSES system from the pattern detection method on both data. The ascending trend in VALA outlines the ability of the M-SVNFSES methodology to adjust to the TRA data and excel in offering accurate classifier of unnoticed data, demonstrating robust generalized capabilities.

Fig. 6 exposes a comprehensive depiction of training loss (TRLA) and validation loss (VALL) curves of the M-SVNFSES algorithm at various epochs. The progressive reduction in TRLA highlights the M-SVNFSES system optimizing the weights and minimizing the classification error on both data. The outcome implies an accurate understanding of the M-SVNFSES algorithm connected with the TRA data, highlighting its proficiency in

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

capturing patterns in both data. Noticeably, the M-SVNFSES algorithm continually progresses its parameters in reducing the changes among the predictive and real TRA classes.

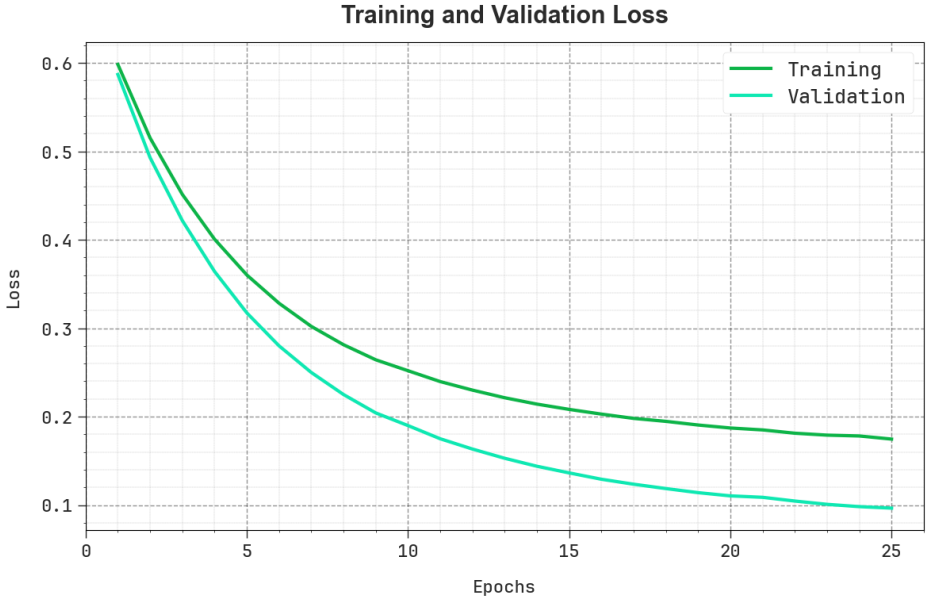

Figure 6: Loss curve of the M-SVNFSES system

In Table 3 and Fig. 7, the performance of the M-SVNFSES methodology is compared with existing models [20]. The outcomes represented the enhanced outcomes of the M-SVNFSES system. It is noticed that the AdaBoost model has attained reduced performance. Meanwhile, LightGBM, ET, and RF approaches have achieved closer outcomes. Furthermore, the XGBoost system has gained considerable performance with $accu_y$ of 97.85%, $prec_n$ of 97.12%, $reca_l$ of 98.06%, and F_{score} of 97.58%. Nevertheless, the M-SVNFSES technique gains better performance with maximum $accu_y$ of 98.33%, $prec_n$ of 98.08%, $reca_l$ of 98.57%, and F_{score} of 98.29%. Thus, the M-SVNFSES methodology was executed for ransomware detection and classification processes.

Table 3: Comparative analysis of M-SVNFSES technique with recent methods

Model	$Accu_y$	$Prec_n$	$Reca_l$	F_{Score}
XGBoost	97.85	97.12	98.06	97.58
LightGBM	96.14	95.19	96.12	95.65
Extra Tree (ET)	96.57	97.03	95.15	96.08
Adaptive Boosting (AdaBoost)	93.99	94.06	92.23	93.14
Random Forest (RF)	97.00	95.28	98.06	96.65
M-SVNFSES	98.33	98.08	98.57	98.29

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

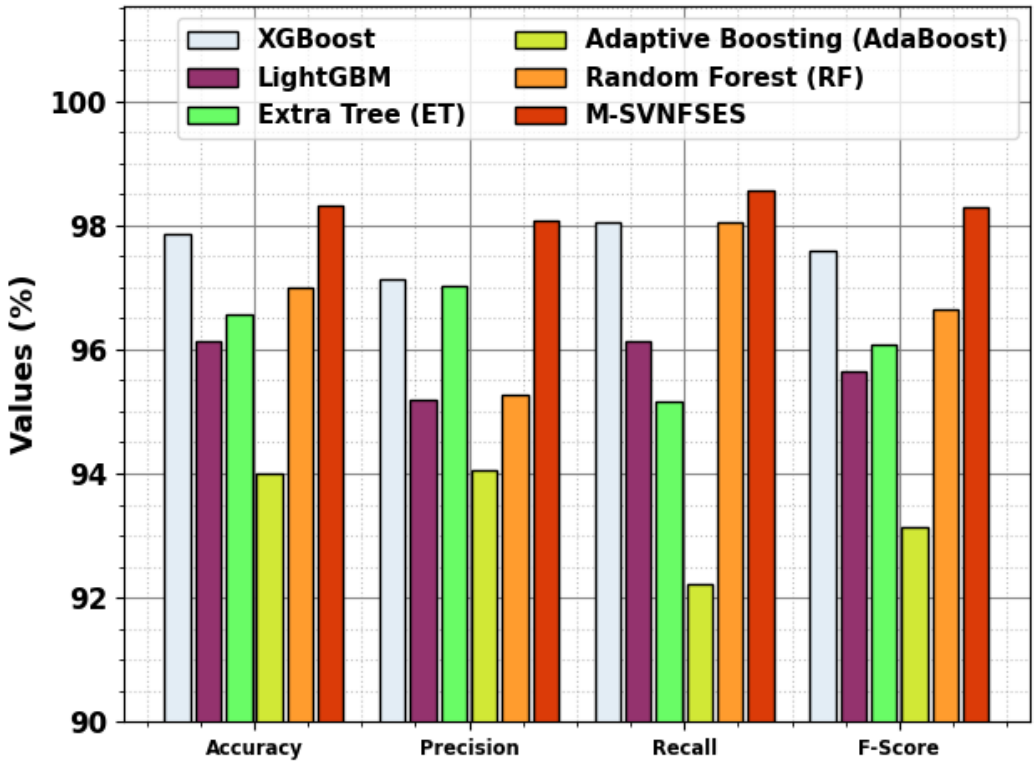

Figure 7: Comparative outcome of M-SVNFSES system with recent methods

5. Conclusion

In this work, we have introduced an M-SVNFSES technique for cyberattack detection. The major purpose of the M-SVNFSES algorithm is to detect and recognize the presence of cyberattacks in the financial sectors. It contains three different processes such as preprocessing, cyberattack detection using SVNFSES, and BOA-based hyperparameter tuning. At initial pre-processing stage, the M-SVNFSES technique, min-max normalization is used. For the identification of cyberattacks in the financial sectors, the M-SVNFSES technique uses the SVNFSES model. To enhance its performance, the M-SVNFSES technique makes use of BOA. The performance of the M-SVNFSES algorithm was extensively studied using financial datasets. The experimental outcome demonstrated that the M-SVNFSES system reaches optimal detection performance in the attack detection process.

Funding: "The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through a Small-group Research Project under grant number (RGP.1/309/44)"

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

References

[1] Sharmeen, S., Ahmed, Y.A., Huda, S., Koçer, B.Ş. and Hassan, M.M., 2020. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access, 8, pp.24522-24534.

[2] Al-Hawawreh, M. and Sitnikova, E., 2019, August. 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 (pp. 126-130).

[3] Manjezi, Z. and Botha, R.A., 2019. Preventing and Mitigating Ransomware: A Systematic Literature Review. In Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17 (pp. 149-162). Springer International Publishing.

[4] Al-Alawi, A.I. and Al-Bassam, M.S.A., 2020. The significance of cybersecurity system in helping managing risk in banking and financial sector. Journal of Xidian University, 14(7), pp.1523-1536.

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024

[5] Hirano M, Kobayashi R. Machine Learning-based Ransomware Detection Using Low-level Memory Access Patterns Obtained From Live-forensic Hypervisor. In 2022 IEEE International Conference on Cyber Security and Resilience (CSR). 2022.
[6] Singh A, Ikuesan RA, Venter H. "Ransomware detection using process memory," arXiv preprint arXiv:2203.16871, 2022.
[7] Medhat M, Essa M, Faisal H, Sayed SG. Yaramon: A Memory-based Detection Framework for Ransomware Families. In 2020 15th International Conference for Internet Technology and Secured Transactions (ICITST). 2020.
[8] Dener M, Ok G, Orman A. Malware detection using memory analysis data in big data environment. Appl Sci 2022;12:8604.
[9] Mishra, R., Butakov, S., Jaafar, F. and Memon, N., 2020, August. Behavioral Study of Malware Affecting Financial Institutions and Clients. In 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 79-86). IEEE.
[10] Cyriac, N.T. and Sadath, L., 2019, November. Is Cyber security enough-A study on big data security Breaches in financial institutions. In 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (pp. 380-385). IEEE.
[11] Gong, Y., Zhu, M., Huo, S., Xiang, Y. and Yu, H., 2024. Enhancing Cybersecurity Resilience in Finance with Deep Learning for Advanced Threat Detection. arXiv preprint arXiv:2402.09820.
[12] Albakri, A., Alhayan, F., Alturki, N., Ahamed, S. and Shamsudheen, S., 2023. Metaheuristics with deep learning model for cybersecurity and Android malware detection and classification. Applied Sciences, 13(4), p.2172.
[13] Nkongolo Wa Nkongolo, M., 2024. RFSA: A Ransomware Feature Selection Algorithm for Multivariate Analysis of Malware Behavior in Cryptocurrency. International Journal of Computing and Digital Systems, 15(1), pp.893-927.
[14] Musonda, M., Zimba, A. and Sinyinda, M., 2023, December. Machine learning-based crypto ransomware detection model on windows platforms. In Proceedings of International Conference for ICT (ICICT)-Zambia (Vol. 5, No. 1, pp. 141-147).
[15] Florence, S.M., Raghava, A., Krishna, M.Y., Sinha, S., Pasagada, K. and Kharol, T., 2024. Enhancing Crypto Ransomware Detection Through Network Analysis and Machine Learning. In Innovative Machine Learning Applications for Cryptography (pp. 212-230). IGI Global.
[16] Jagan, S., Ashish, A., Mahdal, M., Isabels, K.R., Dhanke, J., Jain, P. and Elangovan, M., 2023. A meta-classification model for optimized ZBot malware prediction using learning algorithms. Mathematics, 11(13), p.2840.
[17] Henderi, H., Wahyuningsih, T. and Rahwanto, E., 2021. Comparison of Min-Max normalization and Z-Score Normalization in the K-nearest neighbor (kNN) Algorithm to Test the Accuracy of Types of Breast Cancer. International Journal of Informatics and Information Systems, 4(1), pp.13-20.
[18] Al-Sharqi, F., Al-Quran, A., Khalifa, H.A.E.W., Alqahtani, H., Yousif, B.A.A., Rawan, A. and Aladil, M., Orthogonal distance and similarity for single-valued neutrosophic fuzzy soft expert environment and its application in decision-making.
[19] Wang, Y., Wang, P., Zhang, J., Cui, Z., Cai, X., Zhang, W. and Chen, J., 2019. A novel bat algorithm with multiple strategies coupling for numerical optimization. Mathematics, 7(2), p.135.
[20] Aljabri, M., Alhaidari, F., Albuainain, A., Alrashidi, S., Alansari, J., Alqahtani, W. and Alshaya, J., 2024. Ransomware detection based on machine learning using memory features. Egyptian Informatics Journal, 25, p.100445.

DOI: https://doi.org/10.54216/IJNS.240222
Received: October 12, 2023 Revised: February 14, 2024 Accepted: May 02, 2024