Computer Software and Media Applications 2024, 7(1), 5224.
https://doi.org/10.24294/csma.v7i1.5224

Article

Ftdho Zfnet: Block chain based Fractional Tasmanian Devil Harris optimization enabled deep learning using attack detection and mitigation

S. Sengamala Barani, R. Durga*

Department of Information Technology, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai 600117, India

*** Corresponding author:** R. Durga, drrdurgaresearch@gmail.com

CITATION

Barani SS, Durga R. Ftdho Zfnet: Block chain based Fractional Tasmanian Devil Harris optimization enabled deep learning using attack detection and mitigation. Computer Software and Media Applications. 2024; 7(1): 5224. https://doi.org/10.24294/csma.v7i1.5224

ARTICLE INFO

Received: 14 March 2024
Accepted: 7 April 2024
Available online: 4 June 2024

Abstract: Block chain technology is regarded for enhancing the characteristics of security because of decentralized design, safe distributed storage, and privacy. However, in recent times the present situation of block chain technology has experienced some crisis that may delay the quick acceptance and utilization in real-time applications. To conquer this subdues, a blockchain based system for attack detection and mitigation with Deep Learning (DL) named Fractional Tasmanian Devil Harris Optimization_Zeiler and Fergus network (FTDHO_ZFNet) is introduced. In this investigation, the entities utilized are owner, block chain, server, trusted authority and user. Here, authentication phase is done by means of Ethereum block chain by Key Exchange module and privacy preserved data sharing and communication is also done. Then, recorded log file creation is executed by the below mentioned stages. At first, a log file is generated with the basis of communication to record the events. After wards, the features are extracted by BoT-IoT database. Then, feature fusion is done by overlap coefficient utilizing Deep Q-Network (DQN). Moreover, data augmentation (DA) is doneusing bootstrapping method. At last, attack detection is observed by ZFNet tuned by FTDHO. Here, FTDHO is unified by Fractional Tasmanian Devil Optimization (FTDO) and Harris Hawks Optimization (HHO). Additionally, FTDO is integrated by Fractional Calculus (FC) concept and Tasmanian devil optimization (TDO). Furthermore, attack mitigation is performed. The performance measures applied for FTDHO_ZFNet are accuracy, and True Negative rate (TNR), observed supreme values with 92.9%, 93.8% and 92.9%.

Keywords: block chain technology; attack detection and mitigation; Deep Q-Network (DQN), Harris Hawks Optimization (HHO); Tasmanian Devil Optimization (TDO)

1. Introduction

Blockchain is established with the intent of generating robust sharing database, which discards the requirement for central authorization. This turns out be one of the enhanced technologies over the past decades and deployed in healthcare, voting, supply chains, finance, and internet of vehicles (IoV), art and other sectors. In Blockchain database, the data is distributed by entire users that defined as nodes yet it may not be altered on Blockchain managed by a system known as consensus module [1]. The Blockchain enhancement provides unchallengeable, trustless, and de-centralized ledger applies for revolutionizing monetary transmits with other applications [2]. A distributed ledger module depends on peer to-peer network (P2P) is a new determination prototype with trustless distribution since it has transparency, decentralization, resistance to tampering, and programmability [3,4]. Nevertheless, it had inherent weaknesses of the block chain network layer like architectural heterogeneity, complex management and incompatible network protocol; it experiences more network layer security threats [3]. Kademlia DHT structural graph [4] is employed amongst block chain network layer nodes for exchanging the significant ledger state information and hence the attackers may target the structural security vulnerabilities and launch network traffic attacks for capturing unlawful interests. Once network layer attacks like large-scale eclipse attacks, Sybil and Erebus attacks, and attacked subnet are suffered, network distribution creates in block chain network layer where its node resources cut off from primary network of prime network of block chain. The incessant enhancement and widespread utilization of Internet promote more network users from quantity of feature [5].

Network security is one of essential part along with the utilization of network, which is relevant to computers, networks, programs, various data, and so on, wherein the principle of defense is deployed for preventing unauthorized access and alteration. Nevertheless, the enhancing number of internet-connected systems in finance, E-commerce, and military creates it as network attack targets that result in enormous amount of risk and damage quantity. Most significantly, it is significant for providing effectual techniques to predict and protect attacks and control network privacy. Moreover, several types of networks needed to be progressed in several manners and how to recognize those various kinds of network attacks, therefore the prime challenge in network security need to be resolved [6]. The attack detection and mitigation is also referred as stateful firewall that prevents the attacks in network traffic. This enhancement may be either information gathering search or an attack to cooperate, immobilize, or damage a network resource. The ability for supporting an autonomous process and communications, Internet of Things (IoT) is currently play a vital role in real world since IoT is capable for supporting these functions [7]. The constant utilization of security protection approaches at minimal levels and effortlessness with the devices may be accessed from everywhere through internet, the conventional systems of IoT are vulnerable to a large diversity of security attacks, where these attacks are specifically damaging since they may negotiate the reliability of sensitive data [8].

The privacy threat linked with IoTs ecosystem is essentially larger than conventional network, which is due to the enhanced prospective for malicious attacks for taking control of significant structures such as significant sensors, migrating vehicles as well as nuclear facilitates creates damage [8]. Deep reinforcement learning (DRL) agents are trained to determine the ideal system parameters in response to the network status, and they are utilized to adaptively maximize the security level and system throughput in order to accomplish this goal. According to the simulation results, the suggested DQNSB scheme maintains a high security level while offering a significantly greater TPS than the current DRL-enabled blockchain technology [6]. Cyber attack detection is deployed to detect and respond for malicious or unauthorized tasks in networks, computer systems, and digital environments. Effectual cyber attack detection and prevention provided for integrality by degrading economic loss, electronic waste, controlling trust, enhancing energy efficacy, introducing dependable digital transformation, assuring supply chain flexibility and conserving strong environmental damage [9]. Several Machine Learning (ML) modules are developed for attack detection and mitigation. Some of the approaches have limitations like Genetic Algorithm (GA), which had more complexity, simple for falling into premature concurrence and it is based on initial population as well as Particle Swarm Optimization (PSO)drops rapidly into local optimum and reduced management on discrete optimization issues [10].

The organization of this research is to implement a block chain-based module for attack detection and mitigation using DL named FTDHO_ZFNet. The entities employed here are owner, blockchain, server, trusted authority and user. Here, authentication stage is carried out with Ethereum block chain using Key Exchange module and privacy preserved data distribution and communication is also performed and then recorded log file creation is progressed by the further progress. A log file is generated and features are extracted by BoT-IoT database. Thereafter, feature fusion is done using overlap coefficient with DQN. After that, DA is done by bootstrapping technique. Lastly, attack detection is accomplished by ZFNet trained by FTDHO, and then attack mitigation is also achieved.

Proposed FTDHO_ZFNet for attack detection and mitigation: A novel technique is developed for attack detection and mitigation named FTDHO_ZFNet. Here, FTDHO is combined by FTDO and HHO, where FTDO is obtained by FC and TDO. The attack is detected by using proposed ZFNet that is trained by FTDHO; in addition to that attack mitigation is also observed.

The remaining part of this approach is followed by: In section 2, the knowledge of former techniques of attack detection and mitigation along with its challenges. The fragment 3 exploits the systematic model of this research. The segment 4 deliberates the proposed methodology. In segment 5, the finest resultant of FTDHO_ZFNet is elucidated and concludes with future work in segment 6.

2. Motivation

Attack detection and mitigation structure requires having adequate ability for accommodating attack volume, support the diverge range of attack detection and obtain accurate and rapid attack detection with minimal collateral damage for valid traffic. Henceforth, attack detection and mitigation are a challenging one. The investigators got motivated by the difficulties learned through prior modules of attack detection as well as mitigation and decided to design a module based on this.

2.1. Literature survey

Pros and cons of various papers—analysis of literature survey (**Table 1**).

Table 1. Literature survey.

Ref	Year of Publication	Pros	Cons
Sanda, O., et al. [1]	2023	Introduced Deep Learning (DL) module. This module was deployed as mitigating checkpoint for maximal range attacks on Proof-of-Stake (PoS) based block chains.	Nevertheless, it was unable to improve security, performance as well as produce equality on proof-of-stake consensus
Dai, Q., et al. [5]	2022	Established Convolutional Neural Network (CNN) approach. This approach exhibited essential enhancement while comparing to prior detection modules and classical ML algorithms	However, this technique had less sensitivity.

Table 1. (*Continued*).

Ref	Year of Publication	Pros	Cons
Jia, B. and Liang, Y., [2]	2020	Developed Anti-D Chain technique. Even though, module introduced here attained supreme outcomes with appropriate performance,	it obtained high computational complexity
Albakri, A., et al. [9]	2022	Established block chain-assisted hybrid metaheuristics with a machine learning-based cyber attack detection and classification (BHMML-CADC) algorithm. This module surpassed with extreme outcomes with maximal outputs.	Nevertheless, it did not discover the applications of block chain-based ML for cyber attack detection in several fields behind conventional IT networks, like critical structure security, autonomous vehicles, or smart cities
Jiang, S., et al. [11]	2017	Block chain-based SDN-targeted DDoS defense framework (BSD-Guard). This system appropriately detected the DoS/DDoS attacks in numerous controllers' environment and concerns where the precise protective schemes near source of attack by recognizing attack path.	However, blacklists stored on block chain and computerized implementation of smart contracts did not avert being corrupted by cruel attackers.

2.2. Challenges

The drawbacks acquired while reviewing the conventional techniques in **Table 1** are described as follows.

1) A DL approach designed [1] provided highly effective outcomes, yet it did not utilize use reinforced learning for learning about malicious nodes and several kinds of malicious activities done by validator nodes on PoS block chain.
2) The developed technique in Eclipse Attack detection BC Network Layer [2] achieved stronger generalization assessment. Nevertheless, the artificial block chain in this technique neglected to guide DDoS attack defense in actual block chain.
3) CNN module [5] did not degrade the complexity for the enhancement of real-time assessment of eclipse attack detection in complex blockchain network layer environment.
4) The scheme established in vision-based mobile robot learning by deep Q-network [11] was more lightweight. However, Software defined network DN controller did not managed well as well as normal service traffic was notimpacted by defense policy.
5) In recent times, the entire investigations based on attacks and threats reveals denial-of-service attack is the prime concerns for smart grids. A network attack rendered the smart grid terminal since smart grids are generating a network.

3. System model

In this module, the system module based on attack detection and mitigation are briefly described in the below segments.

3.1. Authentication

Once data encryption is progressed, authentication progress is implemented. The user given an authentication request J to server by,

$$J = k[(G_{id}||l) \oplus mod\, n] \oplus v \tag{1}$$

here, $v = 16\mu^4 + 8\mu^2 + 14\mu$, and $\mu = k\left(G_{pwd}||n\right)$. The user id G_{id} is merged with security factor l, and final outcome is XORed with modulus value of n, and hashing function is used. The resultant is XORed with Chebyshev polynomial v for creating an authentication request J. After receiving the request, it compared them with saved request $\sim J$. If a request meets saved request, a server validates user request and transmits message to Trusted Authority

$$(\text{TA}M = k(R_s \oplus G_{id}^{**}) \oplus N \tag{2}$$

here, N indicates timestamp. The message M is created with EXORing timestamp T together with hashed valued of EXORed outcome of private key $R_s$and user ID G_{id}^{**}. Based on obtainingamessage M, TA validates time stamp, and when a message $\sim M$ is confirmed, session progress is sustained, or it is concluded. The confirmed message is formulated by

$$\sim M = k(R_s^* \oplus G_{id}^{****}) \oplus N \tag{3}$$

M is created by XORing hashed value of user ID G_{id}^{***} along with private key R_s^* and then XORing aresultant with timestamp N. If a session is not concluded, TAtransmits One Time Token (OTT) to user that is represented by

$$OTT = k\left[\left(G_{pwd}^{****} \oplus s\right)||R_X\right] \tag{4}$$

here, hashed value of secret key X_R merged with XORed value of security factor$s$ and stored user password G_{id}^{***} provides OTT, which is given to a user, wherein a replica of OTT is stored as OTT^*, and it is subjected again to TA for user authentication. When a created OTT and obtained OTT are equivalent, TA authenticates a user.

3.2. Block chain system model

Block chain technology provides secure cryptographic approaches for detecting and authorizing users thus produce an access control in an appropriate manner. Block chain technology is a better one for effectual management of data. Normally, block chain has a collection of information linked with chain on blocks referred as group of user devices, which remains data based on specific transactions like financial. Block chain controls more information determinedly consistent since some approaches develops over the enhancement of block chain obtain secure distribution of data amongst illegal users. For example, when a client 'X' decided to broadcast secure descriptions to user 'Y', information is ensured by more number of nodes and management of information is represented as user 'X', which transmits an information with channel to 'Y' who is a current undertaker. The verification exchanged ownership is registered in public repository for next sources. When threat occurs in such situation, assuring the nodes may recognize features and resolve the issues. There is a need for repository that is safe and unchallengeable. The block chain is meant for secure data distribution as well as trustless transaction execution [14]. Block chain is composed of data upload and model download. This assures data distribution privacy yet total information cannot be larger because of several computing ability of user limitations. Consequently, every user is a data uploader and demand requester when participating with less scale global data distribution [15]. The systematic view of block chain is designed in **Figure 1**.

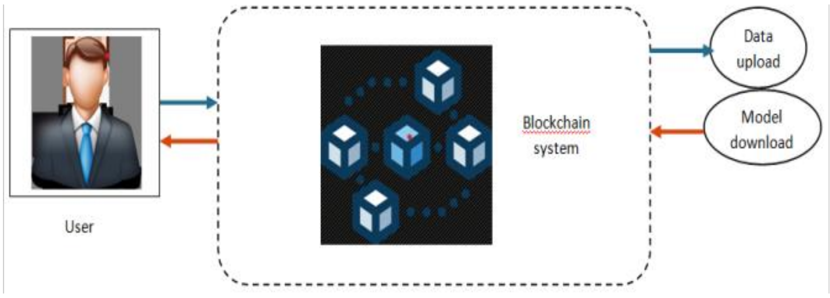


Figure 1. Systematic illustration for blockchain for privacy preserved data sharing.

4. Proposed Ftdho_Zfnet for attack detection and mitigation

The prime intention of this exploration is to implement an attack detection and mitigation in blockchain utilizing Deep Learning based on hybrid optimization named FTDHO_ZFNet. The entities involved in this investigation are owner, blockchain, server, trusted authority and user. In this exploration, authentication phase is performed on the basis of Ethereum block chain utilizing Key Exchange mechanism and privacy preserved data sharing and communication is also carried out. After that, recorded Log file creation is processed by employing the following stages. Initially, a log file is created based on the communication for recording the events. Then, the features are extracted using BoT-IoT dataset [16]. Afterwards, the extracted features are fused together in feature fusion section by employing overlap coefficient with DQN [17,18]. Thereafter, data augmentation is conducted by means of bootstrapping technique. Finally, attack detection is accomplished by ZFNet [19] that is trained by FTDHO, where FTDHO is integrated by FTDO and HHO [20]. Moreover, FTDO is designed by incorporating FC concept [21] and TDO [22]. Moreover, attack mitigation is performed. **Figure 2** displays illustrative diagram of FTDHO_ZFNet for attack detection and mitigation.

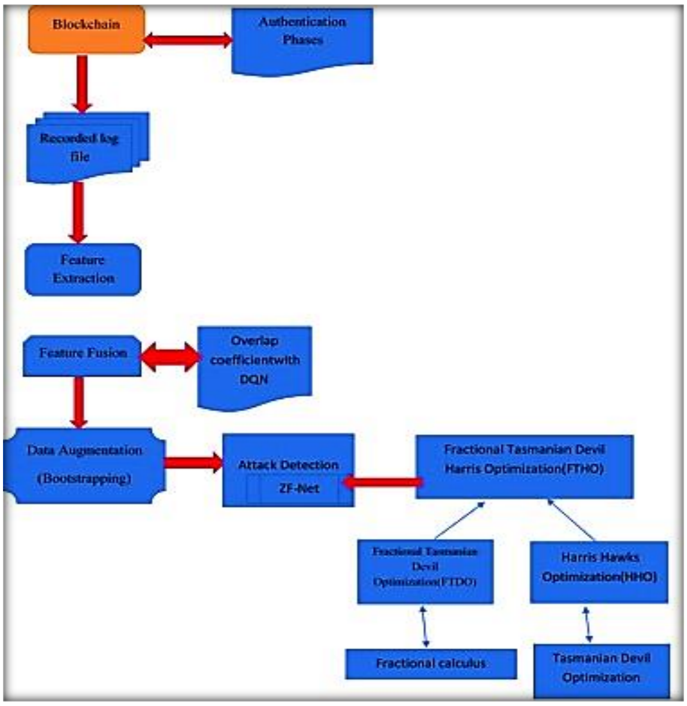

Blockchain
Authentication Phases
Recorded log file
Feature Extraction
Feature Fusion
Overlap coefficientwith DQN
Data Augmentation (Bootstrapping)
Attack Detection ZF-Net
Fractional Tasmanian Devil Harris Optimization(FTHO)
Fractional Tasmanian Devil Optimization(FTDO)
Harris Hawks Optimization(HHO)
Fractional calculus
Tasmanian Devil Optimization

Figure 2. Block diagram of FTDHO_ZFNet for attack detection and mitigation.

A. Data Acquisition

Let us assume a standard database for detecting and mitigating the attack with b number of data that is originated as,

$$A = \{A_1, A_2, \ldots. A_a, \ldots\ldots A_b\} \tag{5}$$

here, database defines A, A_a implies a^{th} input data deployed for entire progression and A_b considers total count of data.

B. Feature Extraction

It is a progress of dimensionality degradation where collection of data is considered as well as transformed them into group of features for easier progress. The input data A_a is forwarding to feature extraction stage, where the proper feature vectors are acquired using BoT-IoT features, which is computed as,

$$F_a = \{f_1, f_2, \ldots. f_m\} \tag{6}$$

here, obtained extracted feature signifies F_a and m implies total features.

C. Feature Fusion using overlap coefficient with DQN

This method is based on the combination of extracted features from several databases for obtaining only one feature file. The extracted feature F_a is allowed for fusion process, which is conducted using DQN in accordance with overlapping coefficient.

1) Arranging features by overlap coefficient

The extracted feature F_a is effectually classified employing overlap coefficient by evaluating the similarity amongst two distributions by,

$$O = \frac{|M \cap N|}{min(|M|, |N|)} \tag{7}$$

here, dimension of distribution setindicates M and N. Here, the features classified by overlap coefficient are implied as D_a^d.

2) Fusion of features

Normally, feature fusion is done for effectually discoverclassified features to incorporaterelevant information for improving the accuracy of detection task that is computed by

$$A = \sum\nolimits^{B}_{\substack{d=1 \\ d=d+\frac{E}{B}}} \frac{\alpha}{K} D_a^d \tag{8}$$

here, entire features signify E and B enumerates selected features. Furthermore, $z = \frac{\mathrm{E}}{\mathrm{B}}$, where $1 \leq K \leq G$ and coefficient denotes σ.

3) Generateσemploying DQN

In this model, the coefficient σ is produced by employing DQN that is formulated as

$$\sigma = O[RD, \beta] \tag{9}$$

here, recorded data signifiesRD, $D_a$exploits overlap coefficient, and β enumerates average data belongs to the class.

a) Architecture of DQN

DQN [17,18] deploys CNN and Q-learning approach for estimation of action-value function. The reinforcement learning is unbalanced or differed when action value function represented utilizing nonlinear function. The variations in data distribution by minute renew of Q-value and correlation of state observations createsunsteadiness of technique. Therefore, for conquering this issue, DQN deploys replay approach. Multi-layered network action value $k(p,m,\alpha)$ for resultant vector f and its loss, which is computed as,

$$H_o(\gamma_o) = I_{g,h,i,H`}\left[\left(P_o - \ell(g,h,\gamma)\right)^2\right] \tag{10}$$

whereas,

$$P_o = \left(j + \upsilon\, max_c \quad \ell(g',h',\gamma^{-\prime})\right) \tag{11}$$

here, γ_o defines online-network factor, U_a enumerates expected error stored by γ_o, γ^- indicates factor alienated from targeted network, c defines action, reward denotes j, g symbolizes multiple-layered neural network state, discount parameter exploits υ, and I_o indicates target considered for deliberating network factor, $\ell(g',h',\gamma^{-\prime})$ enumerates mean loss function error. Therefore, target and gradient network employed for increasing learning updates that is,

$$\nabla_{\gamma_o} H_o(\gamma_o) = P_{g,h,i,H`',}\left[\left(I_o - \ell(g,h,\gamma)\right)\nabla_{\gamma_o}\ell(g,h)\right] \tag{12}$$

Henceforth, the maximal ability is set for degrading associated functions, and creates replay memory; prior outcomes are transferred for updating the network. The fused feature is signified as D_a with dimension $x \times z$. **Figure 3** reveals DQN structure, where the coefficient α is generated when classified features D_a^d given to DQN.

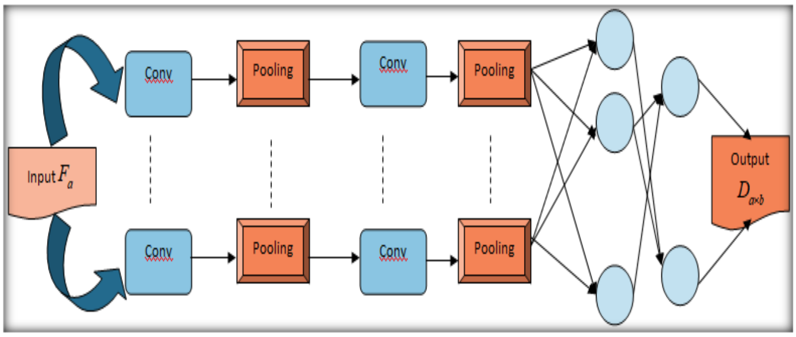


Figure 3. Illustrative diagram of DQN structure.

D. Data Augmentation

It refers the group of techniques for dynamically increasing the total amount of data points from existing data. In this process, fused feature D_a with dimension $x \times z$ isallowed to DA, where the data is augmented by utilizing boot strapping technique.

1) Boot strapping technique

Bootstrap technique [23] is a resampling approach deployed for evaluating the statistics on population with sampling a database with alternate solution iteratively and then this technique selected the sample dimension and number of repetitions. This is employed for analyzing statistics like mean or standard deviation deployed in ML for determining an effectualness of ML when predicting the data, which is not involved in training data.

The augmented data is illustrated as B_a with dimension of $c \times z$.

E. Attack detection

Attacks might be identified as an effort for avoid security policy of system that provides attackers for simple access to attain or alter the information by demolishing the system. Several types of attacks for cyber systems, like flooding, abnormal packet attack, and spoofing are present in the attack system. So, the investigators developed number of solutions for conquering these kinds of attack threats. Amongst these solutions, attack detection is an effectual way that furnishes a dynamic security method for controlling, prohibiting, and opposing the attacks. In this enhancement, the augmented data B_a with dimension of $c \times z$ is forwarded to detection unit to detect the attack using ZF-Net, which is trained by utilizing FTDHO, where FTDHO is the combination of FTDO and HHO; moreover, FTDO is obtained by FC and TDO.

1) Structure of ZFNet

ZFNet [19] architecture is composed of convolution (conv) layer, max-pooling layer and fully connected (FC) layer. Here, the depth of every layer describes about the kernels, pooling or filter implies about the kernel dimension and strides described about the transmission of kernels. Here, Rectified Linear Unit (ReLU) deployed as activation function and softmax deployed as loss function in final layer for classifying database.

a) Convolution layer

In the place of transmitting image into 1D array, the CNNs conducts conv progress over input image. The minute matrices known as filters are randomly progressed in convstage. The kernels are transmitted all over the area and increased at each position. Every multiplication provides single outcome and thus the final outcome has degraded dimensions, where the progress of increasing all over the area with filters defines conv layer. In this layer, four major factors are considered such astotal kernels, kernel dimension, stride and padding controls image dimension.

b) Pooling layer

The operation of pooling layer is to degrade spatial dimension of image for representing the reduced amount of factors and network computation, and for managing over-fitting. This layer is frequently shown amongst successive conv layer for providing translation invariance. Max pooling is the commonly employed, where maximal number from sub-matrices present in input image and considered as an outcome, by transmitting strides formleft to rightas well as top to bottom.

c) Fully connected layer

Artificial Neural Network (ANN) is designed withinput layer wherein an image is flattened to 1D array, hidden layers that comprises activation function output layer are parallel to total classes. The obtainedresultant compared with original outcomes and determine the loss for modifying matrices elements, thus the loss is deduced and then performed similarthings till the assessment of networkprevents the enhancement. **Figure 4** displays demonstration of ZFNet.

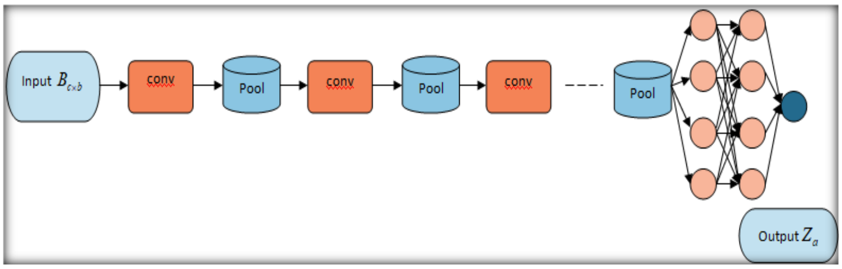


Figure 4. Structure of ZFNet.

1) Training Algorithm of FTDHO

Here, the ZFNet is trained by utilizing FTDHO for improving the performance of the network. TDO [22] is designed with the behavior of Tasmanian devil's feeding as well as natural traits. This follows two diverge phases like prey hunting and feeding by absorbing carnivores in initial phase as well as feeding on prey by hunting in next stage. This has extreme exploration ability for determining optimum region with search space. Correspondingly, FC [21] is deployed for enhancing optimization traits and convergence to the solution with several integral as well as derivative expressions. The assessment of this computation is improved and non-effectual solutions acquired over search space are eliminated with the amalgamation of FC with TDO. HHO [20] is designed by the motivation of prey exploration and diverge attacking schemes of Harris hawks, which is population based and gradient free optimization module, thus it is deployed for optimization concerns for obtain suitable computation. The FTDHO module is arithmetically designed by the following stages.

a) Solution Encoding

It is used for determining the position encoding for observing the supreme solution in a search space (λ),

$$\lambda = [1 \times \varepsilon] \tag{13}$$

here, learning factor of ZFNet signifies ε.

b) Fitness function

This measure is used for obtaining extreme results based on Mean Squared Root (MSE), which is formulated by,

$$fit = \frac{1}{b}\sum_{a=1}^{b}[\tau_a - Z_a]^2 \tag{14}$$

Here, targeted output implies τ_a, and detected output as Z_a.

c) Algorithmic Steps

The algorithmic steps of FTDHO are deliberated as follows.

Step 1: Initialization.

Initially, the population of search agents is arbitrarily produced by assuming the limitations of concern. The concerns of entire variables is equivalent to more elements for every vector population is in arithmetic format that is elucidated as,

$$W = \{W_1, W_2, \ldots, W_p, \ldots, W_q\} \tag{15}$$

here, Tasmanian devil population symbolizes W, W_p and W_q implies the population of p^{th} and q^{th} candidate solution.

Step 2: Determine Fitness value.

The computation of fitness value is conducted for recognizing optimum position that is specified in Equation (14).

Step 3: Feeding by consuming carrion.

With the aid of eating carrion strategy, Tasmanian devils employed for considering feeding on carrion other than hunting prey in feeding process. The characteristics of Tasmanian devil search over environmentfor identifying carrion and exploration strategy in various regions for carrion is determined by employingupgrade equation,

$$w_{p,q}(r+1) = w_{p,q}(r)[1 - \Re.V + y] + \Re.G_{p,q} + \frac{1}{2}yw_{p,q}(r-1) + \frac{1}{6}(1-y)w_{p,q}(r-2 + \frac{1}{24}y(1-y)(2-y)w_{p,q}(r-3) \tag{16}$$

here, carrion choose by p^{th} Tasmanian devil implies G_p, position of Tasmanian devil at r^{th} iteration indicates $w_{p,q}(r)$, new position of Tasmanian devil at $(r+1)^{th}$ iteration as $w_{p,q}(r+1)$ fitness function of selected carrion and p^{th} Tasmanian devil enumerates U_{G_p} and U_p, $\Re$ symbolizes random number with [0, 1], and random number as [1,2] is V, derivative order as y, Tasmanian devil position at $(r-1)^{th}$ iteration as $w_{p,q}(r-1)$, $w_{p,q}(r-2)$ signifies Tasmanian devil position at $(r-2)^{th}$ iteration, and $w_{p,q}(r-3)$ indicates Tasmanian devil position at $(r-3)^{th}$iteration.

From HHO [20], the standard expression is integrated to compute the final update solution that is,

$$W(r+1) = W_{\Re}(r) - x_1|W_{\Re}(r) - 2x_2W(r)|n \geq 0.5 \tag{17}$$

Let us consider,

$$W(r+1) = w_{p,q}(r+1) \tag{18}$$

$$W(r) = w_{p,q}(r) \tag{19}$$

Assume $W_{\Re}(r) > 2 \cdot x_2(r)$ and substitute the Equations (18) and (19) in Equation (17),

$$w_{p,q}(r+1) = W_{\Re}(r) - x_1\left(W_{\Re}(r) - 2x_2w_{p,q}(r)\right) \tag{20}$$

$$w_{p,q}(r+1) = W_{\Re}(r) - x_1W_{\Re}(r) + 2x_1x_2w_{p,q}(r) \tag{21}$$

$$w_{p,q}(r+1) = W_{\Re}(r)(1-x_1) + 2x_1x_2w_{p,q}(r) \tag{22}$$

$$w_{p,q}(r) = \frac{w_{p,q}(r+1) - W_{\Re}(r)(1-x_1)}{2x_1x_2} \tag{23}$$

Substituting Equation (23) in Equation (16),

$$w_{p,q}(r+1) = \left[\frac{w_{p,q}(r+1) - W_{\Re}(r)(1-x_1)}{2x_1x_2}\right][1 - \Re.V + y] + \Re.G_{p,q} + \frac{1}{2}yw_{p,q}(r-1) + \frac{1}{6}(1-y)w_{p,q}(r-2) + \frac{1}{24}y(1-y)(2-y)w_{p,q}(r-3) \tag{24}$$

$$w_{p,q}(r+1) - \frac{w_{p,q}(r+1) - [1 - \Re.V + y]}{2x_1x_2} = \left[\frac{W_{\Re}(r)(x_1-1)[1 - \Re.V + y]}{2x_1x_2}\right] + \Re.G_{p,q} + \frac{1}{2}yw_{p,q}(r-1) + \frac{1}{6}(1-y)w_{p,q}(r-2) + \frac{1}{24}y(1-y)(2-y)w_{p,q}(r-3) \tag{25}$$

$$\frac{w_{p,q}(r+1)}{2x_1x_2}[2x_1x_2 - 1 + \Re.V - y] = W_{\Re}(r)(x_1-1)[1 - \Re.V + y] + \left[\frac{\begin{bmatrix}\Re.G_{p,q} + \frac{1}{2}yw_{p,q}(r-1) + \frac{1}{6}(1-y)w_{p,q}(r-2) \\ + \frac{1}{24}y(1-y)(2-y)w_{p,q}(r-3)\end{bmatrix}2x_1x_2}{2x_1x_2}\right] \tag{26}$$

$$w_{p,q}(r+1) = \frac{W_{\Re}(r)(x_1-1)[1 - \Re.V + y] + \begin{bmatrix}\Re.G_{p,q} + \frac{1}{2}yw_{p,q}(r-1) + \frac{1}{6}(1-y)w_{p,q}(r-2) \\ + \frac{1}{24}y(1-y)(2-y)w_{p,q}(r-3)\end{bmatrix}2x_1x_2}{2x_1x_2 - 1 + \Re.V - y} \tag{27}$$

here, constant enumerates w, randomly selected hawk in generation$r$implies $W_{\Re}(r)$, and random value signifies x_1, x_2 which is in the range of [0,1].

Step 4: Feeding by hunting prey.

The second stage is hunting progress of Tasmanian devil that is conducted in two phases namely, scanning selection region and attacking prey, and Tasmanian devil feeds on chased prey. Here, selection and attack in initial phase is illustrated as,

$$M_p = W_k, \quad p = 1,2,\ldots,H \quad k \in \{1,2,\ldots,H | k \neq p\} \tag{28}$$

here, prey selected by p^{th} Tasmanian devil as M_p.

After selection progress, upgraded position is recognizedfor enhancing target function value that is formulated as

$$w_{p,q}(r+1) = \begin{cases} w_{p,q}(r) + \Re.\left(J_{r,s} - V.w_{p,q}(r)\right), & U_{M_p} < U_p; \\ w_{p,q}(r) + \Re.\left(w_{p,q}(r) - M_{p,q}\right), & Otherwise, \end{cases} \tag{29}$$

here, the value of intent function represents U_{M_p}. The position of Tasmanian devil is placed at neighborhood center and adjacent neighborhood in chasing progress that is determined as,

$$Radius = 0.01\left(1 - \frac{r}{r_{max}}()\right) \tag{30}$$

here, maximum iteration signifies r_{max} and r indicates iteration counter. Therefore, new Tasmanian devil position on chasing progress formulated as,

$$w_{p,q}(new) = w_{p,q} + (2\Re - 1).Radius.w_{p,q} \tag{31}$$

Step 5: Re-computation of error.

The optimum solution is recognized by fitness value mentioned in Equation (15) and it is effectually altered with new solution.

Step 6: Termination.

Algorithm 1 Pseudo code of FTDHO

```
input: $H, r_{max}$
output: $w_{p,q}(r+1)$
Begin
  Initialization the position
    Compute fitness by Equation (14)
for $r = 1: r_{max}$
for $r = 1: H$
if $\Re < 0.5$
Exploration phase
  Identify carrion using Equation (16)
Upgrade Tasmanian devil position Equation (27)
Else
Selection of prey and attacking
Evaluate prey by Equation (28)
Else
Upgrade Tasmanian devil position byEquation (29)
Chasing prey
      Modify neighbourhood radius byEquation (30)
Upgrade Tasmanian devil position byEquation (31)
end if
end for$r = 1: r_{max}$
end for$p = 1: H$
Examinefinest solution byEquation (15)
End
```

The abovementioned stages employed for the detection progress will be iteratively perform till it obtains the extreme finest solution; moreover pseudo code of FTDHO is specified in Algorithm 1.

Henceforth, the attack is detected using FTDHO_ZFNet and it is symbolized by Z_a.

F. Attack Mitigation

Attack Mitigation is a progress of controlling the susceptibilities in this module for concluding the threat from discriminating the network. This includes by several control techniques for detection progress, prevent and mitigate the attacks. In this module, data rate is degraded for attack node. Let us assume time interval implies Δu and number of packets symbolizes $\eta(\Delta u)$ and mean of packet size is formulated as,

$$\vec{\kappa} = \frac{1}{\eta}\sum_{\hbar=1}^{\eta} \kappa_{\hbar}\, ; 60 \leq \vec{\kappa} \leq \kappa_{max} \tag{32}$$

here, maximal packet size represents κ_{max} and $\hbar^{th}$ packet size signifies $\kappa_{\hbar}$. Here, 50% of data is degraded when packet dimension fixed beyond the range. The outcome of attack mitigation signifiesY_a.

5. Results and discussions

In this fragment, the resultants of FTDHO_ZFNet is discussed and evaluated by utilizing traditional approaches, database description, and evaluation measures are also deliberated.

1) Experimental Setup

The novel scheme FTDHO_ZFNet is successfully executed by PYTHON tool in Windows 10 OS.

2) Dataset description

The description of database is employed for FTDHO_ZFNet is elucidated as:

(1) Bot-IoT database

This database [16] is composed of more files in various formats namely, original pcap, created argus, .csv files. Here, the .csv and pcap files with 16.7 GB and 69.3 GB. Attacks deployed here are DoS, Keylogging, OS and service scan, Distributed DoS (DDoS), and data exfiltration attacks. The pcap files have more than 72,000 records.

3) Evaluation Metrics

The metrics deployed forFTDHO_ZFNet is elucidated as follows,

(1) Accuracy

It is engagedto compute the feasibility or preciseness of diagnose is determined as,

$$\mathrm{Acc} = \frac{\mathrm{Tp} + \mathrm{Tn}}{\mathrm{Tp} + \mathrm{Tn} + \mathrm{Fp} + \mathrm{Fn}} \tag{33}$$

(2) TPR

It is the ratio of actual cases which are precisely identified by the developed technique that are determined as

$$\mathrm{TPR} = \frac{\mathrm{Tp}}{\mathrm{Tp} + \mathrm{Fn}} \tag{34}$$

(3) TNR

This metric is deployed for determining the original resultants of actual negative analyzed by

$$\mathrm{TNR} = \frac{\mathrm{Tn}}{\mathrm{Tn} + \mathrm{Fp}} \tag{35}$$

here, true positive, true negative, false positive and false negative implies $\mathrm{Tp}, \mathrm{Tn}, \mathrm{Fp}, \mathrm{Fn}$ respectively.

4) Comparative Methods

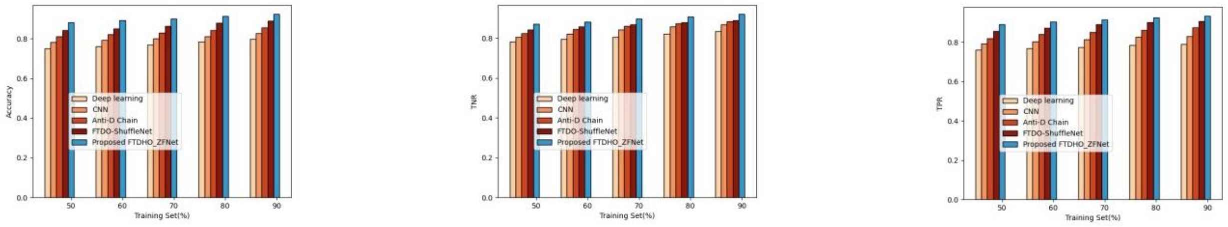
Deep learning [1], CNN [5], Anti-D Chain [2], FTDO-ShuffleNet are the other modules evaluated for proving the effectualness of proposed FTDHO_ZFNet.

5) Comparative Analysis

The comparative examination of FTDHO_ZFNet is analyzed by differing training set and k-value with the existing approaches.

(1) Examination of FTDHO_ZFNet differing training set

In **Figure 5**, the examination of FTDHO_ZFNet is illustrated by differing training set. **Figure 5a** elucidates the accuracy of FTDHO_ZFNet. Examination of FTDHO_ZFNet is evaluated by accuracy with training set of 90% gained 0.924, wherein performance improvement of conventional strategieslike Deep learning, CNN, Anti-D Chain, and FTDO-ShuffleNet observed by comparing are 13.700%, 10.372%, 7.409% and 3.587%. In **Figure 5b**, valuation of FTDHO_ZFNet with relevance of TPR is represented. When training set of 90%, FTDHO_ZFNet attained TPR with 0.933, whereas preceding approaches obtained performance enhancement of TPR of 15.279%, 10.948%, 6.285% and 2.708%. **Figure 5c** depicts the valuation of TNR for FTDHO_ZFNet. The novel approach FTDHO_ZFNet is examined with conventional approachesacquired TNR with 0.920, as well as traditional strategies accomplished performance gain with 9.184%, 5.539%, 4.049% and 3.368% with *k*-value as 9.

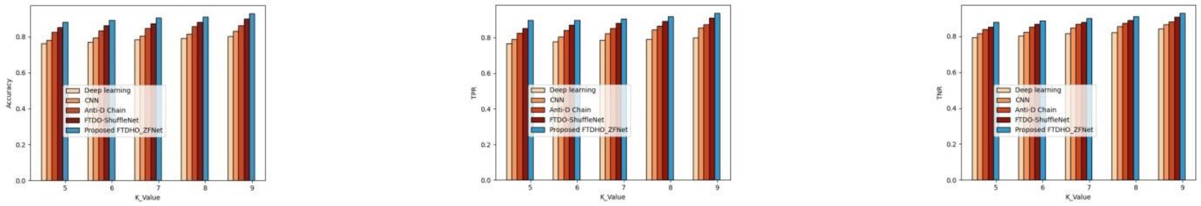


(a) **(b)** **(c)**

Figure 5. Examination of FTDHO_ZFNet differing training set. **(a)** Accuracy; **(b)** TPR; **(c)** TNR.

(2) Examination of FTDHO_ZFNet differing *k*-value

In **Figure 6**, the valuation of FTDHO_ZFNet is designed by differing k-value. **Figure 6a** expounds the accuracy of FTDHO_ZFNet. Evaluation of FTDHO_ZFNet is analyzed by accuracy with *k*-value of 9 achieved 0.929, whereas performance enhancement of prior schemes acquired by comparing are 13.625%, 10.551%, 7.031% and 3.179%. In **Figure 6b**, evaluation of FTDHO_ZFNet with respect to TPR is illustrated. When k-value is 9, FTDHO_ZFNet observed TPR of 0.938, where former techniques accomplished performance gain of TPR of 14.643%, 8.820%, 6.898% and 2.771%. **Figure 6c** enumerates the analysis of TNR for FTDHO_ZFNet. The proposed technique FTDHO_ZFNet is analyzed with other techniques attained TNR with 0.929, as well as former models accomplished performance gain of 9.336%, 6.884%, 4.985% and 2.260% while k-value is considered as 9.



(a) **(b)** **(c)**

Figure 6. Examination of FTDHO_ZFNet differing *k*-value. **(a)** Accuracy; **(b)** TPR; **(c)** TNR.

6) Algorithmic Methods

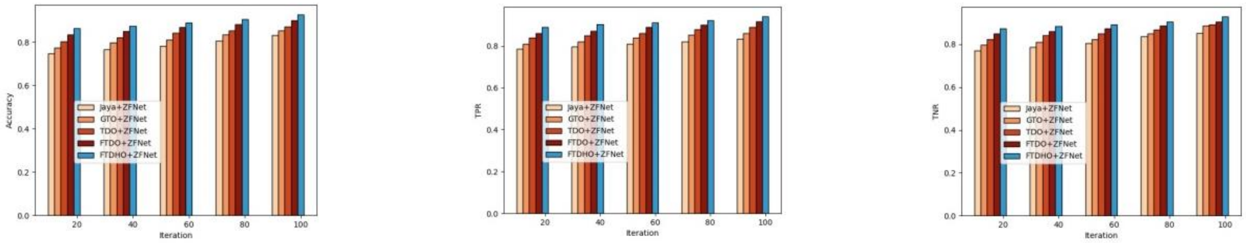
The algorithmix evaluation is performed on the basis of existing algorithms namely, Jaya+ZFNet [19,24] Gorilla Troops Optimization (GTO)+ZFNet [19,25] TDO+ZFNet [19,22] and FTDO+ZFNet for the extreme outcome of FTDHO+ZFNet.

7) Algorithmic Analysis

The following fragments expounds the algorithmic analysis of FTDHO_ZFNet is evaluated by differing iterations from 20 to 100.

(1) Examination of FTDHO_ZFNet differing iterations

In **Figure 7**, the analysis of FTDHO_ZFNet is enumerated by differing iterations. **Figure 7a** deliberates the accuracy of FTDHO_ZFNet. Analysis of FTDHO_ZFNet is determined by accuracy with iteration of 100 observed 0.927, whereas performance enhancement of traditional strategies like, Deep learning, CNN, Anti-D Chain, and FTDO-ShuffleNet acquired by comparing are 10.159%, 8.016%, 5.850% and 2.719%. In **Figure 7b**, evaluation of FTDHO_ZFNet with respect to TPR is illustrated. When iteration is 100, FTDHO_ZFNet observed TPR of 0.940, where former techniques accomplished performance gain of TPR of 11.204%, 8.476%, 5.250% and 2.462%. **Figure 7c** enumerates the evaluation of TNR for FTDHO_ZFNet. The FTDHO_ZFNet is determined with existing modelsachieved TNR with 0.928, as same as that of old modules obtained performance gain of 8.108%, 4.388%, 3.882% and 2.453% while iteration is considered as 100.



(a) **(b)** **(c)**

Figure 7. Examination of FTDHO_ZFNet differing iterations. **(a)** Accuracy; **(b)** TPR; **(c)** TNR.

8) Comparative Discussion

In this fragment, the comparative discussion ofFTDHO_ZFNet is examined with traditional approaches for proving the effectualness of proposed technique. **Table 2** depicts comparative discussion of FTDHO_ZFNet. The performance measures employed for FTDHO_ZFNet observed utmost values with92.9%, 93.8% and 92.9%.

Table 2. Comparative discussion.

Alterations based on	Metrics/Methods	Deep learning	CNN	Anti-D Chain	FTDO-ShuffleNet	Proposed FTDHO_ZFNet
Training set = 90%	Accuracy	79.7%	82.8%	85.5%	89.1%	92.4%
	TPR	79.0%	83.1%	87.4%	90.8%	93.3%
	TNR	83.6%	86.9%	88.3%	88.9%	92.0%
k-value = 9	Accuracy	80.2%	83.1%	86.3%	89.9%	92.9%
	TPR	80.0%	85.5%	87.3%	91.2%	93.8%
	TNR	84.2%	86.5%	88.2%	90.8%	92.9%

6. Conclusion

In this exploration, a blockchain based system for attack detection and mitigation is developed with DL named FTDHO_ZFNet. The entities deployed here are stated as owner, blockchain, server, trusted authority and user. Here, authentication phase is done with Ethereum block chain by Key Exchange module as well as privacy preserved data distribution and communication is also performed. The generation of recorded log file is done with beneath progresses. The log file is generated with the aid of communication to record the events. The extraction of feature is conducted by Bot-Iot database. Then, feature fusion section is carried out by overlap coefficient with DQN. Moreover, DA is done using bootstrapping method. At last, attack detection is observed by Z-FNet tuned by FTDHO. Here, FTDHO is unified by FTDO and HHO. Additionally, FTDO is integrated by FC concept and TDO. Furthermore, attack mitigation is performed. The analytic measures deployed for FTDHO_ZFNet achieved utmost values with 92.9%, 93.8% and 92.9%. In future, the location of the attacker will be identified and to implement this statistical evaluation of flagged obtained signal will be explored.

Author contributions: Conceptualization, SSB and RD; methodology, SSB and RD; software, SSB; validation, RD and SSB; formal analysis, SSB; investigation, SSB; resources, SSB; data curation, SSB; writing—original draft preparation, SSB; writing—review and editing, SSB; visualization, SSB; supervision, RD; project administration, RD. All authors have read and agreed to the published version of the manuscript.

Conflict of interest: The authors declare no conflict of interest.

References

1. Sanda O, Pavlidis M, Seraj S, et al. Long-Range attack detection on permissionless blockchains using Deep Learning. Expert Systems with Applications. 2023; 218: 119606. doi: 10.1016/j.eswa.2023.119606
2. Dai Q, Zhang B, Dong S. Eclipse attack detection for BC network layer based on deep feature extraction. Wireless Communications and Mobile Computing; 2022.
3. Jia B, Liang Y. Anti-D chain: A lightweight DDoS attack detection scheme based on heterogeneous ensemble learning in blockchain. China Communications. 2020; 17(9): 11–24. doi: 10.23919/jcc.2020.09.002
4. Jiang S, Yang L, Gao X, et al. BSD-Guard: A Collaborative Blockchain-Based Approach for Detection and Mitigation of SDN-Targeted DDoS Attacks. Chen Y, ed. Security and Communication Networks. 2022; 2022: 1–16. doi: 10.1155/2022/1608689

5. Sivaganesan DD. A data driven trust mechanism based on blockchain in IoT sensor networks for detection and mitigation of attacks. Journal of Trends in Computer Science and Smart Technology. 2021; 3(1): 59–69.
6. Albakri A, Alabdullah B, Alhayan F. Blockchain-Assisted Machine Learning with Hybrid Metaheuristics-Empowered Cyber Attack Detection and Classification Model. Sustainability. 2023; 15(18): 13887.
7. Javed M, Tariq N, Ashraf M, et al. Securing Smart Healthcare Cyber-Physical Systems against Blackhole and Greyhole Attacks Using a Blockchain-Enabled Gini Index Framework. Sensors. 2023; 23: 9372.
8. Jones CB, Kingsley DJ. Decentralized Blockchain With Convolutional Neural Network Model For Security Attack Mitigation", ICTACT Journal on Communication Technology. 2023; 14(1).
9. Lian Z, Zeng Q, Su C. Privacy-preserving Blockchain-based Global Data Sharing for Federated Learning with Non-IID Data. 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW). Published online July 2022. doi: 10.1109/icdcsw56584.2022.00044.
10. Xia Q, Sifah E, Smahi A, et al. BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments. Information. 2017; 8(2): 44. doi: 10.3390/info8020044
11. Sasaki H, Horiuchi T, Kato S. A study on vision-based mobile robot learning by deep Q-network. 2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE). Published online September 2017. doi: 10.23919/sice.2017.8105597
12. Jin B, Yang J, Huang X, et al. Deep deformable Q-Network. Proceedings of the International Conference on Web Intelligence. Published online August 23, 2017. doi: 10.1145/3106426.3109426
13. Brownlee J. A Gentle Introduction to the Bootstrap Method. Available online: https://machinelearningmastery.com/a-gentle-introduction-to-the-bootstrap-method/ (accessed on 12 January 2023).
14. Satapathy SC, Joshi A. Information and Communication Technology for Intelligent Systems (ICTIS 2017)—Volume 2. Springer International Publishing; 2018. doi: 10.1007/978-3-319-63645-0
15. Dehghani M, Hubalovsky S, Trojovsky P. Tasmanian Devil Optimization: A New Bio-Inspired Optimization Algorithm for Solving Optimization Algorithm. IEEE Access. 2022; 10: 19599–19620. doi: 10.1109/access.2022.3151641
16. Bhaladhare PR, Jinwala DC. A Clustering Approach for the l-Diversity Model in Privacy Preserving Data Mining Using Fractional Calculus-Bacterial Foraging Optimization Algorithm. Advances in Computer Engineering. 2014; 2014: 1–12. doi: 10.1155/2014/396529
17. Heidari AA, Mirjalili S, Faris H, et al. Harris hawks optimization: Algorithm and applications. Future Generation Computer Systems. 2019; 97: 849–872. doi: 10.1016/j.future.2019.02.028
18. Venkata Rao R. Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems. International Journal of Industrial Engineering Computations. Published online 2016: 19–34. doi: 10.5267/j.ijiec.2015.8.004
19. Abdollahzadeh B, Soleimanian Gharehchopogh F, Mirjalili S. Artificial gorilla troops optimizer: A new nature-inspired metaheuristic algorithm for global optimization problems. International Journal of Intelligent Systems. 2021; 36(10): 5887–5958. doi: 10.1002/int.22535
20. Reddy S, Shyam GK. A machine learning based attack detection and mitigation using a secure SaaS framework. Journal of King Saud University—Computer and Information Sciences. 2022; 34(7): 4047–4061. doi: 10.1016/j.jksuci.2020.10.005
21. Wu Y, Wei D, Feng J. Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey. Security and Communication Networks. 2020; 2020: 1–17. doi: 10.1155/2020/8872923
22. Hassanzadeh A, Stoleru R, Chen J. Efficient flooding in Wireless Sensor Networks secured with neighborhood keys. 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Published online October 2011. doi: 10.1109/wimob.2011.6085415
23. Anita. N, Vijayalakshmi. M. Blockchain Security Attack: A Brief Survey. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). Published online July 2019. doi: 10.1109/icccnt45670.2019.8944615
24. Anderson L, Holz R, Ponomarev A, et al. New kids on the block: an analysis of modern blockchains. Available online: https://arxiv.org/abs/1606.06530 (accessed on 21 January 2022).
25. BOT-IOT dataset. Available online: https://ieee-dataport.org/documents/bot-iot-dataset (accessed on 16 October 2019).