Measurement: Sensors 24 (2022) 100431

Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Attack prevention in IoT through hybrid optimization mechanism and deep learning framework

Regonda Nagaraju [a,*], Jupeth Toriano Pentang [b], Shokhjakhon Abdufattokhov [c], Ricardo Fernando CosioBorda [d], N. Mageswari [e], G. Uganya [f]

[a] Department of Information Technology, St.Martin's Engineering College, Dhulapally, Secunderabad, 500100, India
[b] Western Philippines University, Philippines
[c] Automatic Control and Computer Engineering Department, Turin Polytechnic University in Tashkent, Tashkent, Uzbekistan
[d] Universidad Autónoma del Perú, Lima, Peru
[e] Department of ECE, Ashoka Women's Engineering College, Kurnool, Andhra Pradesh, India
[f] Department of ECE, Assistant Professor, Saveetha School of Engineering, SIMATS, Chennai, India

ARTICLE INFO

Keywords:
Grey wolf optimization
Whale optimization
Internet of things
Deep learning
Cybersecurity
Whale with grey wolf optimization

ABSTRACT

The Internet of Things (IoT) connects schemes, programs, data management, and operations, and as they continuously assist in the corporation, they may be a fresh entryway for cyber-attacks. Presently, illegal downloading and virus attacks pose significant threats to IoT security. These risks may acquire confidential material, causing reputational and financial harm. In this paper hybrid optimization mechanism and deep learning,a frame is used to detect the attack prevention in IoT. To develop a cybersecurity warning system in a huge data set, the cybersecurity warning systems index system is first constructed, then the index factors are picked and measured, and finally, the situation evaluation is done.Numerous bio-inspired techniques were used to enhance the productivity of an IDS by lowering the data dimensionality and deleting unnecessary and noisy input. The Grey Wolf Optimization algorithm (GWO) is a developed bio-inspired algorithm that improves the efficacy of the IDS in detecting both regular and abnormal congestion in the network. The smart initialization step integrates the different pre-processing strategies to make sure that informative features are incorporated in the early development stages, has been improved. Researchers pick multi-source material in a big data environment for the identification and verification of index components and present a parallel reduction approach based on the classification significance matrix to decrease data underlying data characteristics. For the simulation of this situation, grey wolf optimization and whale optimization were combined to detect the attack prevention and the deep learning approach was presented. Utilizing system software plagiarism, the TensorFlow deep neural network is intended to classify stolen software. To reduce the noise from the signal and to zoom the significance of each word in the perspective of open-source plagiarism, the tokenization and weighting feature approaches are utilized. Malware specimens have been collected from the Mailing database for testing purposes. The experimental findings show that the suggested technique for measuring cyber security hazards in IoT has superior classification results to existing methods. Hence to detect the attack prevention in IoT process Whale with Grey wolf optimization (WGWO) and deep convolution network is used.

1. Introduction

Internet technological advances have brought more convenience to individuals around the globe than it has ever been, thanks to the rapid expansion of data and telecommunications infrastructure. Nevertheless, the increasing number and varieties of cyberattacks (such as networking viruses, malicious attacks, malicious eavesdropping, and so on) pose a significant threat to women's information security and property protection. As a result, both people and communities as a whole have grown dependent on information and communication technology protection. Firewalls are extensively used and extensively installed as a basic protective measure. It is no longer appropriate for units that require strong

* Corresponding author.
E-mail addresses: nagcse01@gmail.com (R. Nagaraju), jupeth.pentang@wpu.edu.ph (J.T. Pentang), sh.abdufattohov@polito.uz (S. Abdufattokhov), ricardo.cosio.borda@gmail.com (R.F. CosioBorda), magesmaniengg@gmail.com (N. Mageswari), uganyaece@gmail.com (G. Uganya).

https://doi.org/10.1016/j.measen.2022.100431
Received 11 June 2022; Received in revised form 3 August 2022; Accepted 24 August 2022
Available online 29 August 2022

security due to the difficulties of human customization and the delay for new sorts of attacks (e.g., government units, military bases, etc.).As a result, network security experts have developed a novel method for detecting and dealing with anomalous networking intrusion detection systems (IDSs) [1].In terms of developing a robust solution, selection of features (FS) is a preliminary procedure for extracting the most relevant aspect. This is a critical phase that seems to have a direct impact on the effectiveness of the IDS. Filter-based and wrapper-based methods to FS are the two basic approaches. The filter-based approach assesses the resolution based on the learning algorithms during search and optimum procedures, whereas the wrapper-based method assesses the solutions related to the learning algorithms during search and evaluation procedures. The confirmed outcomes of the wrapper-based strategy make it the most widely utilized approach, rather than the less costly filter-based method [2].

An intrusion detection system deployed in the network could help limit security concerns from IoT applications. By constantly tracking inbound and outbound internet traffic collected by IoT devices, the IDS identifies any signals of cyber-attacks. It has two kinds of threat identificationapproach: signature-based and anomaly-based. The signature-based intrusion detection system uses criteria derived from established known attacks, and it recognizes a risk if recorded events meet these rules. An anomaly-based strategy, on the other hand, develops a simulation using the state's typical behavior. The discrepancy between observed and learnedbehavior could then be utilized to identify the assault using this approach.The main problem with these approaches is that they would only represent a small number of processing behaviors, which is insufficient for IoT networks with a variety of component kinds. Furthermore, different device kinds might cause diverse network behaviors, lowering the accuracy of detecting attacks. Deep learning-based IDS may transcend existing difficulties and improve detection and prevention accuracy, as evidenced by the development of deep learning in various sectors. Indeed, the deep learning model is more effective than some other supervised learning models at learning complicated and nonlinear properties in network traffic. Because the labeling procedure is time-consuming and labor-intensive, it is impractical to keep the labeled datasets up to date. Furthermore, high-quality datasets for training IDSs are difficult to come by, even though they are critical to improving IDS detection accuracy. The primary cause of this scarcity is privacy concerns [3].

Any organization's electronic information is a critical resource, and an individual's information might be quite valuable to them, something that they can afford to give up. In today's modern digital environment, information security has grown critical, and it necessitates viable countermeasures to every danger. As a result, for data-driven or informationreliant on operations, cyber security and risk mitigation are critical.Cyber security is the protection of rules, human activities, and technological tools that help safeguard electronic information resources. Cyber attackers are surpassing defenses, which raised doubts about the protection of important digital content. Most information-sharing technologies, particularly mobile networks, are at a significant refuge threat, according to data on vulnerability and unauthorized. Identifying assets is the first step in analyzing a system's cybersecurity or assessing risks. Finding a complete technique that is best right to the risky circumstance is critical. This facilitates the use of the latest cutting-edge technique for forecasting and mitigating cybersecurity threats. The most appropriate model may also be determined by the attack types and attack targets [4]. The broad classification of artificial intelligence techniques is depicted in Fig. 1. Among cryptography and intelligent systems, there is a broad range of cross-disciplinary connections. In a mobile phone network, deep learning technologies could have been used to create complex models for malware classification, intrusion detection, and cyber threat sensing. To reduce vulnerabilities and guarantee improved data security, AI models involve complex cybersecurity and security technologies, and a secure federation educational experience. Artificial intelligence has spawned a slew of new fields, including machine learning, natural language processing, and machine learning [5].

This does not, therefore, imply that now the dangers of leveraging the system's capability have indeed been diminished. The numerous developments in the mobile system sector assist the new generation of

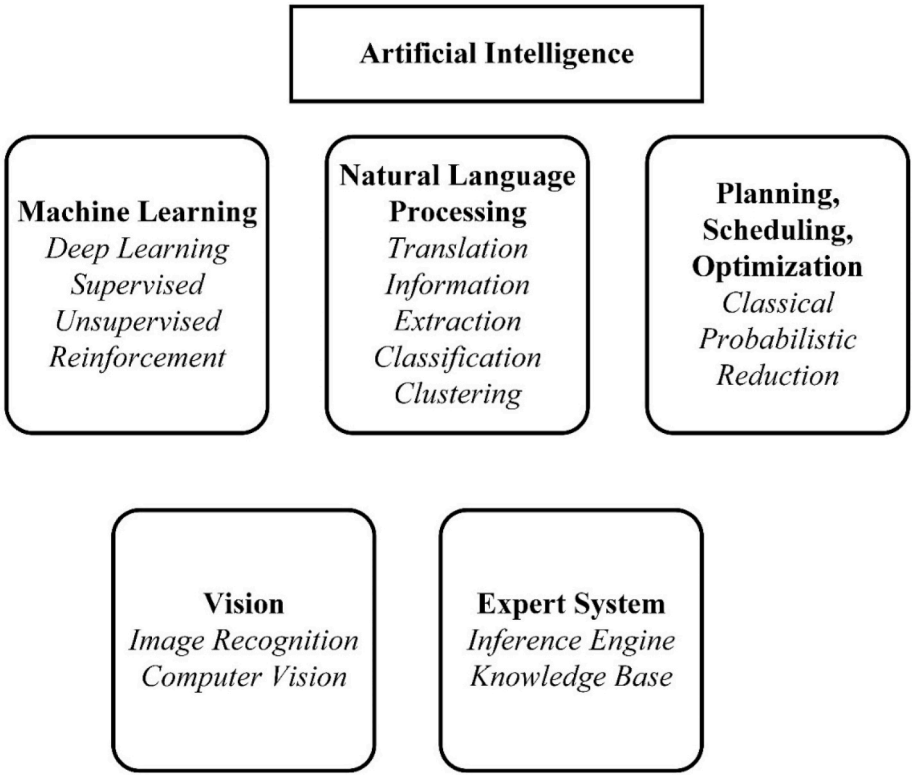

Fig. 1. AI taxonomy.

networking is becoming considerably faster and more reliable than previous iterations. Nonetheless, the threat of recognized and unknown risks highlights the necessity for continuing risk management systems to be extended. As a result, despite the abundance of frameworks on protecting an organization's resources from cyberthreats, cyber security decision-makers still have a difficult task.Crypto mining, fraudulent applications, and finance are all examples of mobile malware. Trojans are one of the most prevalent mobile phone network threats. Smartphones have overtaken desktop applications as the most preferred way of accessing tailored solutions like email, banking, internet ordering, and automatic gadget control. Hacking has used patching mechanisms to infect mobile applications, making them an attractive target for criminals. Appropriate security methods look to be inadequate for upcoming mobile technologies, which have boosted network transmission speed. Advanced forms are breaking new ground in the security of different vital services, some of which are dependent on mobile networks, thanks to advancements in Artificial intelligence [5].

The Internet - Of - things (IoT) is a system of connected devices that are linked together using Bluetooth, near-field communications (NFC), and Wi-Fi. Smart objects (thermometers, freezers, etc.), health care, computer peripherals, security devices, military, agricultural, and other applications use IoT devices extensively. The Internet Protocol (IP) is used by these IoT devices to convey packets to the destination. This IP protocol recognizes the machine and allows for quick communication without the need for human involvement. Nevertheless, IoT devices alter a person's existence in a variety of ways, and IoT security vulnerabilities pose a serious security risk. Current intruder recognition systems may not be sufficient to guard against today's modern advanced threats.As a result, the risk of IoT intrusion was evaluated in this study by using a sparse convolute net to fight threats and attacks. Large data gathering, physical and virtual setting connectivity, multifaceted negative impacts on the environment, and centralized architecture are all characteristics of IoT devices. These features allow the Internet of Things to function effectively, but they also allow threat actors to exploit communications [6].

Weaponization and hijack of IoT systems for Distributed Denial of Service (DDoS) assaults, man-in-the-middle assaults, targeted code injection, and human pose are all possible. Furthermore, malicious actors could directly influence IoT devices, which has a substantial impact on data transmission throughout the system. To prevent intermediary assaults in a distributed system, maintaining and preserving IoT security is more important. The safety dangers are then decreased by securing the entire network, segmenting IoT devices, tracking, inspecting, and enforcing policies, and taking prompt automated steps if the system is harmed. The Intrusion Detection System was used to achieve IoT security (IDS).The IDS system employs a variety of hardware & system programs to detect and forecast harmful network activity. Assume that the systems or Internet of things are subject to any security information and event monitoring (SIEM) controls. SIEM distinguishes harmful activities by combining several source outcomes and alarm processing mechanisms. Network-based, wireless intrusion, network conduct analysis, and host-based intrusion detection and prevention systems are the four types of intrusions that are avoided. These four main types constantly monitor networks, wireless networks, and software packages, successfully predicting malicious packets. Harris Hawks Sparse Auto-Encoder Networks are used in the preventive procedure to identify the talks [7].

To solve the challenges outlined previously, many deep learning approaches have been proposed. Data mining methods, contrary to signature-based techniques, strive to construct a data-driven model for infection identification based on stated features. Steady and transient approaches are the two most used types of malware classification for extraction of feature. The static analysis has been performed in a non-runtime context, and the connected components, such as byte-sequence or string characteristics, can sometimes be retrieved from executable code through source code. To perform a performance simulation, malware must be executed in an enclosed environment to watch its activity and catch hostile activities. Subject specialists could develop valuable aspects of an application for malware region detection on static or dynamic assessments [8].

The following sections are included as follows. Section 2 describes on related works. Section 3 on materials and methods. Section 4 and 5 depicted on proposed works. Section 6 showcases the results and discussion. Section 7 provides the conclusion part.

2. Related works

Malware assaults have been one of the most serious dangers to cybersecurity. Developing the most effective malware detection method became a crucial issue in cybersecurity. Machine learning algorithms have previously been shown to be a viable way to solve this issue. Many suggested solutions transform malware executable code into image pixels and classify malware using convolution neural networks (CNNs). Transforming malware executable code to pictures, on the other hand, may cause the binary code's one-dimensional structure to be twisted. To overcome this issue, researchers investigate malware playable bit and byte patterns and formulate appropriate one-dimensional (1D) CNNs for malware classification. These tests use two benchmark datasets to assess their hypothesized 1D Convolution layers.The suggested 1D CNN methods outperform previous 2D CNN malware designed to describe in terms of experimental outcomes by allowing for smaller scaling bit/byte-level sequences at a reduced computational expense. While binary software packages were transforming and scaling to larger pictures, such as 128 $\times$ 128 pixels, the suggested solution did not always offer superior efficiency. The explanation for this could be that bigger datasets require a more sophisticated model that learns the relevant characteristics, such as ResNet or EfficientNet [9].

The number of Internet of Things devices, and the information recorded by these gadgets, has increased dramatically. Because of their constrained resources, contributing gadgets to IoT networks could be difficult, and the safety of such equipment is frequently disregarded. As a result, attackers now have a stronger motivation to attack IoT devices. As the number of crimes that can be launched against a network grows, conventional intrusion detection systems (IDS) find it much harder to keep up. Various machine learning (ML) approaches are addressed in this section, including k-nearest neighbor (KNN), artificial neural network (ANN), decision tree (DT), naïve Bayes (NB), random forest (RF), support vector machine (SVM), and logistic regression (LR).On the Bot-IoT database, ML techniques are evaluated for multi-dimensional and multi-categorization. Researchers evaluated Machine learning using numerous criteria such as precision, accuracy, recall, F1-measure, and logarithmic loss in an experimental. The reliability of RF in the particular scenario of an HTTP distributed denial-of-service (DDoS) assault is 99%. Additional simulation outcomes, such as accuracy, sensitivity, F1 measure, and log loss metric, show that RF surpasses all sorts of assaults in the classification model. KNN, on the other hand, beats other ML algorithms in multi-class categorization, with an efficiency of 99%, which is 4% higher than RF. In the approach, researchers want to include the models investigated in this study into an IDS prototype for testing utilizing a variety of data, along with a variety of assaults, to validate our findings [10].

The Internet of Things (IoT), which may be thought of as a more upgraded system of machine-to-machine communications technologies, was presented as a way to achieve intelligent thing-to-thing communication through the use of Internet access. The "things" in the Internet of Things are typically heterogeneous and resources to support. Furthermore, such devices communicate with one another using low-power, lossy channels. For endpoints only with encryption components, researchers suggest an inter-device identification and session-key transmission mechanism in this work. Unlike autonomous sensor setups in which the key is distributed by the key distribution hub, each sensor is employed in the manufacture of credentials in the present scheme.

Furthermore, the suggested technique improves efficiency by allowing the authorized devices to compute the session code in preparation.Man-in-the-middle attacks, replay occurrences, and wiretapped secret-key assaults are all possible with the suggested verification and session-key subscription model.The suggested technique could only ensure a certain level of protection if kIR is hacked. The suggested scheme in this research, like so many other proposed systems that use preset secret keys, presupposes safe communications and storage methods. Nevertheless, more study is required to achieve secure kIR sharing [11].

Estimating the parameters of photovoltaic panels is an important step in measuring, assessing, and enhancing the effectiveness of solar systems. An effective optimization approach is necessary to obtain the best solution for uncertain parameters. The development of the sooty tern enhancement (STO) method for parameter calculation of a solar cell/module is presented in this study. The simulation and experimental results were contrasted to four previously developed optimization techniques: the sine cosine (SCA) method, hybrid particle swarm optimization, gravitational search algorithm (PSOGSA), gravitational search algorithm (GSA), and whale optimization (WOA). The STO approach outperforms the other optimization strategies in terms of convergence speed and root mean square error. Furthermore, statistical results demonstrate that the STO approach is more resilient and accurate on average.The Friedman rating test additionally validates the STO method's high quality and durability. The STO is an effective and reliable method for predicting the uncertain optimized values of a solar PV module design during normal operating conditions, as per the prior explanation [12].

In terms of developing a robust solution, selection of features (FS) is a preliminary procedure for extracting the most relevant aspects. This is a critical phase that seems to have a direct impact on the effectiveness of the IDS. Filter-based and wrapper-based approaches to FS are the two basic approaches. The filter-based approach assesses the resolution based on the learning algorithms during search and optimum procedures, whereas the wrapper-based method assesses the solutions related to the learning algorithms during search and evaluation procedures. The confirmed outcomes of the wrapper-based strategy make it the most widely utilized approach, rather than the less costly filter-based method. Because of its superior accuracy, bio-inspired meta-heuristic methods are frequently utilized in the wrapper-based technique for selecting features in the intrusion detection system. The literature is mostly focused on the binarization procedure employing various differential equations. Different operations including mutation and crossover are used at the algorithmic layer to enhance the search capacity and evade getting caught in local goals. The random initialization technique is widely employed without consideration for incorporating the filter-based method into the rapper-based method. By producing the desired fitness in the early development stages, the most practicable initial population has a direct impact on fast convergence [13].

3. Materials and methods

As illustrated in Fig. 1, researchers present a modeling approach for cyber security intimidations and preventive strategies in commercial IoT. The suggested proposed architecture uses four datasets in cloud services. The raw network traffic is stored in database one; the prior information is saved in database two, and the fresh characteristics of identified malware and viruses are entered into database three. IoT gadgets help the cracker keep pirated software in databases 4. Analyzing a massive volume of information takes a long time. The preprocessing data function processes the raw data files in database one. The information from the pre-processing is then transferred to the detecting module.The detection method learns from characteristics in databases three and four to detect malware and pirate software threats. If harmful behavior is detected in the system, the system administrator is notified and instructed to take appropriate action.

4. Identification of threats

4.1. Data preprocessing

To translate the malware detection challenge into a classification task, color descriptions are produced from raw binary files. It distinguishes the proposed study from current methods, which transform malware data files into a grayscale containing 256 colors. This technique somehow doesn't rely on reverse software components like disassembler or decompile. When opposed to grayscale photos with only 256 colors, color photos could recover more information.Furthermore, improved features of malware photos can excel in malware family categorization. Previously, using grayscale photos, many virus detection technologies based on machine learning algorithms produced superior results. The color photos were converted to grayscale visualization before being classified using feature extraction algorithms. Using feature reduction strategies to reduce the number of features, categorization performance can be enhanced. Because it produces exponential quantities utilizing color photos, the results demonstrated that machine learning techniques are not a improved alternative for virus identification [14]. Deep learning systems outperform large malware datasets because they can dynamically reduce noise using filters.As a consequence, utilizing color photos with deep learning methods produces superior outcomes. There are four stages to converting a malware binary code to a color image. To begin, binary digital data are used to generate hexadecimal strings (0–15). Secondly, a hexadecimal channel is split into chunks of an 8-bit vector, each of which is restrained as an unsigned integer (0–255). The 8-bit vector is then transformed into a two-dimensional matrices field in the third step. Fourth, each 8-bit number is shown with red, green, and blue shading hues generated from two-dimensional geometry. The stages of data preparation are depicted in detail in Fig. 2.

4.2. Deep convolution neural network

To undertake an in-depth malware analysis of the data, the Deep Convolutional Neural Network (DCNN) is proposed. Fig. 1 shows the five components that make up the DCNN. The input layer is where the planned neural network model gets its training images. The convolution layer is first utilized to reduce noise and enhance signal qualities. Secondly, the pooling layer is utilized to reduce data latency while still keeping important data. Third, the fully connected layer converts the two-dimensional arrays to a one-dimensional array, which is subsequently fed into the specified classification. Finally, using the classifiers, the malware families from the individual photos are detected [15].

4.3. Convolution neural network

The significant features have been extracted by applying a convolution operation to reduce the appearance of variables. Scale invariance and interpretation invariance, rotation invariance, are all part of the convolution layer. It reduces the problem of over-fitting and introduces the generalization notion into the basic construction [16]. The convolutional layer receives many maps as inputs, as shown in Equ(1):

$$a_m^n = f\left[\sum_{u \in L_m} a_m^{n-1} * k_{um}^n + y_m^n\right] \tag{1}$$

The given map cluster is denoted as L_m, the convolutional kernel is defined as k_{um}^n and the input feature map utilized for connecting the feature map output mth and the bias reliable to the uth feature map and the activation function is denoted as. y_m^n.

4.3.1. Pooling layer

The phrase "sub-sampling layer" refers to a pooling layer that has two types of pooling: maximal and average pooling. That is unaffected by backward propagation and can be utilized to reduce the effects of

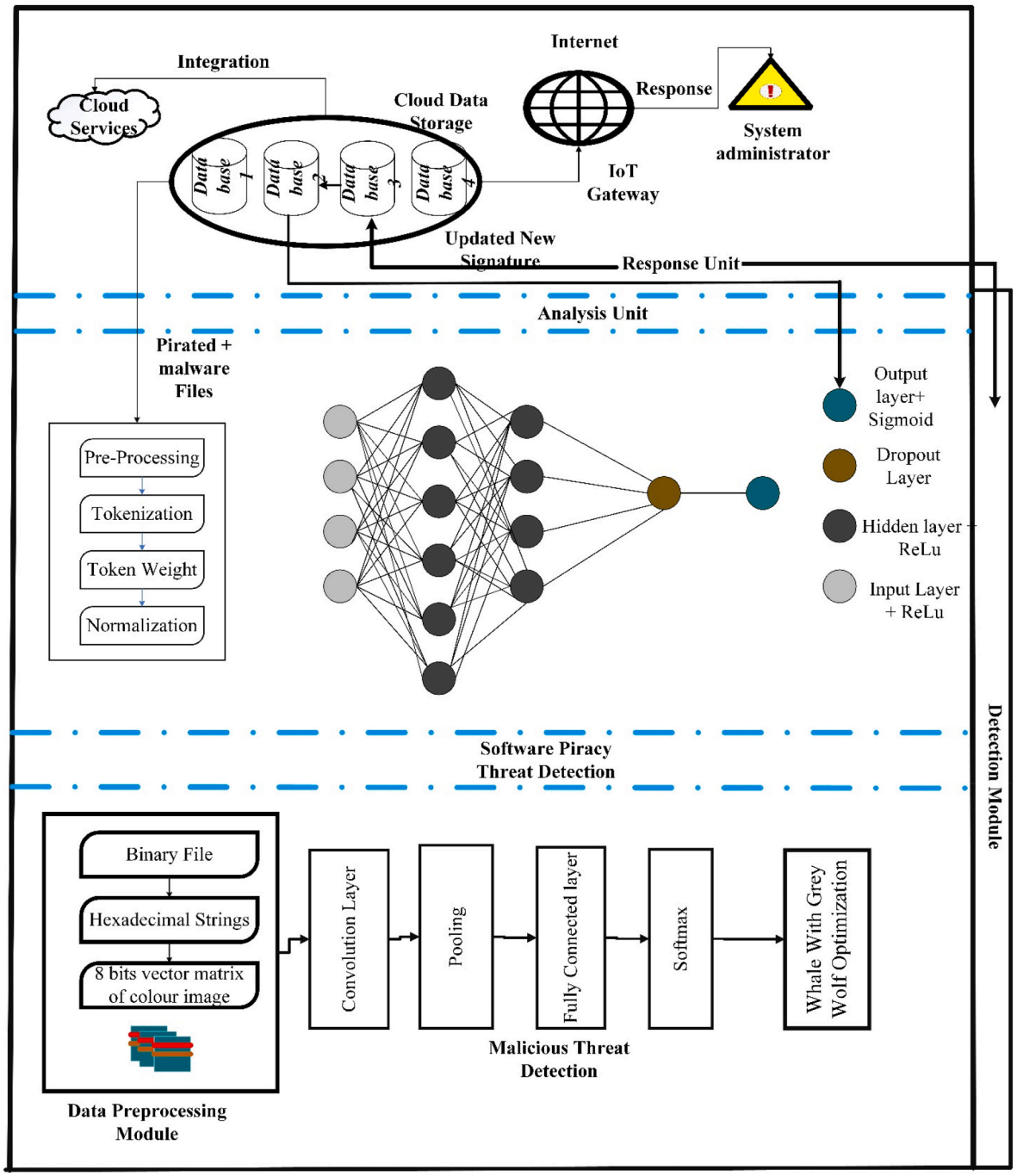

Fig. 2. Framework on cyber threat forecast in IoT.

visual distortions. As demonstrated in Equ (2), it also reduces the features' factor while increasing the suggested DCNN functionality.

$$a_m^n = f\left(down\left(a_m^{n-1}\right) + y_m^n\right) \tag{2}$$

The pooling task is performed by down and the bias value is represented by y.

4.3.2. Fully connected layer

The output of the max-pooling is classified using the fully connected layer. Every neuron has a fully linked layer that connects it to the neuron before it. This layer is designed to increase model generalization capability by reducing the problem of overfitting.

4.3.3. Learning

The malware variants are correctly classified according to their bloodline. SoftmaxCross-Entropy loss is used to train the suggested DCNN framework in this study. Equ (3) represents the Loss for the training data k.

$$Loss = -log\left(\frac{ep(f_{zt})}{\sum_k ep(f_{zt})}\right) \tag{3}$$

where fzt represents the kth grades, and fzt represents the proper family grade. The system variables are learned using the Adam optimizer, which attempts to diminish the loss of the training examples.

To minimize the training data loss hybrid optimization i.e) Improved whale optimization and adapted Grey Wolf Optimization is used, the

following section could determine the optimization process [17].

5. Hybrid optimization algorithm for optimal intrusion system

5.1. Whale optimization

Clustering separates the overall link into smaller, distinct clusters. As a result of clustering, a massive network seems smaller and much less active. Various system nodes are designated as Cluster - head in typical clusters, and it functions as a regional coordinator for every cluster and conducts communications inside it. A non-CH node that conducts intra-cluster transmissions is referred to as a clustermember. The data received on the Cluster - head is forwarded to the target via an intermediary Intermediate node, a process known as inter-cluster communication. A CH is not required to be present in every cluster [18]. CHs store route and topological data, removing thedemand from the conventional mobile node; yet, they act as network bottlenecks.The whale optimization algorithm (WOA) is based on humpback whale hunting behavior. Whales are among the world's largest mammals. A mature whale can reach 30 m in length and weigh 180 tonnes. Whales are primarily thought of as killers that never rest since they must breathe from the ocean's surface and only rest half of their brain. Spindle neurons are seen in some parts of the whales' brains that are comparable to those found in humans. Emotions, human judgment, and social behaviors are all controlled by these cells. Whales have been shown to understand, study, judge, interact, and become passionate in the same way as humans do, though with a far lower degree of intelligence [19].

$$A1_{u,v}^{g,k}(a)=\frac{K_{u,v}(a)k_{u,v}^{'}(a)}{\sum_{v\in\mathbb{N}_{i(a)}^{k}}K_{u,v}^{q1}(a)k'^{q1}_{u,v}(a)} \tag{4}$$

The parameters $\mathbb{N}_f^u$ and $\mathbb{N}_f$ depend on the number of accessible feeds for the u-th ant and the issue, respectively. Whenever an ant chooses a particular route for the source vertex, the set of possible searching paths is updated. The two probability transfer rules are used by the TAS method. For selecting the next nodes, the first stochastic transitioning rule is defined. The chance of the k-th ant picking node v, while it is positioned at a node $A1_{u,v}^{g,k}$. It is determined using heuristic information $k_{u,v}^{'}(a)$ and pheromone intensity$K_{u,v}(a)$. The effect of pheromones quantity and heuristic algorithm is determined by two variables, q1 and q2 which are mentioned in Equ (4) and (5):

$$A_{u,v}^{g,k}(a)=\frac{K_{u,v}^{2\gamma}(a)k_{u,v}^{'2\delta}(a)}{\sum_{v\in\mathbb{N}_{i(a)}^{k}}K_{u,v}^{2\gamma}(a)k_{u,v}^{2\delta}(a)} \tag{5}$$

Whales build the solutions by picking one node at a time and assigning one cluster to it.The complete indicates the sequence of vertices that follow their allocated groups while adhering to the restriction that no two adjoining vertices be allocated to different groups. The cost function is constructed using the paths walked and clusters allocated. Whales choose another node and allocate a cluster to it utilizing the probabilistic transition rules (4) and (5).The procedure in which each uses pheromones to indicate the separation between two nodes, increasing the desirability of an edge for the next choice [20].The $k_{u,v}^{'}(a)$ variable quantifies the number of pheromones for this border. For picking nodes, the heuristic functional $k_{u,v}^{'}(a)$ is constructed, which calculates in Equ (6):

$$k_{u,v}^{'}(a)=\frac{1+\left|\mathbb{N}_{u,i}^{k}\right|}{1+\left|\mathbb{N}_{n,u}\right|} \tag{6}$$

Considering the ant k cluster, the result is ak. If node n belongs to cluster L1,L2 = 0, else it is 0. The following is a calculation for the optimization technique mentioned in Equ (7):

$$S=\arg Max\sum_{i=1}^{\mathbb{N}_{sf}}\sum_{j=1}^{\mathbb{N}_z}c_{ij}+n_s \tag{7}$$

$\mathbb{N}_z$ represent the no. of clusters. Furthermore, a set of terminating conditions must be carefully established. It could be a predetermined maximum number of iterations or a difference in average textual length from the cluster centroid among two iterations.

$$F_{WO}=\frac{\sum_{u=1}^{\mathbb{N}^z}\left\{\sum_{v=1}^{\mathbb{N}_u}\frac{dis(z_u,h_v)}{\mathbb{N}_u}\right\}}{\mathbb{N}^z} \tag{8}$$

In the above Equ(8), z_u signifies the centroid vector of the uth cluster and h_v indicates the document vector vth cluster. The distance between the document vector and the centroid vector is combined and defined as (z_u,h_v). A fully interconnected network of a node would be constructed once the IWO classification algorithm has been successfully performed. Every edge is coupled with a given level of pheromone strength, and each enrolment is a document [21].

5.2. Adapted grey wolf optimization

Grey Wolf Optimization (GWO) is a simulation of grey wolf management and foraging behavior in the wild, where they hunt in packs of 5–12 wolves. GWO was created to help address optimization issues by identifying four different sorts of wolf dominance hierarchical structures: alpha, beta, delta, and omega. The key hunt stages of the GWO's behavior are investigation, enclosing, and striking the target. Alpha (a) is the group's most powerful member and decision-maker. Beta (b) serves as alpha's counselor. Fig. 3 shows that delta (d) and omega (w) are the 3rd and 4th ranks in the wolf hierarchy. The first three wolves are in charge of optimization, and the fourth is in charge of tracking down other wolves [22].

GWO is an inhabitant's bio-inspired method, which involves continuously modifying the placements of search agents to generate the optimal solutions. In data mining and machine learning systems, segmentation technique via feature selection algorithms is critical. Selection of features is a meta-heuristic application that selects the most relevant and timely features while disregarding the disruptive and repetitive ones. When the number of nodes grows excessively large, feature selection has become a complex and difficult issue. GWO's binary version outperforms the FS version in addressing the problem [23]. Research suggests a adapted version of the binary GWO, which is particularly useful during the demographic initialization stage. Researchers offer a smart starting strategy that allows us to find the optimal solution in the first iteration, accelerating the speed of convergence. The key change was to initialize the population by consulting filter-based knowledge and employing it in a wrapper-based manner rather than a random approach. The G score, which decides whether or not it should select a characteristic, is used to construct the random number. The

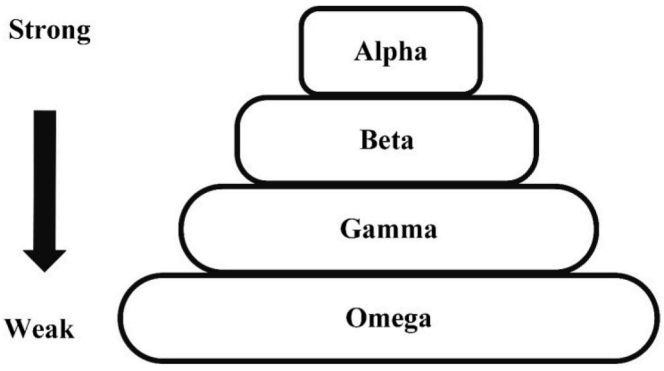

Fig. 3. Grey wolf hierarchy.

following equation (9) represents the calculation of the IG for a certain feature:

$$G(t) = -\sum P(xu)logP(xu) + P(t)\sum P(xu|t)\log P(xu|t) + P(t')\sum P(xu|t')logP(xu|t') \quad (9)$$

In the above Equ (9) the set of features is denoted as x and the no of class labels is denoted as u where the probability of the uth class is denoted as P(xu). The class probability is denoted as P (t) and P(t') and the provisionallikelihood is denoted as $P(xu|t)$ and $P(xu|t')$ based on the feature set t. The Crossover Error Rate (CER), also known as the Equal Error Rate (ERR), was used as the fitness value in this research because of the area of the suggested approach (cyber-security). The CER's major purpose is to reduce the gap between the False Negative Rate (F_{NR}) and the False Positive Rate(F_{PR}) [24]. To put it another way, a lower CER indicates superior efficiency. The following Equ (10) is used to compute the fitness value:

$$\downarrow F_{GW} = \alpha \times (|F_{PR} - F_{NR}|) + \beta \frac{|L|}{|N|} \quad (10)$$

where α and β are parameters ranging from 0 to 1 that represent the weight of each goal (β = 1-α). R denotes the number of characteristics selected. The total number of characteristics is denoted by the letter N. According to the research, F_{PR} stands for the False Positive Rate and F_{NR} stands for the False Negative Rate correspondingly; a was set to 0.99 and β to 0.01 [25].

The Adapted Grey Wolf Optimization methodology is developed as a adapted version of the GWO algorithm (MGWO). To begin, the computation resolution is accelerated by applying a filter-based technique to quantify the relevance of each characteristic and then using the results to inform the subset characteristics in the original population. Second, the ELM was chosen as the basic classification because it is a quick way to tackle the increased complexity. The MGWO was also utilized to fine-tune the ELM's set of weights. The proposed model is summarized in Fig. 4 [26].

The following Equ (11) represents the calculation of fitness function based on optimizing the attack prevention in cyber security using the hybrid whale Optimization and grey wolf optimization. Consider the Fitness function of the whale optimization from Equ (8) and the grey wolf fitness function from Equ (10) which is combined together as

$$F_{WGW} = \left(\frac{\sum_{u=1}^{\mathbb{N}^z} \left\{ \sum_{v=1}^{\mathbb{N}_u} \frac{dis(z_u, h_v)}{\mathbb{N}_u} \right\}}{\mathbb{N}^z} \right) \times \left(\alpha \times (|F_{PR} - F_{NR}|) + \beta \frac{|L|}{|N|} \right) \quad (11)$$

6. Result and discussion

The programming plagiarism test can be utilized to look for code similarities in software piracy. To investigate the methodological approach for software piracy, we used data from Google Code Jam (GCJ).The information is first refined to extract the relevant tokens for each origin together with frequency components. Root words, maximum, stemming, and minimum token lengths, maximum and minimum token frequencies, and so on are all part of the preprocessing process. Second, the tokens' weight is determined using a selection of features and extraction methods such as Term Frequency and Inverse Document Frequency (TFIDF) and Logarithm Word Frequency (LogTF). Just on the x-axis, the letters L1, L2,L3, and L4 represent the programming solutions to four different issues. On the y-axis are the weighting numbers of each programming language. Researchers had four input parameters in the first solid layer since each coder addressed four distinct programming issues. To boost performance, the second and the third levels are set as concealed layers. To avoid the fitting problem, the dropout layer is programmed with inputs and each concealed layer.

Fig. 5 shows a dynamic depiction of validation data, loss, accuracy,

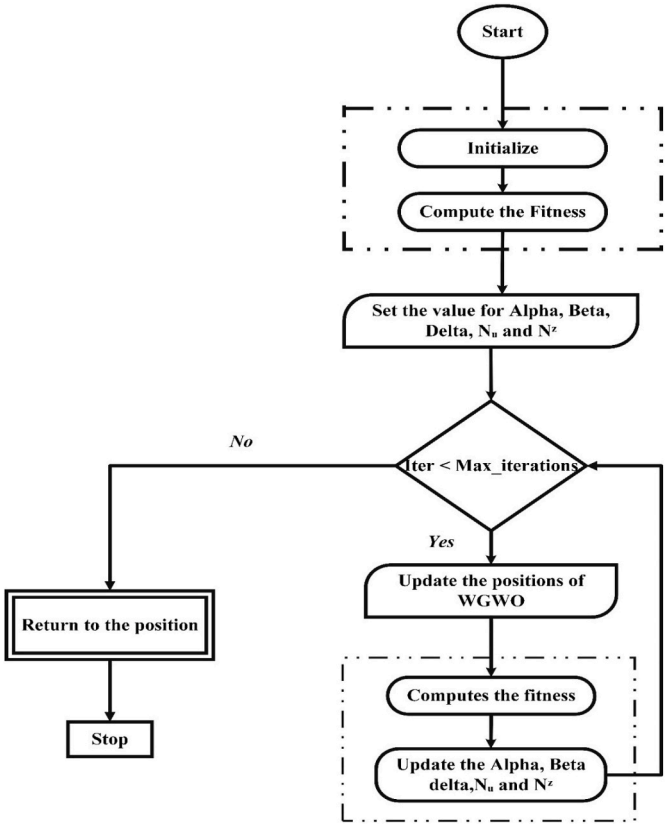

Fig. 4. Flowchart on adapted grey wolf algorithm.

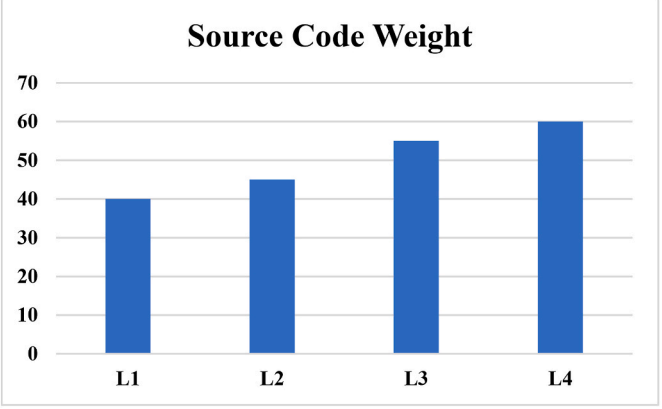

Fig. 5. Source code weight.

and validation loss in terms of percentage. The blue curve in the top image depicts the loss, whereas the green curve depicts the validation loss.

Overfitting occurs when these curves increase or behave oppositely. Table 1 shows a contrastamong the suggested strategy and other state-

Table 1
Piracy detection comparison.

Algorithm	Source	Accuracy
K-nearest network (KNN)	Java	85%
Latent Semantic Analysis (LSA)	C++, Java	97%
Parse Tree	Java	91%
Multiple Linear Regression (MLR)	Python, Java, C++	87%
Deep Neural Network (DNN)	Proposed Method	99%

of-the-art techniques and a graphical representation of the table is presented in Fig. 6.

Researchers investigated the impact of different malware image proportions on the suggested malware detection method's classifier performance. 225 × 225 and 228 × 228 were the image proportions. From the Leopard Smartphone high-dimensional data, we chose 14,733 malware and 2486 benign items. After testing, we found that the 228 × 228 ratio outperformed the 225 × 225 ratio in terms of categorization accuracy. Nevertheless, there was a considerable variation in categorization accuracy between the 228 × 228 and 225 × 225 image sizes. As a result, researchers concluded that the 229 × 228 image ratio is a better fit for the suggested malware detection approach.For 225 × 225 and 228 × 228 image\sratios, the dynamic graphs for accuracy, loss, validatedaccuracy and loss are displayed in Figs. 7 and 8.

Table 2 compares the prediction performance of several picture proportions to illustrate the role of image proportion on classifier efficiency. For the Leopard Mobile dataset, the 228 × 228 image ratio achieved a 98% percent accuracy rate in 35 s. Fig. 9 shows the graphical representation of the efficiency comparison. In above Fig. 9, the blue bar denotes the 225 × 225 proportion, and the grey bar denoted the 224 × 224 proportion.

For the initialization stage, four injecting proportions of 25%, 50%, 75%, and 100% were evaluated, with the average being chosen. Fig. 10 represents the overall assessment. The algorithm showed the best performance when 20 hidden synapses were used and the sigmoid function was used. The population numbers, on the other side, were adjusted to 10 based on a scenario analysis of several value systems: 5, 10, 25, 75, and 100 search agents, as shown in Fig. 11. With 10 candidate solutions, the system efficiency better in terms of accuracy and CER, while the number of repetitions was set at 100 depending on the outcomes.

7. Conclusion

In the coming years, the commercial IoT platform will significantly expand. The key hurdles in the realm of cybersecurity with IoT-based big data include detecting unauthorized copying and malware attacks. For the detection of pirated and malicious files, researchers presented a hybrid deep learning-based technique. First, utilizing software piracy, the TensorFlow neural net is designed to recognize the pirated characteristic of software. To evaluate the proposed methodology, researchers gathered 100 computer operator source code files from GCJ. The source code is cleaned of noise and highly processed to capture even more high-quality information, such as important tokens.In this research, we present an enhanced bio-inspired meta-heuristic approach to improve the

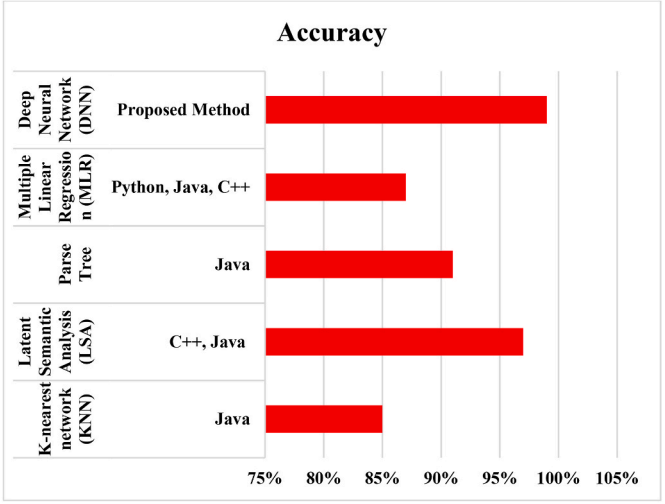

Fig. 6. Accuracy comparison.

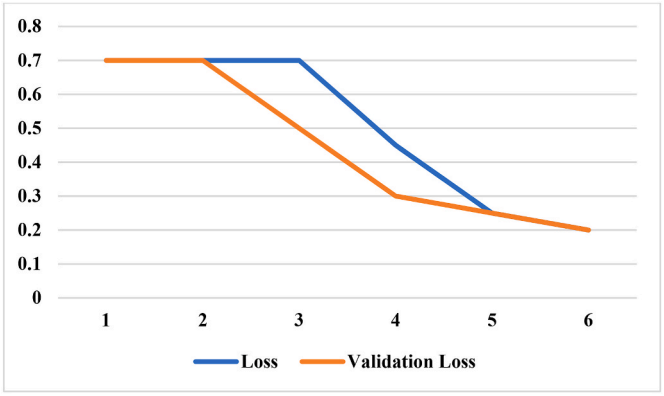

Fig. 7. Comparison on loss and validation loss.

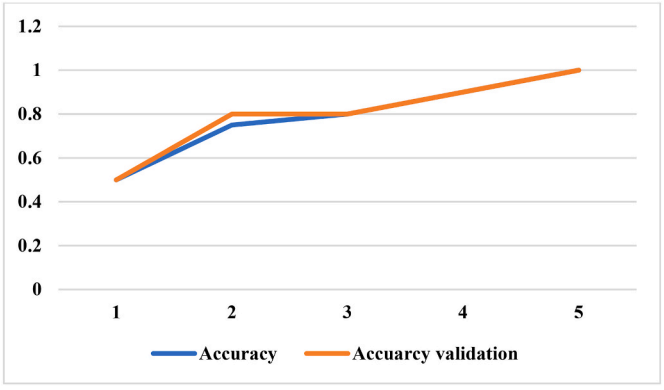

Fig. 8. Accuracy and accuracy validation comparison.

Table 2
Classification efficiency comparison.

Proportion Image	Accuracy	Specificity	Sensitivity	F1 score	Period
225 × 225	96%	95.17%	95.12%	95.15%	18s
228 × 228	98%	97.45%	97.47%	97.45%	35s

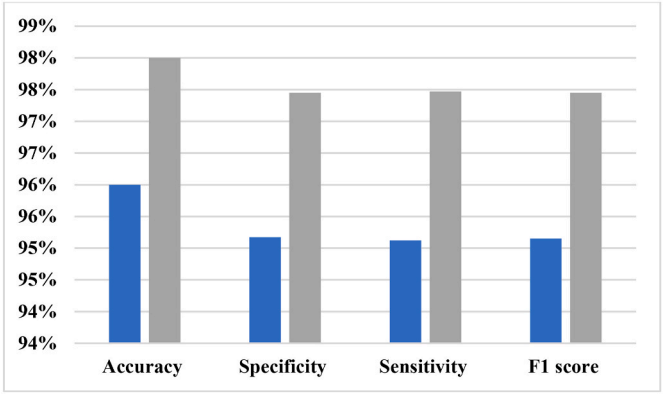

Fig. 9. Classification efficiency comparison.

efficacy of IDSs. The updated GWO was used and enhanced to choose the best feature set and remove unnecessary and noisy features. The updated hybrid optimization enhanced the algorithm's convergence rate by using an intelligent starting method. This intelligent management is part of the G ratings from the filter-based technique to initialize the populace in the wrapper-based method. To counteract the computation enhanced

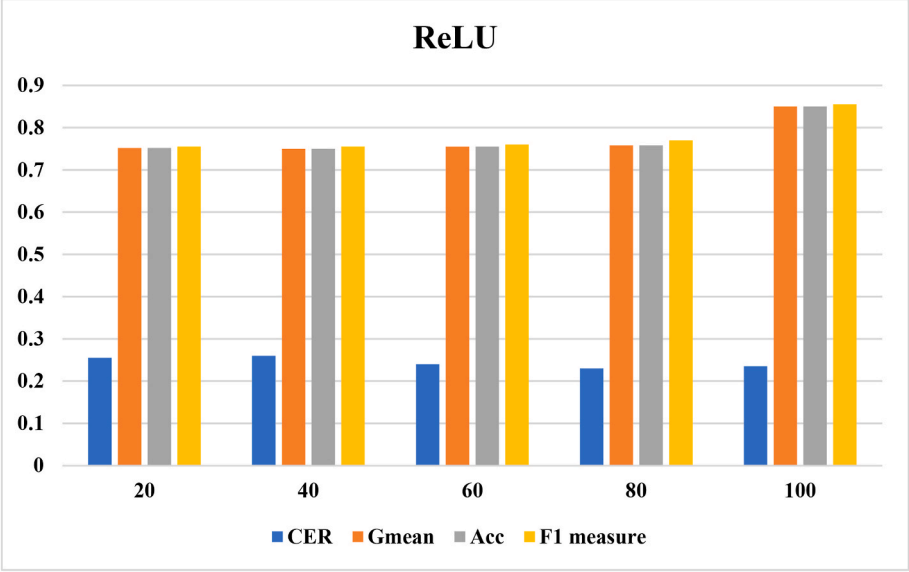

Fig. 10. ReLU outcome.

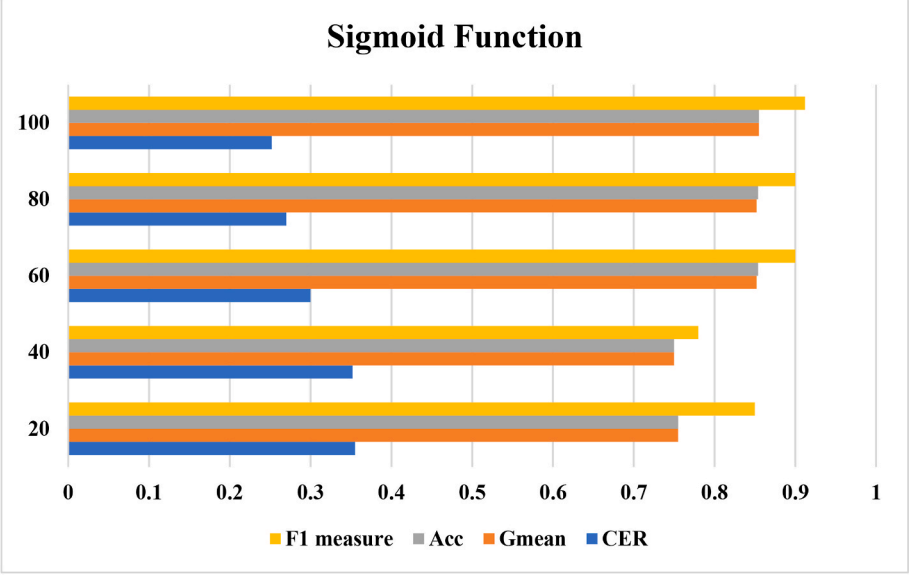

Fig. 11. Sigmoid function outcome.

complexity, the ELM was used as a basic classifier. As a consequence, the hybrid optimization (WGWO) was used to modify the ELM's set of weights in addition to the FS process.The experimental findings show that the suggested technique for measuring cyber security hazards in IoT has superior classification results to existing methods. Hence to detect the attack prevention in IoT process Whale with Grey wolf optimization (WGWO) and deep convolution network is used. The malware's visual properties were then fed into a deep convolutional neural network. The analyzed outcome demonstrated that when contrasted to state-of-the-art methodologies, the combination yields the best classification performance.

Credit author statement

Regonda Nagaraju: Conceptualization. Jupeth Toriano Pentang: Data Collection. Shokhjakhon Abdufattokhov: Problem statement Perseverance., Ricardo Fernando CosioBorda: Implementation and validation. Dr. N. Mageswari: Additional Validation. G. Uganya: Overall Supervision.

Declaration of competing interest

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.

References

[1] Y. Fu, Y. Du, Z. Cao, Q. Li, W. Xiang, A deep learning model for network intrusion detection with imbalanced data, Electronics 11 (6) (Mar. 2022) 898, https://doi.org/10.3390/electronics11060898.

[2] R. Damasevicius, et al., LITNET-2020: an annotated real-world network flow dataset for network intrusion detection, Electronics 9 (5) (2020) 800, https://doi.org/10.3390/electronics9050800.

[3] K.-H. Le, M.-H. Nguyen, T.-D. Tran, N.-D. Tran, IMIDS: an intelligent intrusion detection system against cyber threats in IoT, Electronics 11 (4) (Feb. 2022) 524, https://doi.org/10.3390/electronics11040524.

[4] F.A. Narudin, A. Feizollah, N.B. Anuar, A. Gani, Evaluation of machine learning classifiers for mobile malware detection, Soft Comput. 20 (1) (2016) 343–357, https://doi.org/10.1007/s00500-014-1511-6.
[5] C. Gupta, I. Johri, K. Srinivasan, Y.-C. Hu, S.M. Qaisar, K.-Y. Huang, A systematic review on machine learning and deep learning models for electronic information security in mobile networks, Sensors 22 (5) (2017), https://doi.org/10.3390/s22052017, 2022.
[6] S. Javaid, N. Javaid, T. Saba, Z. Wadud, A. Rehman, A. Haseeb, Intelligent resource allocation in residential buildings using consumer to fog to cloud based framework, Energies 12 (5) (2019) 815, https://doi.org/10.3390/en12050815.
[7] M.H. Ali, et al., Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), Electronics 11 (3) (Feb. 2022) 494, https://doi.org/10.3390/electronics11030494.
[8] H.D. Menéndez, J.L. Llorente, Mimicking anti-viruses with machine learning and entropy profiles, Entropy 21 (5) (2019) 513, https://doi.org/10.3390/e21050513.
[9] W.-C. Lin, Y.-R. Yeh, Efficient malware classification by binary sequences with one-dimensional convolutional neural networks, Mathematics 10 (4) (Feb. 2022) 608, https://doi.org/10.3390/math10040608.
[10] A. Churcher, et al., An experimental analysis of attack classification using machine learning in IoT networks, Sensors 21 (2) (Jan. 2021) 446, https://doi.org/10.3390/s21020446.
[11] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 16 (1) (Dec. 2015) 20, https://doi.org/10.3390/s16010020.
[12] A. Singh, A. Sharma, S. Rajput, A.K. Mondal, A. Bose, M. Ram, Parameter extraction of solar module using the sooty tern optimization algorithm, Electronics 11 (4) (Feb. 2022) 564, https://doi.org/10.3390/electronics11040564.
[13] A. Alzaqebah, I. Aljarah, O. Al-Kadi, R. Damaševičius, A modified grey wolf optimization algorithm for an intrusion detection system, Mathematics 10 (6) (Mar. 2022) 999, https://doi.org/10.3390/math10060999.
[14] G. Liu, B. Peng, X. Zhong, A novel epidemic model for wireless rechargeable sensor network security, Sensors 21 (1) (2020) 123, https://doi.org/10.3390/s21010123.
[15] Y. Fu, Y. Du, Z. Cao, Q. Li, W. Xiang, A deep learning model for network intrusion detection with imbalanced data, Electronics 11 (6) (2022) 898, https://doi.org/10.3390/electronics11060898.
[16] A.A. Ewees, et al., A cox proportional-hazards model based on an improved aquila optimizer with whale optimization algorithm operators, Mathematics 10 (8) (2022) 1273, https://doi.org/10.3390/math10081273.
[17] M.H. Ali, et al., Threat analysis and distributed denial of service (DDoS) attack recognition in the internet of things (IoT), Electronics 11 (3) (Feb. 2022) 494, https://doi.org/10.3390/electronics11030494.
[18] E.M. Ahmed, et al., BONMIN solver-based coordination of distributed FACTS compensators and distributed generation units in modern distribution networks, Ain Shams Eng. J. 13 (4) (2022), 101664, https://doi.org/10.1016/j.asej.2021.101664.
[19] P. Reddy, V. Reddy, T.G. Manohar, Whale optimization algorithm for optimal sizing of renewable resources for loss reduction in distribution systems, Renew. Wind Water Sol. 4 (1) (2017) 1–13, https://doi.org/10.1186/s40807-017-0040-1.
[20] S. Ullah, et al., A new intrusion detection system for the internet of things via deep convolutional neural network and feature engineering, Sensors 22 (10) (May 2022) 3607, https://doi.org/10.3390/s22103607.
[21] Z. Huang, L. Chen, M. Li, P.X. Liu, C. Li, A multiple learning moth flame optimization algorithm with probability-based chaotic strategy for the parameters estimation of photovoltaic models, J. Renew. Sustain. Energy 13 (4) (2021), 043502, https://doi.org/10.1063/5.0048961.
[22] S. Mirjalili, S.M. Mirjalili, A. Lewis, Grey wolf optimizer, Adv. Eng. Software 69 (2014) 46–61, https://doi.org/10.1016/j.advengsoft.2013.12.007.
[23] H. Almazini, K. Ku-Mahamud, Grey wolf optimization parameter control for feature selection in anomaly detection, Int. J. Intell. Eng. Syst. 14 (2) (2021) 474–483, https://doi.org/10.22266/ijies2021.0430.43.
[24] B. Feng, Y. Xu, T. Zhang, X. Zhang, Hydrological time series prediction by extreme learning machine and sparrow search algorithm, Water Supply 22 (3) (2022) 3143–3157, https://doi.org/10.2166/ws.2021.419.
[25] N. Koryshev, I. Hodashinsky, A. Shelupanov, Building a fuzzy classifier based on whale optimization algorithm to detect network intrusions, Symmetry 13 (7) (2021) 1211, https://doi.org/10.3390/ijgi10060382.
[26] H. Faris, I. Aljarah, M.A. Al-Betar, S. Mirjalili, Grey wolf optimizer: a review of recent variants and applications, Neural Comput. Appl. 30 (2) (2018) 413–435, https://doi.org/10.1007/s00521-017-3272-5.