Malware Detection in IoT Enabled Multimedia Environment Using the Feline Cad-based Deep CNN

Seelam Sai Satyanarayana Reddy[1,*,†], Harikrishna Bommala[1,†]

[1]Department of CSE,KG Reddy College of Engineering & Technology, Moinabad, Hyderabad, Telangana, India.

Abstract

With the fast development of data innovation, the Internet of Things (IoT) likewise arose and it helps individuals in their day to day routines to work more brilliant. Nonetheless, the organization is helpless against malware assaults, which should be killed for secure communication. Therefore this examination presents a green malware discovery strategy inside the interactive media environmental elements the use of the AI procedure. At first, the data is accumulated from the IoT empowered interactive media gadgets. Then, at that point, the fundamental 27 ascribes are separated from the assembled data for the evacuation of overt repetitiveness and to decrease the intricacy of calculation. At long last, utilizing the Profound convolution brain organization (Profound CNN) the malware recognition is utilized, which is prepared utilizing the proposed cat scoundrel improvement calculation that coordinates the way of behaving of the birdie with the bothering conduct of the cat to get a more exact discovery. The proposed technique is assessed concerning exactness, awareness, and particularity and acquired the upsides of 99.95%, 97.45%, and 96.12% separately.

Keywords

Machine Learning, IoT, Multimedia, Malware Detection, Optimization

1. Introduction

With the rapid growth and digitization, the Internet of Things (IoT) is utilized to cover enormous smartp devices, technologies, services, and products each other into a single manageable thing. It is widely utilized in several applications in daily lives such as voice assistants, smart grids, sensors, smart homes, cites, traffic, and so on. While considering the traditional networks IoT solves the complicated tasks efficiently because the traditional networks follow several determined rules [1]. Here, for the smart city management, several homes are connected that comprises monitoring and the surveillance system based on the wireless multimedia. In the smart home environment, the camera is considered as a multimedia device, which gathers the information and transmits it to the administrators and the owner of the home. Here, the constrained application protocol is utilized for the communication among the connected devices because it is considered as a lightweight protocol and is appropriate for information sharing among multimedia systems [2]. In public network security, encryption over encryption techniques are used to secure the networks [3]. Many applications Nowadays, IoT is utilized and the information threat is the

ACI'23: Workshop on Advances in Computational Intelligence at ICAIDS 2023, December 29-30, 2023, Hyderabad, India

[*]Corresponding author.

[†]These authors contributed equally.

saisn90@gmail.com (S. S. S. Reddy); haribommala@gmail.com (H. Bommala)
0000-0002-2985-3555 (S. S. S. Reddy); 0000-0002-9932-6152 (H. Bommala)

most challenging task in the network. Public surveillance systems [4] are common applications to prevent from malware attacks. Hence, malware detection is significant for the IoT multimedia device for secure communication among the devices [1]. Malware detection can be done through signature-based methods, visualization ideas, and machine learning-based techniques for the detection and mitigation of malware from the network [5]. The machine learning techniques transform the binary code to image data and visualize the result for various samples and the speed of detection can also be enhanced through machine learning. The malware identification and mitigation are easier and simple while considering the traditional method of the malware detection technique [6]. Machine learning methods [7, 8] are used to identify and predict the network attacks. The non-destructive malware detection method detects the malware without any feature selection strategy. In addition, the optimization strategy of machine learning further enhances the accuracy of detection. Besides, machine learning offers reduced computation complexity with minimal processing time along with robust performance [9]. The research aims to devise an efficient malware detection technique based on the multimedia-enabled IoT scenario. For safe interaction among the devices, malware needs to be detected and prevented. Thus, an automatic malware detection technique is required with a more accurate detection rate. Here, a novel optimization-based machine learning is introduced for malware detection in the multimedia-enabled IoT environment. For this Feline cad optimization algorithm is proposed by integrating the foraging behavior of the birdie and the hounding behavior of the feline, which is used to train the Deep convolutional neural network (Deep CNN) that enhances the detection accuracy through the fast convergence rate and global best solution. The major contribution of the research is:

- Proposed Feline cad optimization: The proposed feline cad optimization is designed by integrating the foraging behavior of the birdie with the hounding behavior of the feline to obtain the global best optimal solution for tuning the weights of the Deep CNN for the malware detection.
- Proposed Cat creep based Profound CNN for malware recognition: The malware location in the mixed media empowered IoT climate is finished utilizing the Profound CNN, which is prepared utilizing the proposed Cat scoundrel streamlining. Here, the loads of the classifier are tuned to get a more exact identification through quick union rate by staying away from the catching at neighborhood optima.

The remaining section of the research is: Section 2 details the literature review along with the challenges faced by the existing system. Section 3 elaborates the system model of the proposed method and the result and discussion is presented in Section 4. Finally, the conclusion is provided in section 5.

2. Motivation

This section details the review of the conventional literature regarding the multimedia-enabled IoT-based malware detection techniques. The challenges faced by the existing system motivate the author to devise a novel malware detection technique based on machine learning.

2.1. Literature Review

The conventional methods of malware detection based on multimedia-enabled IoT is detailed in this section. The multimedia-enabled IoT-based attack detection was utilized by [2] using the adaptive hybrid strategy that uses the timed automata controller technique. Here, the detection of the malware was done through the timed automaton with self-tuning, in which the pattern set for malware was created based on the signature by the crowd-sourcing online repository. Besides, the knowledge regarding the multimedia file format was utilized for the analysis of packets that carries the multimedia files and obtained enhanced classification accuracy. A machine learning-based malware detection was employed in [6] for the IoT environment to avoid the threat. In this strategy, both the unknown and known malware was detected in a very fast manner. Besides, the feature extraction and selection were performed before the detection of malware. Minimal error along with better accuracy was obtained by the method utilized. Dynamic differential game-based cloud-assisted malware detection was utilized by [5] to provide a secure network. Here, the secure data sharing was done using the support vector machine (SVM) and the cost function is minimized through the optimal defense strategy. The utility was evaluated to show the performance enhancement of the malware detection technique. IoT-based malware detection based on the mobile multimedia application was used by [1] through the machine learning approach. Here, the features based on the permission were extracted and were utilized to train the classifier to enhance the classification accuracy. The feature selection was done using the random forest regressor to minimize the number of features for further processing. The accuracy was evaluated to show the performance enhancement. The IoT-based malware detection was employed by [10] based on the intelligent behavior, in which the rule based and learning-based features were selected for the detection of the unknown malware. Here, the elevated accuracy and minimal FNR and FPR were the achievements obtained by the introduced method.

2.2. Challenges

The difficulties looked by the customary media based IoT malware discovery is point by point in this segment.

- The computation complexity of the network is not evaluated and the delays such as state transition and response are neglected [2].
- The machine learning technique for malware detection obtained better accuracy but failed to incorporate the optimization approach that enhances the detection accuracy further [1, 6].
- With the usage of Nash equilibrium criteria, the computation deviation happens, which is considered a non-negligible deviation [5].
- The malware detection technique developed by [10] utilizes an elevated number of features and is not suitable for the detection of new malware.

3. Proposed Methodology

The interaction of device to device in the virtual and physical environment through the collection of protocols, interfaces, and multimedia-related information constitutes the multimedia-enabled IoT. During the communication process, the malware attack in such a network is unavoidable. Hence there is a need for an automatic malware detection technique. Here, an efficient technique named, Feline cad-based Deep CNN is proposed for the detection of malware in the multimedia-enabled IoT network. Initially, the information from the multimedia-enabled IoT devices is gathered and then pre-processed to extract the essential 27 attributes. Here, the first five attributes such as SHA1 hashes and executable MD5 unique attributes along with three textual attributes such as dynamic compilers, functions, and libraries are extracted. In addition, the remaining 22 numerical attributes such as entropy, time data stamp, uninitialized data size, header's optional size, initialized data's size, image and code size, size of the pointer to the symbol table, type of PE, total symbols, total section number, size and virtual address number, magic, machine, the base of the image, alignment of the file, characteristics of dynamic link library, database, and codebase are also extracted. From the extracted 27 attributes, the malware detection is employed using the proposed Feline cad-based Deep CNN, in which the classifier named Profound CNN is prepared utilizing the proposed Cat creep advancement calculation to improve the exactness of recognition. The illustration of the proposed Feline cad-based Deep CNN for malware detection is shown in Fig. 1.

3.1. Data Pre-processing

The data acquisition for the proposed malware detection technique is taken from the Brazilian-malware-dataset [8], in which 22 attributes numeral attributes, 2 unique attributes, and 3 textual attributes are utilized for the malware detection. Initially, the null data needs to be checked and it should be removed if available. Then, the above mentioned 27 significant attributes are extracted and the redundant information is removed for the reduction of the computational complexity.

3.2. Proposed Feline cad based Deep CNN for malware detection

The malware detection in the multimedia-enabled IoT environment is done using the proposed Feline cad optimization based on Deep CNN. Here the malware detection is done using the extracted 27 attributes from the IoT network which is fed as input to the Deep CNN. The Profound CNN is prepared utilizing the proposed Cat lowlife enhancement calculation to expand the precision of identification.

3.2.1. System model of Deep CNN

A deep convolutional neural network (Deep CNN) [11] is widely used in visual imaginary-based applications due to its efficiency, accuracy, and reliability. Besides, Deep CNN is a feed-forward category network, in which the feedback cannot be fed in itself. The Deep CNN comprises several layers such as a fully connected layer, pooling layer, and convolutional layer. The functioning of each layer is detailed below and is illustrated in Fig. 2.

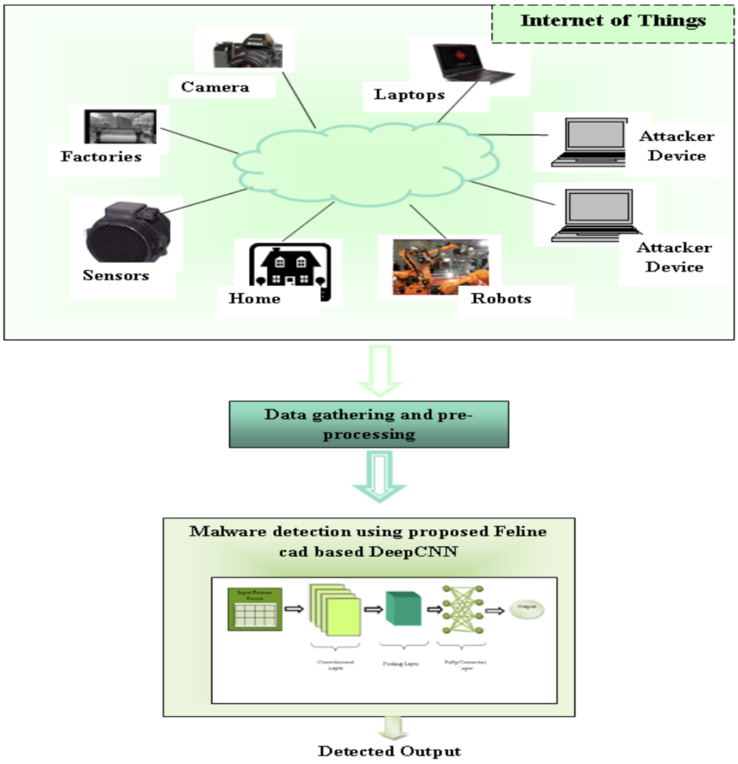


Figure 1: System model of proposed Feline cad based Deep CNN for malware detection

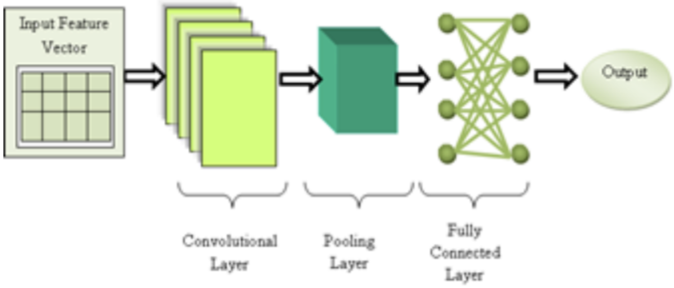


Figure 2: Architecture of Deep CNN

Convolutional Layer: The input attributes are fed into the convolutional layer, in which several patterns are generated, and it performs the convolutional operation with the filters and forms the feature maps. Here, the input is categorized into several windows and these categorized inputs are convolved with the filters based on certain weights. The output obtained by the convolutional neural network is formulated as,

$$X_x^T = E_x^T + \sum_{y=1}^{c1(T-1)} L_{x,y}T \times P_x^{(T-1)} \tag{1}$$

where, L refers to the size of the kernel, the x^{th} feature map with the layer T is notated as X_x^T, the bias is represented as E, and the weight is denoted as P.

Pooling Layer: The down-sampling of the spatial dimension is performed in this layer to avoid overfitting issues. The output obtained in this layer is invariant to distortions and translational shifts.

Fully connected layer: The output produced at this layer is nonlinear. Here, the activation function named Rectified Linear Unit (ReLU) is used to avoid the issues related to the vanishing gradient problem. The output of the fully connected layer is formulated as,

$$X_x^T = f\left(d_x^T\right) \text{ with } d_x^T = \sum_{y=1}^{c1(T-1)} \sum_{p=1}^{2(T-1)} \sum_{q=1}^{c3(T-1)} P_{x,y,p,q}^I \left(X_y^{T-1}\right)_{p,q} \tag{2}$$

where, the weights of the location (p, q) is referred as $P_{x,y,p,q}^I$ and $c1(T-1$, $c2(T-1)$, and $c3(T-1)$ refers to the feature maps $Wei_{r,s,x,y}^I$ refers to the weights of the location. The loads of the classifier are tuned utilizing the proposed Cat Miscreant Advancement calculation to limit the preparation misfortune and to raise the location precision.

3.2.2. Proposed Feline Cad Optimization algorithm

The proposed feline cad optimization is designed by integrating the foraging behavior of the birdie [12] with the hounding behavior of the feline [13] to enhance the searching capability and for the attainment of a more accurate global best optimal solution. Thus, more accurate malware detection is possible through the proposed method. *a) Motivation* Birdie is a bird with strong memory and intelligence and is mostly a residential bird. Cadger and the producer are the two different categories of the birdie in the food search. Here, the cadger obtains food from the producer and the producer obtains its food in the searching process. The low energies birdie utilizes the cadging behavior than the producer. In addition, the feline is a hunting animal with deliberate and hounding characteristics. The hounding characteristic of the feline to hunt the target is high and clear. Thus, in the proposed optimization the foraging behavior of the birdie is incorporated with the hounding behavior of the feline to enhance the convergence rate. *b) Mathematical modeling* For the mathematical modeling of the proposed feline cad optimization, the fol-lowing rules are considered. *Rule 1:* The producers of birdie are high-energy members and they need to direct all the cadger in the group in search of food. The energy reserves depend on the fitness value of the birdie. *Rule 2:* An alarming signal is generated by the birdie when they detect a predator. The producer birdie needs to lead the entire cadger in the group to a safe location when the alarming sound exceeds the threshold level. *Rule 3:* The proportion of both the cadger and the producer remains the same in the population, but the birdie with better food searcher can become the producer of the food source. *Rule 4:* The producers have more energy levels and the cadgers are in search of food when they are in a starving condition. *Rule 5:* The cadgers follow the producers in search of the food and they constantly monitor them for enhancing the level of predation. *Rule 6:* When the birdies in the edge face the danger then they move randomly to-ward the neighbor in the safe area.

Initialization: The birdies in the population can be initialized as,

$$C = \begin{bmatrix} C_{1,1} & C_{1,2} & \cdots & \cdots & C_{1,s} \\ C_{2,1} & C_{2,2} & \cdots & \cdots & C_{2,s} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C_{r,1} & C_{r,2} & \cdots & \cdots & C_{r,s} \end{bmatrix} \tag{3}$$

where, s refers to the dimension of the solution and r refers to the birdie. The fitness of the birdie in the population is formulated as,

$$A_C = \begin{bmatrix} f([C_{1,1} & C_{1,2} & \cdots & \cdots & C_{1,s}]) \\ f([C_{2,1} & C_{2,2} & \cdots & \cdots & C_{2,s}]) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ f([C_{r,1} & C_{r,2} & \cdots & \cdots & C_{r,s}]) \end{bmatrix} \tag{4}$$

Here, the fitness of the unique birdie is represented in a row. The producers have the highest fitness and have the priority in food search and are responsible for guiding all the members. Thus, the producers search more areas compared to the cadger. Here, the search capability of the producer is enhanced by incorporating the hounding capability of the feline in search of food. Then, the position updation of the producer depends on rule 1 and 2 and is formulated as,

$$C_{p,q}^{\tau+1} = \begin{cases} C_{p,q}^{\tau} \cdot \exp\left(\frac{-p}{\beta \cdot i_{\max}}\right) & \text{if Rand 2} < D \\ C_{p,q} + EF & \text{if Rand 2} \geq D \end{cases} \tag{5}$$

where, τ refers to the iteration, the p^{th} birdie in q^{th} dimension is referred as $C_{p,q}$. The random number is represented as $\beta \in [0,1]$, the alarm value is notated as Rand 2 $\in [0,1]$ and the safety threshold is referred as $D \in [0,5,1]$. The random number that satisfies the normal distribution is notated as E and the matrix of size $[1 \times s]$ is denoted as F. The producers search the food when there are no predators found, which satisfies the condition Rand 2 $< D$. The birdies fly to the safe location when they found the predator, the condition for it is Rand 2 $\geq D$.

As per rule 5 cadgers search and monitors the producers and when they found the food immediately move to the food-rich location and compete with the producer. If they win, then the position updation of the cadger is formulated as,

$$C_{p,q}^{\tau+1} = \begin{cases} E \cdot \exp\left(\frac{C_{\text{worst}}^{\tau} - C_{p,q}^{\tau}}{\beta \cdot i_{\max}}\right) & \text{if } p > r/2 \\ C_G^{\tau+1} + \left|C_{p,q}^{\tau} - C_G^{\tau+1}\right| \cdot H^{+} \cdot F & \text{otherwise} \end{cases} \tag{6}$$

where, the optimal position of the producer is referred as C_G, the worst solution is denoted as C_{worst}^{τ} , and $H^{+} = H^{T}\left(HH^{T}\right)^{-1}$. The birdie with the lowest fitness is considered as starving and the condition for it is $p > r/2$.

Let us consider 10% to 20% of the birdie are aware of the danger and according to rule 6 , the position updation is formulated as,

$$C_{p,q}^{\tau+1} = \begin{cases} C_{\text{best}}^{\tau} + \alpha \left| C_{p,q}^{\tau} - C_{\text{best}}^{\tau} \right| & \text{if } a_p > a_v \\ C_{p,q}^{\tau} + I\left(\frac{\left| C_{p,q}^{\tau} - C_{\text{worst}}^{\tau} \right.}{\left(a_p - a_u\right) + \gamma} \right) & \text{if } a_p = a_v \end{cases} \tag{7}$$

where, the constant included to minimize the zero-divisionerror is represented as γ, the control parameter for the step size is referred as α, the best solution is referred as C_{best}^{τ} , and the random number is represented as I, and ranges between $[-1, 1]$. Here, the current birdie's present fitness is represented as a_p and the worst and the best fitness of the birdie are notated as a_u and a_v respectively. The condition $a_p > a_v$ indicates that the birdie is at the edge and $a_p = a_v$ depicts the danger and hence moves towards the other members of the group.

The position updation based on the hounding capability of the feline in search of food is formulated as,

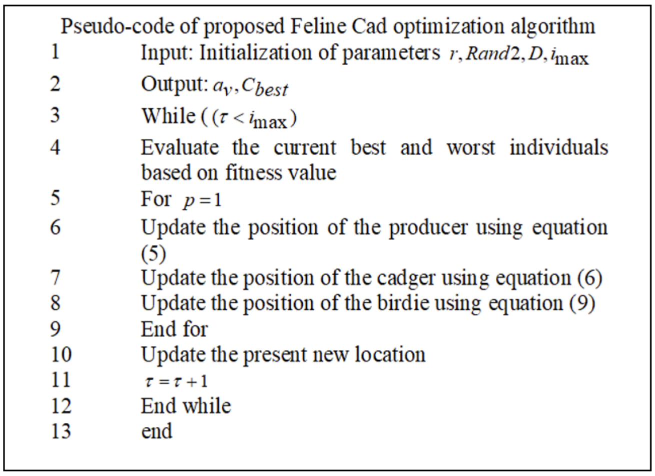
$$C_{p,q}^{\tau+1} = C_{p,q} + V_{k,d} \tag{8}$$

where, the velocity of searching for food by the feline at p^{th} feline in q^{th} dimension.

As per the rule utilized in [14] utilized for the integration of the characteristic behavior of two algorithms by combining equation (7) and equation (8) and is expressed as,

$$Y_l' = 0.5\left[C_{best}^{\tau} + \alpha \left| C_{p,q}^{\tau} - C_{best}^{\tau} \right|\right] + 0.5\left[C_{p,q}^{\tau} + V_{k,d}\right] \tag{9}$$

The pseudo-code for the proposed Feline cad optimization algorithm is presented in Fig. 3 given below.



Pseudo-code of proposed Feline Cad optimization algorithm

```
Input: Initialization of parameters $r, Rand2, D, i_{\max}$
Output: $a_v, C_{best}$
While ( $(\tau < i_{\max})$
Evaluate the current best and worst individuals based on fitness value
For $p = 1$
Update the position of the producer using equation (5)
Update the position of the cadger using equation (6)
Update the position of the birdie using equation (9)
End for
Update the present new location
$\tau = \tau + 1$
End while
end
```

Figure 3: Pseudo-code for the proposed Feline cad optimization algorithm

Here, the global best solution obtained is utilized for tuning the weights of the Deep CNN optimally. The proposed calculation has the capacity to get the worldwide arrangement with quick assembly by staying away from the catching at neighborhood optima utilizing the reasonable investigation and abuse stage. The incorporation of the hounding behavior of the Feline helps the birdie to escape from the attack leading to the maintenance of the population and helps to explore more regions that assist to obtain the global best solution. Thus, the optimal tuning using the proposed optimization algorithm helps to detect the malware in the network more accurately and hence the preventive mechanism can be employed to avoid the damage.

4. Result and Discussion

The result evaluated by the proposed Feline cad-based DeepCNN is detailed in this section based on the performance metrics such as accuracy, sensitivity, and specificity.

4.1. Experimental Setup

For the evaluation of the proposed malware detection technique, MATLAB is uti-lized with an Intel i3 core processor, 2GB RAM, and Windows 10 OS.

4.2. Dataset description

The Brazilian-malware-dataset [15] comprises of 80GB malicious binary samples with 23,033 unique samples with a total of 29,704 samples. In addition, each sample consists of 27 attributes, in which 3 textual, two unique, and 22 numerical attributes.

4.3. Comparative Methods

The analysis of the proposed method is compared with the traditional malware de-tection techniques such as Neural Network [16], Deep CNN [11], PSO- based DeepCNN [17],CSO-based DeepCNN [13] and Sparrow search based DeepCNN [12].

4.4. Performance metrics

The efficiency of the developed Feline cad-based DeepCNN is evaluated in terms of accuracy, sensitivity and specificity.

Accuracy (A): The measure of the closeness of the target obtained by the proposed method is measured in terms of accuracy and is formulated as,

where, Pos^t represent true positive, $\mathrm{Pos}^f{}_{\text{indicate}}$ false positive, Neg^t indicate true negative, and Neg^f represent false negative.

Sensitivity (S1): The ratio of a positive which correctly detected by the proposed malware detection technique and is expressed as,

$$S_1 = \frac{\mathrm{Pos}^{\,t}}{\mathrm{Pos}^{\,t} + Neg} \tag{10}$$

Specificity ($S2\ :$) :The ratio of negatives that are correctly detected by the proposed malware detection technique and is represented by,

$$S_2 = \frac{Neg^t}{Neg^t + \ \mathrm{Pos}^{\,f}} \tag{11}$$

Table 1
Comparison based on Statistical Analysis

Metrics/ Methods		NN	DeepCNN	PSO based DeepCNN	CSO based DeepCNN	Sparrow search based DeepCNN	Feline cad based DeepCNN
Accuracy (	Best	74.56	85.23	82.54	83.26	85.26	99.95
	Mean	74.56	85.23	82.54	83.26	85.26	99.95
	Variance	0.003	0.0031	0.0029	0.0025	0.003	0.0019
Sensitivity (	Best	78.51	82.17	86.51	86.97	89.25	97.45
	Mean	78.51	82.17	86.51	86.97	89.25	97.45
	Variance	0.0029	0.0027	0.003	0.0032	0.0021	0.0018
Specificity (	Best	79.54	82.56	85.65	87.23	91.15	96.12
	Mean	79.54	82.56	85.65	87.23	91.15	96.12
	Variance	0.0032	0.0027	0.0035	0.0032	0.0028	0.002

4.5. Comparative Analysis

Table 1 depicts the comparative analysis of the proposed Feline cad optimization based DeepCNN with the conventional methods such as NN, Deep CNN, PSO- based DeepCNN, and Sparrow search based DeepCNN. The proposed method obtained the maximal accuracy of 99.95%, which is 25.40%, 14.73%, 17.42%, 16.70%, and 14.70% better than the existing NN, Deep CNN, PSO-based DeepCNN, and Sparrow search based DeepCNN. Likewise, the sensitivity acquired by the proposed method is 97.45%, which is 19.44%, 15.68%, 11.23%, 10.75%, and 8.41% better than the existing NN, Deep CNN, PSO- based DeepCNN, and Sparrow search based DeepCNN. The maximal specificity acquired by the proposed method is 96.12%, which is 17.25%, 14.11%, 10.89%, 9.25%, and 5.17% better than the existing NN, Deep CNN, PSO- based DeepCNN, and Sparrow search based DeepCNN.

5. Conclusion

This research proposed a malware detection technique for the multimedia enabled IoT environment. Here, the data gathered from the IoT environment is extracted based on 27 attributes for the reduction of the computational complexity and is fed to the input for the detection of the malware using the DeepCNN, which is trained using the proposed Feline cad optimization approach that is designed by integrating the forag-ing behavior of the birdie with the hounding behavior of the feline to obtain the glob-al best optimal solution for tuning the weights. The proposed method obtained the maximal accuracy, sensitivity, and specificity and obtained the values of 99.95%, 97.45%, and 96.12% respectively.

References

[1] R. Taheri, R. Javidan, Z. Pooranian, Adversarial android malware detection for mobile multimedia applications in IoT environments, Multimed. Tools Appl. 80 (2021) 16713–16729.

[2] S. Venkatraman, B. Surendiran, Adaptive hybrid intrusion detection system for crowd sourced multimedia internet of things systems, Multimed. Tools Appl. 79 (2020) 3993–4010.

[3] V. Madaan, D. Sethi, P. Agrawal, L. Jain, R. Kaur, Public network security by bluffing the intruders through encryption over encryption using public key cryptography method, in: Advanced Informatics for Computing Research: First International Conference, ICAICR

2017, Jalandhar, India, March 17–18, 2017, Revised Selected Papers, Springer, 2017, pp. 249–257.

[4] N. Mohod, P. Agrawal, V. Madan, Human detection in surveillance video using deep learning approach, in: 2023 6th International Conference on Information Systems and Computer Networks (ISCON), 2023, pp. 1–6. doi:10.1109/ISCON57294.2023.10111951.

[5] A. V. Srinivas, S. S. S. Reddy, A novel approach for excavating communication using taxonomy and outline mechanisms, in: 2021 Sixth International Conference on Image Information Processing (ICIIP), IEEE, 2021.

[6] J. Jeon, J. H. Park, Y.-S. Jeong, Dynamic analysis for IoT malware detection with convolution neural network model, IEEE Access 8 (2020) 96899–96911.

[7] R. Shanker, P. Agrawal, A. Singh, M. W. Bhatt, Framework for identifying network attacks through packet inspection using machine learning, Nonlinear Engineering 12 (2023) 20220297.

[8] R. Shanker, V. Madaan, P. Agrawal, Fss-part: Feature grouping subset model for predicting network attacks, SN Computer Science 5 (2023) 94.

[9] X. Liu, J. Zhang, Y. Lin, H. Li, ATMPA: Attacking machine learning-based malware visualization detection methods via adversarial examples (2018). arXiv:1808.01546.

[10] O. Aslan, M. Ozkan-Okay, D. Gupta, Intelligent behavior-based malware detection system on cloud computing environment, IEEE Access 9 (2021) 83252–83271.

[11] A. Anand, S. Rani, D. Anand, H. M. Aljahdali, D. Kerr, An efficient CNN-based deep learning model to detect malware attacks (CNN-DMA) in 5G-IoT healthcare applications, Sensors (Basel) 21 (2021) 6346.

[12] J. Xue, B. Shen, A novel swarm intelligence optimization approach: sparrow search algorithm, Syst. Sci. Control Eng. 8 (2020) 22–34.

[13] B. Binu D Kariyappa, Rider deep LSTM network for hybrid distance score-based fault prediction in analog circuits, IEEE Transactions on Industrial Electronics (2020).

[14] S. S. S. Reddy, G. Sowmya, V. B. Reddy, B. D. Kumar, A. Kumar, Deep cnn based whale optimization for predicting the rice plant disease in real time, in: International Conference on Artificial Intelligence and Data Science, Springer, 2021, pp. 191–202.

[15] F. Ceschin, F. Pinage, M. Castilho, D. Menotti, L. S. Oliveira, A. Gregio, The need for speed: An analysis of brazilian malware classifiers, IEEE Secur. Priv. 16 (2018) 31–41.

[16] D. Binu, B. Kariyappa, Rider-deep-lstm network for hybrid distance score-based fault prediction in analog circuits, IEEE Transactions on Industrial Electronics 68 (2020) 10097–10106.

[17] H. Bommala, R. Aluvalu, S. Mudrakola, et al., Machine learning job failure analysis and prediction model for the cloud environment, High-Confidence Computing 3 (2023) 100165.