International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 3S, 2025
https://www.theaspd.com/ijes.php

Hybrid Intrusion Detection for Malware Threats in Cloud Computing using Principal Component Analysis and Harris Hawks Optimization

R. Swathi[1], Sivakumar Depuru[2], Anjana Devi Nandam[3], S Sivanantham[4], K. Amala[5], Ch Penchala Vara Prasad[6]
[1,5] Sri Venkateswara College of Engineering, Tirupati, A.P, India
[2,6] School of Computing, Mohan Babu University, Tirupati
[3]Koneru Lakshmaiah Education Foundation, Vaddeswaram
[4]Saveetha School of Engineering, SIMATS, Chennai
siva.depur@gmail.com

Abstract The increasing threats from malware are challenging defensive mechanisms in the continuously evolving world of cloud computing. Malicious malware now poses one of the biggest challenges towards cloud data security. To overcome this, a novel Cloud Malware Intrusion Detection System has been proposed in this paper using a hybrid approach incorporating Harris Hawks Optimization along with Multilayer Perceptron and Principal Component Analysis. This hybrid methodology integrates the capability of PCA for dimensionality reduction so that the extraction of significant features is allowed to occur efficiently, while HHO optimizes hyperparameters for MLP so that accuracy and performance are improved. By leveraging deep learning in order to detect subtle abnormalities indicative of malware threats, the core of a vigilant data monitoring system was found within the cloud architecture as MLP. It has been discovered that the hybrid PCA-HHO-MLP model is an incredibly effective and flexible security mechanism against the constantly changing malware field. According to experimental results, the suggested approach may successfully protect cloud resources while providing exceptional detection performance with accuracy: 98.45% , precision: 98.55% , recall: 99.88% , and F1 Score: 99.21% .

Keywords: Cloud computing, Malware Detection, Harris Hawks Optimization technique, Principal Component Analysis, Multilayer Perceptron.

I. INTRODUCTION

Nowadays, the modern information technology infrastructure consists mostly of cloud computing since it provides scalable resources and reasonably priced services for people and businesses. Large volumes of data—which could include sensitive information including financial records, intellectual property, and personal user data—are stored and processed on cloud platforms by companies even more often. At the same time, this fast adoption of cloud services has increased the attack surface for malicious entities, making security a paramount concern [1].

Malware ranges from ransomware to spyware, trojans, among other types and attacks cloud systems' vulnerabilities with unauthorized access or system disruption through data theft. In a traditional cloud environment, such an interconnectivity presents complications for implementing old security strategies as the speed at which a single attack will move through these networks can prove destructive. More specifically, some traditional defences include firewalls, signature-based antivirus solutions, and static rule sets that prove less effective when fighting adaptive modern cyber threats.

A big problem in finding malware is that harmful programs can change and hide what they're doing. Techniques such as code obfuscation, polymorphism, and metamorphism allow malware to change its structure and execution patterns to avoid detection by signature-based systems [2]. Machine Learning and Deep Learning are widely used by companies to develop much adaptable security solutions since these methods analyze data for new pattern causing threat to security. Yet finding the specific malware type is not detected.

Multilayer Perceptron is a familiar deep learning model which is good at exploring complex realtions in high dimensional data space. However, factors like feature selection and tuning of hyperparameters tuning influence the optimal performance of perceptron. Presence of unnecessary features may reduce the accuracy in the task. In the same way, if the hyper parameter tuning is not proper the model becomes less reliable and takes much time to reach a solution.

These problems are addressed by Principal Component Analysis. PCA reduces data dimension by retaining only key components that hold the major information. Thus, resulting in higher accuracy and model generalization.

The model performance can be enhanced by configuring the number of hidden layers, activation function and learning rate. Hyperparameter optimization has achieved success through the application of metaheuristic algorithms that emulate natural processes. Harris Hawks Optimization (HHO) is a relatively novel metaheuristic inspired by the collaborative hunting strategies of hawks. It provides a harmonic mix of exploration and exploitation, therefore facilitating effective search in high-dimensional parameter domains. Studies have shown that HHO discovers optimal configurations for machine learning models [5] better than conventional optimization methods.

This paper presents a hybrid Cloud Malware Intrusion Detection System comprising PCA for feature selection, HHO for hyperparameter optimization, and an MLP as the fundamental detection engine. By offering a strong, scalable, and flexible security solution, this system is meant to solve the changing scene of cloud-based threats. This paper is arranged mostly as follows: Section II analyzes pertinent work on malware detection and optimization strategies; Section III detailed description of the suggested methodology; Section IV gives experimental data and analysis; Section V summarizes the research with future directions; Section VI includes the references.

II. RELATED WORK

Research into malware detection has changed immensely over the ages, especially with machine learning and deep learning techniques. Early studies relied on signature-based methods that required updates all the time and could not meet the challenge of new threats. These shortcomings led to a natural shift towards behavior-based techniques and anomaly detection systems that are based on finding unusual patterns in system activity.

The proposed hybrid approach integrates Harris Hawks Optimization, PCA and MLP for cloud security. An elaborate review of similar hybrid approaches involving HHO, PCA and other machine learning models is conducted.

A Hybrid intrusion detection system was proposed by Zhou et al., in 2019. Improvisation was made in HHO with multi-information fusion and sine-based escape energy mechanism. The technique was reliable on several datasets like KDD, NSL KDD and UNSWNB15.

In their work, Tiwari and Murugappan integrated Deep learning models with Harris Hawks Optimizer to monitor intrusion detection in house attacks in cloud environments [7]. The model employed stacked autoencoders for optimizing anomaly detection, thus achieving an enhancement in the detection of cyber threats throughout standardized intrusion detection datasets.A Hybrid Harmony Search-Harris Hawks Optimization-based Deep Reinforcement Learning (HSHO-Deep RL) system was developed by Prakash et al. for the purpose of identifying malicious conduct-exploiting IoT networks [8]. The algorithm distinctly optimized feature selection and attained high precision in intrusion detection (96.9%). Kalaiselvi et al. teamed up to propose a hybrid version of Harris Hawks Optimization and feature selection in conjunction with stacked autoencoders and CNN-BiLSTM architectures [9]. The model reached above 99% accuracy, precision, and recall on the NSL-KDD dataset that greatly exemplifies the value of feature selection in heightening detection performance. Sumathi et al. worked on the hybridization of Harris Hawks Optimization and Particle Swarm Optimization (PSO) for hyperparameter tuning on recurrent neural networks [10]. This lifted the role of deep learning models in DDoS attack detection, with a great relief in the number of false positives [22][32][33].

Liu et al. scheduled tasks in cloud computing using an Enhanced Harris Hawks Optimization technique [11] [27]. Reducing task makespan and SLA breaches compared to classical optimization techniques like GA and ACO, the method optimized service-level agreement (SLA) compliance reduces Their hybrid deep learning-based IDS [12] [26] used Principal Component Analysis (PCA). Combining PCA with clustering and deep learning methods effectively lowered data dimensionality, therefore enabling faster training and greater detection accuracy (99.19%). Using HHO-trained artificial neural networks (HHO-ANN), Narendrangbam and Dey presented an anomaly detecting system [13][28]. Across several datasets, the model attained accuracy rates of 98% surpassing existing bio-inspired optimization methods [31].

For blockchain-assisted IoT settings, Katib and Ragab presented a hybrid HHO and sine-cosine-based deep learning system to identify DDoS attacks [14] [25]. With a 99.05% detection accuracy, the system proved how successful it is to use deep learning with HHO in distributed security systems. Manickavasagan et al. [15] optimized cloud resource allocation using an Enhanced Harris Hawks Optimization method. Their method lowered latency, energy use, response times, and system performance [23][24].

Few research have merged PCA, HHO, and deep learning models in a single framework for cloud malware detection notwithstanding these developments. These studies show generally that in cloud computing and IoT systems, combining optimization techniques with deep learning and feature selection greatly improves detection accuracy, resource allocation efficiency, and general performance. This suggested work expands on other studies by suggesting a hybrid PCA-HHO-MLP method that uses the strengths of every component to attain outstanding detection performance [30] [29].

III. PROPOSED METHODOLOGY

Combined in the proposed Cloud Malware Intrusion Detection System three main components: Principal Component Analysis (PCA), Harris Hawks Optimization (HHO), and a Multilayer Perceptron (MLP). The System architecture supports tuning of hyper parameters and detecting anomalies and ensures high reliability and adaptability in malware detection in cloud.

A. Principal Component Analysis (PCA)

A preprocessing method called PCA is used to lower the dataset's dimensionality. Noise and repeated data in high-dimensional data might compromise the performance of machine learning models [16]. PCA finds orthogonal components with maximum variation in the data so allowing the system to concentrate on the most important aspects. This stage improves detection process accuracy as well as computing efficiency.

PCA is applied first by computing the covariance matrix of the input data then eigenvalues and eigenvectors. The data is projected onto the main components, which are chosen depending on their respective eigenvalues, therefore obtaining a reduced feature set. This change not only speeds up model training but also removes pointless features, therefore lowering the overfitting risk.

B. Harris Hawks Optimization (HHO)

Optimizing the hyperparameters of the MLP model falls to the HHO technique. The performance of the model is highly influenced by hyperparameters including the activation functions, learning rate, and number of hidden layers. For complicated, high-dimensional search environments, traditional grid search and random search approaches can be ineffective; hence, metaheuristic optimization strategies become necessary.

HHO behaves cooperatively, much as Harris hawks do. The method dynamically changes its approach depending on the fitness of possible solutions, alternately in exploration and exploitation stages. There are six major phases to the method:

1. Dataset and Features (PCA Application)

Given the malware detection dataset say D, let X be the input data, where:

$$X = \{x_1, x_2, ..., x_n\},\ \ x_i \in R^m$$

Where,

- N-> Number of samples
- M-> Number of features per sample

PCA reduces m features to k significant components, where k<m. The reduction is represented as:

$$X\_reduced = X \cdot P,\ \ P \in R^{mxk}$$

2. Hyperparameter Optimization Problem (Fitness Function)

The major objective of the work is to optimize hyperparameters for the MLP model, which includes:

- H-> Learning rate
- L-> Number of hidden layers
- N-> Number of neurons in each layer

The aim of the optimization is to maximize detection performance using the reduced dataset named $X_{reduced}$. The fitness function based on the F1-score is presented below:

$$Fitness(H) = F1\_score(H) = (2 * Precision * Recall) / (Precision + Recall)$$

3. Exploration Phase (Random Search on Hyperparameters)

In the exploration phase, hyperparameter candidates (hawks) search the hyperparameter space randomly. The update equation is:

$$H\_(t+1) = H\_t + r_1 * (H\_rand - H\_t)$$

Where,

- H_t-> Current hyperparameter candidate
- H_{rand}-> Randomly selected candidate from the population
- r_1-> Random number between 0 and 1

4. Exploitation Phase (Convergence Toward Optimal Parameters)

Once a promising hyperparameter set (prey) is identified, hawks start to converge toward it. The update equation is presented as:

$$H\_(t+1) = H\_prey - \Delta H * |J * (H\_prey - H\_t)|$$

Where,

- H_prey-> Current best hyperparameter candidate
- ΔH-> Adaptive step size

- J-> Random jump strength

5. Adaptive Step Size

The adaptive step size is defined as:

$$\Delta H = 2 * (1 - t / T) * (H\_prey - H\_t)$$

Where,

- T-> Current iteration
- T-> Total number of iterations

6. Final Model Training and Evaluation

Once the hyperparameters are optimized, the MLP is trained on the reduced training dataset. The final evaluation is done as

$$F1\_score = (2 * Precision * Recall) / (Precision + Recall)$$

C. Multilayer Perceptron (MLP)

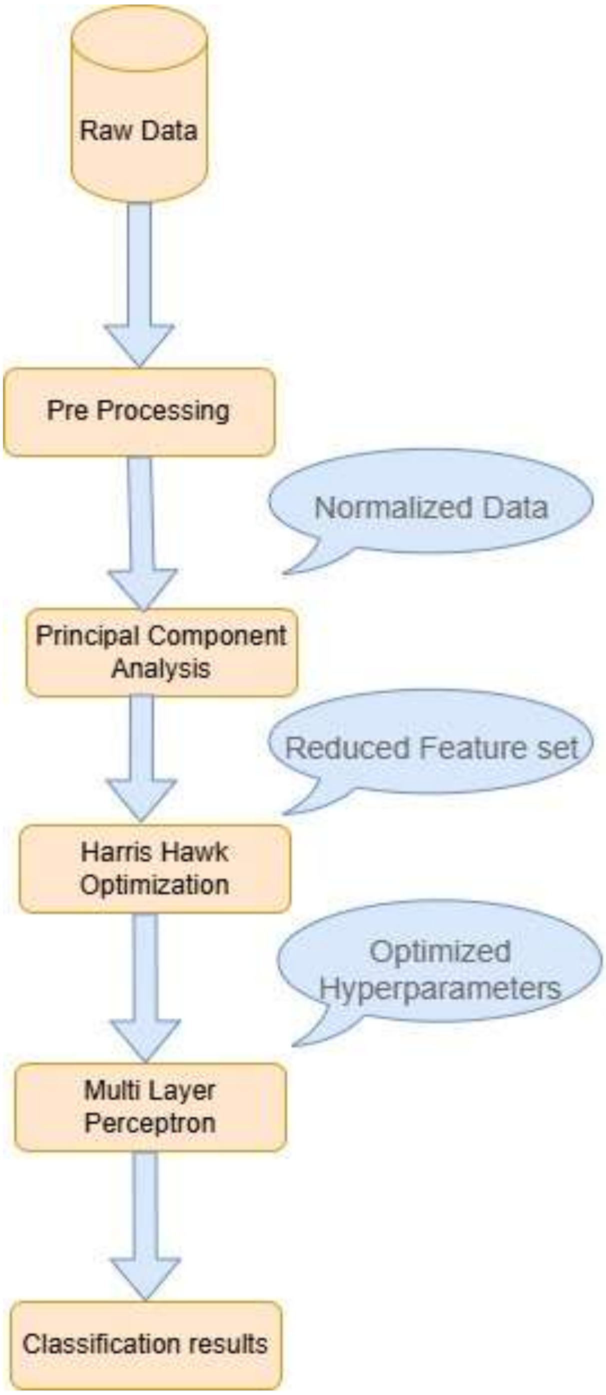
The central detecting engine of the system is the MLP. Comprising an input layer, one or more hidden layer, and an output layer, it is a kind of feedforward neural network. Every layer comprises of linked neurons whereby each one uses a non-linear activation mechanism on weighted inputs [18, 17].

Using backpropagation and gradient descent, the MLP learns to classify input data by minimizing a loss function, say cross-entropy, in the training phase. The hyperparameters tuned by HHO improve the generalizing capacity of the model by means of neurons, learning rate, activation functions, and other aspects. The ideal MLP can identify minute trends suggestive of malware activity, hence facilitating real-time intrusion detection.

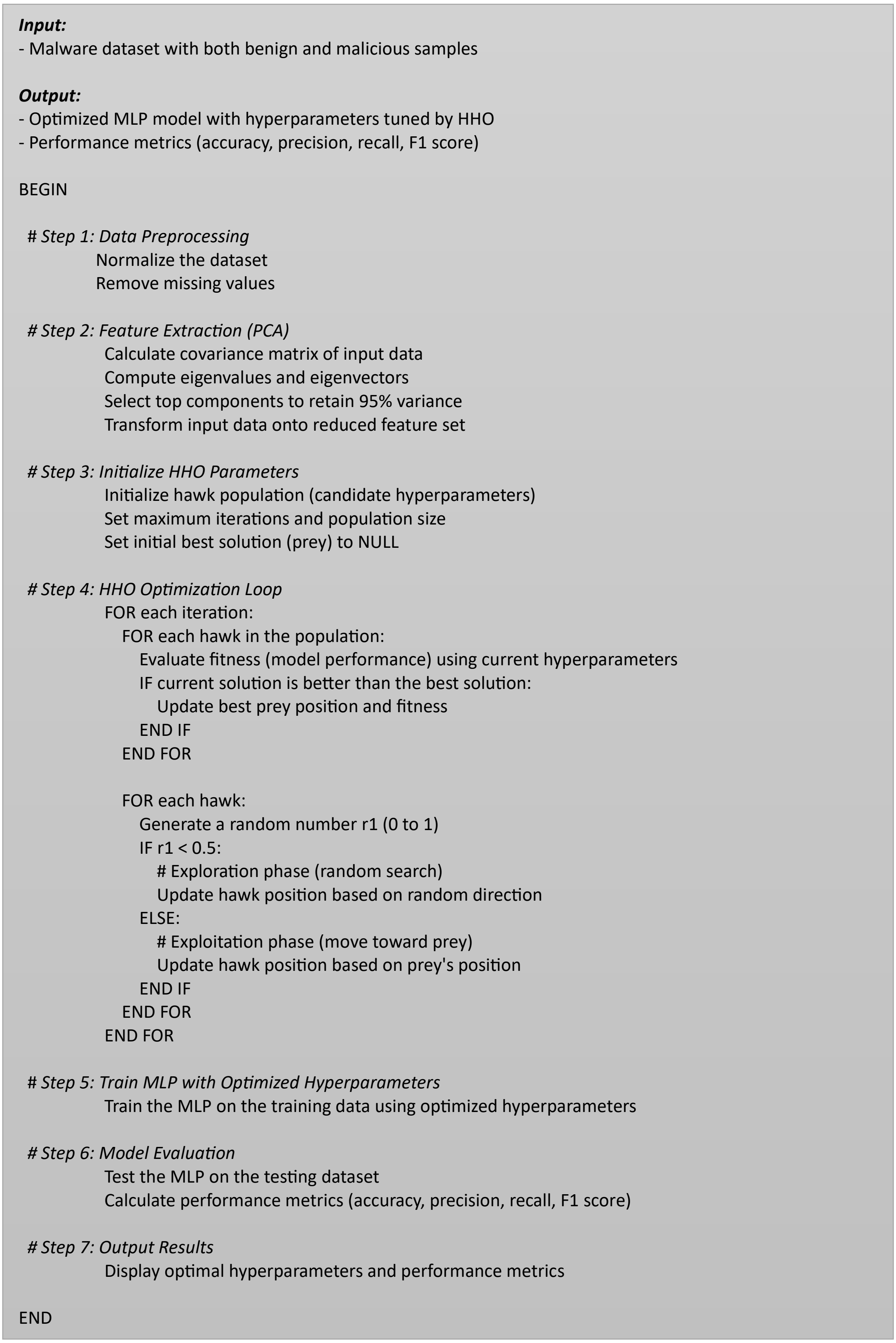
D. System Workflow

Figure 1 shows the suggested system's whole working flow. The method starts with PCA feature extraction in preprocessing of input data. The MLP, which the HHO technique has optimized, receives the smaller feature set next. The technology tracks cloud resources constantly for irregularities and sends real-time alerts upon possible hazards.

Figure 1: The proposed model



A simple algorithm for Hybrid PCA-HHO-MLP based Intrusion Detection System shall be presented as below,



```
Input:
- Malware dataset with both benign and malicious samples

Output:
- Optimized MLP model with hyperparameters tuned by HHO
- Performance metrics (accuracy, precision, recall, F1 score)

BEGIN

 # Step 1: Data Preprocessing
         Normalize the dataset
         Remove missing values

 # Step 2: Feature Extraction (PCA)
          Calculate covariance matrix of input data
          Compute eigenvalues and eigenvectors
          Select top components to retain 95% variance
          Transform input data onto reduced feature set

 # Step 3: Initialize HHO Parameters
          Initialize hawk population (candidate hyperparameters)
          Set maximum iterations and population size
          Set initial best solution (prey) to NULL

 # Step 4: HHO Optimization Loop
          FOR each iteration:
            FOR each hawk in the population:
              Evaluate fitness (model performance) using current hyperparameters
              IF current solution is better than the best solution:
                Update best prey position and fitness
              END IF
            END FOR

            FOR each hawk:
              Generate a random number r1 (0 to 1)
              IF r1 < 0.5:
                # Exploration phase (random search)
                Update hawk position based on random direction
              ELSE:
                # Exploitation phase (move toward prey)
                Update hawk position based on prey's position
              END IF
            END FOR
          END FOR

 # Step 5: Train MLP with Optimized Hyperparameters
          Train the MLP on the training data using optimized hyperparameters

 # Step 6: Model Evaluation
          Test the MLP on the testing dataset
          Calculate performance metrics (accuracy, precision, recall, F1 score)

 # Step 7: Output Results
          Display optimal hyperparameters and performance metrics

END
```

The suggested approach is fit for dynamic cloud environments since it balances computational economy, accuracy, and adaptability by including PCA, HHO, and MLP.

IV. Experimental Results

A. Experimental Setup

Using the CICIDS2017 malware dataset, a well-known benchmark dataset used for intrusion detection system evaluation, the proposed Cloud Malware Intrusion Detection System was experimentally evaluated. Collected from many cloud applications and services, the collection consists of benign as well as malicious samples.The data was standardized and missing value-free cleansed to ensure consistency [19]. Subsets of training (70%), and testing (30%), made up the dataset. PCA was applied on the training data to find the most relevant features after a threshold selected to retain 95% of the total variance [20].

The hyperparameters of the MLP were optimized using the HHO method including activation functions (ReLU and sigmoid), learning rate (between 0.001 and 0.01), and hidden layer count ranging from 1 to 5.Python was used for implementation; TensorFlow and Scikit-learn tools for model training and evaluation.

B. Evaluation Metrics

Following evaluation criteria were applied to evaluate the suggested system:

i. Accuracy: Out of all the samples, what percentage of correctly categorized ones?

ii. Precision: The proportion of real positive detections to the total positive predictions.

iii. Recall: The ratio of genuine positive detections to the total actual positive cases.

iv. F1 Score: The harmonic mean of accuracy and recall.

The above measures have been considered for a thorough evaluation of the proposed system's performance in terms of dependability and efficiency.

C. State of art Methods

To evaluate the effectiveness of the hybrid PCA-HHO-MLP approach, comparisons were made with several baseline methods commonly used for malware detection:

1. **Random Forest (RF)**: The most familiar ensemble learning technique known for its robustness particularly in solving classification problems.
2. **Support Vector Machine (SVM)**: A commonly used hyperplane-based algorithm that separates data using support vectors in high dimensional space.
3. **Deep Neural Network (DNN)**: A multilayer neural network model similar to the MLP. Optimization of hyperparameters and feature reduction are not available in built [21].

D. Results and Comparison

Table 1 summarizes the comparative analysis of the experimental results obtained for the baseline methods and the proposed work. The hybrid PCA-HHO-MLP system demonstrated superior performance in all key metrics.

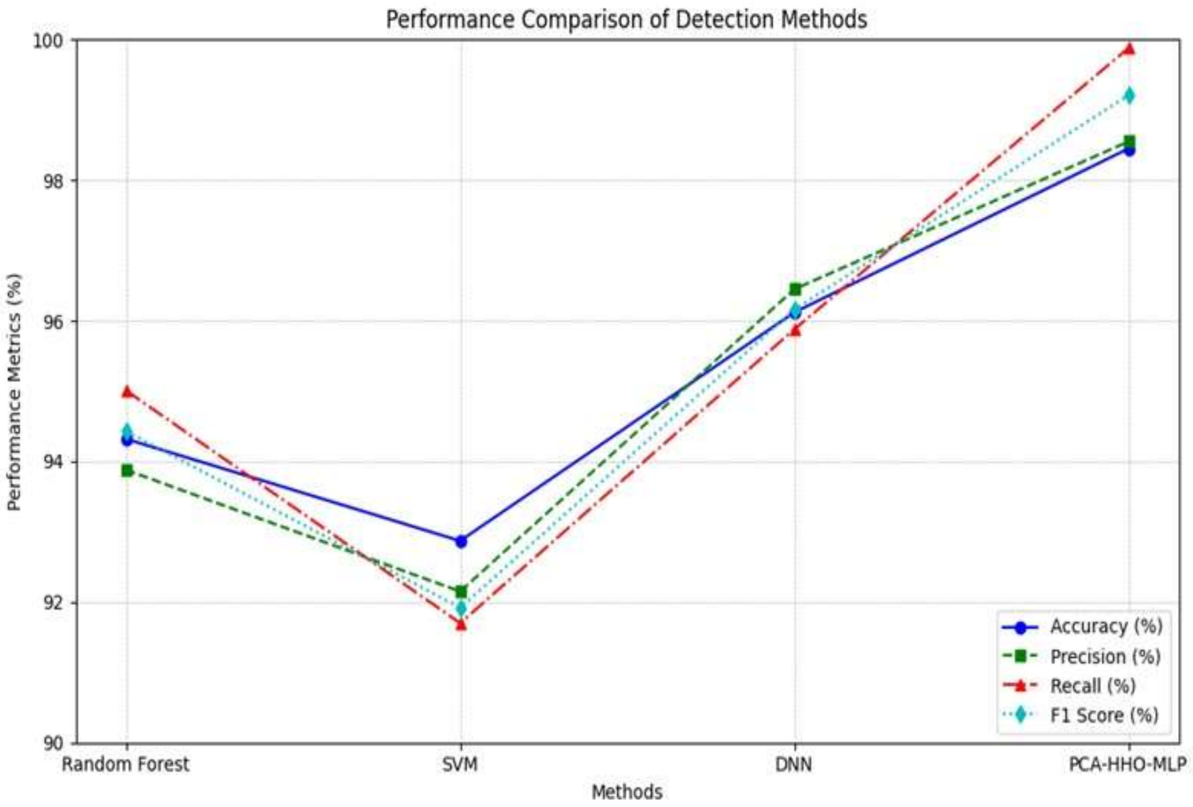
Table 1: Comparison of Performance Metrics

Method	**Acc** (%)	**Precision** (%)	**Recall** (%)	**F1 Score** (%)

RF	94.32	93.88	95.01	94.43
SVM	92.87	92.15	91.70	91.92
DNN	96.12	96.45	95.88	96.16
PCA-HHO-MLP	98.45	98.55	99.88	99.21

The results indicate that the integration of PCA for feature selection and HHO for hyperparameter optimization enhances both the accuracy and efficiency of the MLP model as shown in figure 2.

Figure 2: Performance comparison graph



Furthermore, the system's high recall value demonstrates its ability to detect most malicious samples without missing significant threats. Comparative study of several malware and intrusion detection systems in cloud environments shows that conventional methods suffer with scalability, real-time adaptation, and thorough performance throughout several scenarios. Although many research lack quantitative results or use out-of-date information, techniques including machine learning, deep learning, and optimization methods have showed promise in improving detecting capability.

Table 2: State of Art Work comparison

Authors	Paper Title	Approach used	Dataset	Key Performance	Pros	Cons
S. Gupta, P. Kumar	System cum Program-Wide Lightweight Malicious Program Execution Detection	System call structure-based anomaly detection in cloud	UNM Sendmail dataset	Effective program-level and system-level detection	Combines system- and program-level anomaly detection	Older dataset used; limited relevance to modern attacks
P. Mishra, E. Pilli, V. Varadharajan, U. Tupakula	Efficient approaches for intrusion detection in cloud environment	Machine learning with parallelization for improved detection speed	Custom framework and analysis	Improved detection speed and security frameworks	Focuses on speed and parallelization for faster detection	Results not generalized beyond the proposed framework
R. Ahmadi, R. Macredie, A. Tucker	Intrusion Detection Using Transfer Learning in Machine Learning Classifiers	Transfer learning between cloud and non-cloud datasets	KDDCup99, cloud-specific dataset	Accurate detection across cloud and non-cloud environments	Utilizes transfer learning for cross-environment detection	Limited dataset compatibility for transfer learning
R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, S. Venkatraman	Deep Learning Approach for Intelligent Intrusion Detection System	Deep neural networks for scalable intrusion detection	KDDCup99, NSL-KDD, CICIDS 2017	Accurate detection and low false-positive rates	High scalability and accurate detection with deep learning	Focus on static datasets; limited real-time testing
A. R. Melvin, G. Kathrine, J. I. Johnraja	The Practicality of Using Virtual Machine Introspection Technique	Virtual Machine Introspection with C4.5 and ML algorithms	Custom dataset with VMI behavior data	Detection accuracy of up to 93%	Achieves high accuracy using Virtual Machine Introspection	Limited to a specific dataset; lacks scalability tests
D. Praveena, G. Kamalesh, T. Kamalesh, D. Lokesh	A Review of Machine Learning Methodologies for Malware Detection	Review of ML algorithms in cloud malware detection	Various public datasets for malware	Insights for developing effective ML-based IDS	Provides an extensive survey of ML techniques for cloud security	No direct implementation details or metrics provided

P. Wasnik, N. Chavhan	A Review Paper on Designing Intelligent Intrusion Detection System	Deep learning with hyperparameter optimization on IDS data	KDDCup99, NSL-KDD, UNSW-NB15	Flexible intrusion detection with unsupervised learning	Applies flexible deep learning for evolving threats	Performance metrics are not provided for comparison
S. Sharma	Advancements in Machine Learning for Intrusion Detection in Cloud Environments	Machine learning techniques, ensemble learning, threat intelligence	Real-world case studies (cloud data)	Enhanced detection accuracy with reduced false positives	Improved intrusion detection with adaptive learning techniques	No detailed quantitative results provided
M. U. Abdullahi, M. A. Onawo, B. A. Ajayi, K. T. Anyachebelu, A. Suleiman	Analysis of intrusion detection system in cloud computing using artificial neural network	ANN-based IDS using adaptive architecture and TensorFlow	University of New Brunswick dataset	91.7% training accuracy and low false-positive rates	Achieves near-perfect accuracy with ANN and adaptive architecture	Dataset may require regular updates; limited scope on evolving threats
V. Gazeau, K. Gupta, M. K. An	Advancements of Machine Learning in Malware and Intrusion Detections	AI-driven intrusion and malware detection using ML methods	Malware datasets (varied sources)	High accuracy and adaptability to evolving threats	Highlights advancements in AI-based malware detection	No precise performance metrics mentioned
Proposed Work PCA-HHO-MLP	Hybrid Intrusion Detection for Malware Threats in Cloud Computing Using PCA and HHO	Hybrid PCA for feature extraction, HHO for hyperparameter optimization, and MLP for detection	CICIDS2017 (malware dataset)	Achieved 98.45% accuracy, 98.55% precision, 99.88% recall, and 99.21% F1 score	Integrates PCA, HHO, and MLP to achieve robust performance	Requires computational resources for optimization and training

With extraordinary performance metrics—98.45% accuracy, 98.55% precision, 99.88% recall, and 99.21% F1 score—our suggested hybrid system integrates Principal Component Analysis (PCA) for feature selection, Harris Hawks Optimization (HHO) for hyperparameter tuning, and a Multilayer Perceptron (MLP) for anomaly detection. This approach provides a strong and scalable protection against developing cloud-based malware threats, so effectively balancing computing efficiency, detection accuracy, and flexibility, so defining a new benchmark for intrusion detection systems.

V. Conclusion

The research paper introduces a hybrid Cloud Malware Intrusion Detection System using Principal Component Analysis, Harris Hawks Optimization, and a Multilayer Perceptron. Through the combination of these methods, the proposed system introduces an effective and adaptive solution to the issues brought about by dynamic malware threats in cloud computing. Experimental results validate that the system provides high detection accuracy, precision, recall, and F1 scores, thus making it a promising tool for cloud resource security.

The research work can be extended to investigate the performance od hybrid systems by combining the other optimization algorithms and feature extraction techniques to improve attack detection performance. In addition, the incorporation of real-time monitoring features and scalability enhancements will also be investigated in future work.

REFERENCES

1. S. Sharma, "Advancements in Machine Learning for Intrusion Detection in Cloud Environments," *International Journal of Scientific Research in Engineering and Management*, 2023.
2. R. Melvin, G. Kathrine, and J. I. Johnraja, "The Practicality of Using Virtual Machine Introspection Technique with Machine Learning Algorithms for the Detection of Intrusions in Cloud," 2021.
3. P. Mishra, E. Pilli, V. Varadharajan, and U. Tupakula, "Efficient approaches for intrusion detection in cloud environment," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, pp. 1211-1216, 2016.
4. V. Gazeau, K. Gupta, and M. K. An, "Advancements of Machine Learning in Malware and Intrusion Detections," in *2024 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1-7, 2024.
5. R. Ahmadi, R. Macredie, and A. Tucker, "Intrusion Detection Using Transfer Learning in Machine Learning Classifiers Between Non-cloud and Cloud Datasets," in *Lecture Notes in Computer Science*, pp. 556-566, 2018.
6. P. Zhou, H. Zhang, and W. Liang, "Research on hybrid intrusion detection based on improved Harris Hawk optimization algorithm," *Connection Science*, vol. 35, 2023.
7. R. Tiwari and S. Murugappan, "Enhancing Security in Cloud Computing Using Harris Hawks Optimizer with Deep Learning for Intrusion Detection," in *2023 Int. Conf. Sustainable Communication Networks and Application (ICSCNA)*, pp. 170-175, 2023.
8. P. G. O. Prakash, B. Maram, and G. Nalinipriya, "Harmony search Hawks optimization-based Deep reinforcement learning for intrusion detection in IoT," *Int. J. Wavelets Multiresolution Inf. Process.*, vol. 19, 2021.
9. B. Kalaiselvi, S. Gogul, S. Siva, R. Dhineshkumar, and M. Logeshwaran, "Enhanced Intrusion Detection System Using Hybrid Harris Hawks Inspired Feature Selection," in *2024 Int. Conf. Computing and Data Science (ICCDS)*, pp. 1-6, 2024.
10. S. Sumathi, R. Rajesh, and S.-K. Lim, "Recurrent and Deep Learning Neural Network Models for DDoS Attack Detection," *Journal of Sensors*, 2022.
11. J. Liu, C. Lei, and G. Yin, "Enhanced Harris Hawks Optimization Algorithm for SLA-Aware Task Scheduling in Cloud Computing," *Int. J. Adv. Comput. Sci. Appl.*, 2024.
12. K. Prabu and P. Sudhakar, "A hybrid deep learning approach for enhanced network intrusion detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 33, 2024.
13. L. Narengbam and S. Dey, "Harris hawk optimization trained artificial neural network for anomaly-based intrusion detection system," *Concurrency and Computation: Practice and Experience*, vol. 35, 2023.
14. Katib and M. Ragab, "Blockchain-Assisted Hybrid Harris Hawks Optimization Based Deep DDoS Attack Detection in the IoT Environment," Mathematics, 2023.
15. V. Manickavasagan, E. Petchiammal, and S. R. Sudha, "Enhancing Cloud Resource Allocation Efficiency with Harris Hawk Optimization Algorithm," in *2024 IEEE Int. Students' Conf. Electrical, Electronics and Computer Science (SCEECS)*, 2024.
16. S. Gupta and P. Kumar, "System cum Program-Wide Lightweight Malicious Program Execution Detection Scheme for Cloud," *Information Security Journal: A Global Perspective*, vol. 23, pp. 86-99, 2014.
17. S. Depuru, P. Hari, P. Suhaas, S. R. Basha, R. Girish and P. K. Raju, "A Machine Learning based Malware Classification Framework," *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, Tirunelveli, India, 2023, pp. 1138-1143, doi: 10.1109/ICSSIT55814.2023.10060914.

18. R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," *IEEE Access*, vol. 7, pp. 41525-41550, 2019.
19. D. Praveena, G. Kamalesh, T. Kamalesh, and D. Lokesh, "A Review of Machine Learning Methodologies for Malware Detection in Cloud Infrastructure," 2021.
20. P. Wasnik and N. Chavhan, "A Review Paper on Designing Intelligent Intrusion Detection System Using Deep Learning," in *2023 11th International Conference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP)*, pp. 1-6, 2023.
21. M. U. Abdullahi, M. A. Onawo, B. A. Ajayi, K. T. Anyachebelu, and A. Suleiman, "Analysis of intrusion detection system in cloud computing environment using artificial neural network," *World Journal of Advanced Research and Reviews*, vol. 19, pp. 1-10, 2023.
22. Usharani, S., Lakshmanan, R., Rajakumaran, G., Basu, A., Nandam, A., & Depuru, S. (2025). Detection of location-specific intra-cranial brain tumors. *IAES International Journal of Artificial Intelligence (IJ-AI), 14*(1), 428-438. doi: http://doi.org/10.11591/ijai.v14.i1.pp428-438
23. Depuru, N. S. (2024). Enhancing flight delay prediction and classification using a hybrid Bi-LSTM: machine learning. Deleted Journal, 31(6s), 440–451. https://doi.org/10.52783/cana.v31.1235
24. Dr. Srinivasa Babu Kasturi, Sreedhar Burada, Dr. Sowmyashree M.S, Sharath.S, Dr. M.Sunil Kumar,Dr. D. Ganesh, "An Improved Mathematical Model by Applying Machine Learning Algorithms for Identifying Various Medicinal Plants and Raw Materials", Communications on Applied Nonlinear Analysis ISSN: 1074-133X ,Vol 31 No. 6s 2024.
25. B. Sangamithra, Asha K.H, M. Sunil Kumar,""An Improved Information Retrieval System using Hybrid RNN LSTM for Multiple Search Engines", Communications on Applied Nonlinear Analysis ISSN: 1074-133X ,Vol 31 No. 5s 2024.
26. Sreedhar Burada,B.E. Manjunathswamy, M. Sunil Kumar, "Early detection of melanoma skin cancer: A hybrid approach using fuzzy C-means clustering and differential evolution-based convolutional neural network",Measurement: Sensors, Volume 33, June 2024, 101168.
27. M. Sunil KumarJ KumarnathSachin S PundMansing Rathod,""A Secure IoT Smart Network Model for the Contributory Broadcast Encryption for the Text Policy Management Scheme", international Journal of Intelligent Systems and Applications in Engineering IJISAE, 2023, 11(3s), 42–48 2023.
28. Hari Prasad Gandikota ,Abirami. S,Sunil Kumar M, "PLoS ONE 18(11): e0292785. https://doi.org/10.1371/journal.pone.0292785.
29. Hari Prasad Gandikota* | S. Abirami M. Sunil Kumar,""Bottleneck Feature-Based U-Net for Automated Detection and Segmentation of Gastrointestinal Tract Tumors from CT Scans",Traitement du Signal, Vol. 40, No. 6, December, 2023, pp. 2789-2797.
30. Burada, S., Manjunathswamy, B.E. & Kumar, M.S. Deep ensemble model for skin cancer classification with improved feature set. Multimed Tools Appl 84, 7599–7626 (2025). https://doi.org/10.1007/s11042-024-19039-5.
31. E.Ramesh Babu, Dr.M.Sunil Kumar,"The Role of Optimization Techniques in Advancing Big Data Analytics : A Survey", Communications on Applied Nonlinear Analysis ISSN: 1074-133X Vol 32 No. 1s 2025.
32. Meriga Kiran Kumar, Rajeev Kudari, C. Sushama, M. Sunil Kumar, P. Neelima, D. Ganesh, "Efficient Algorithms for Vehicle Plate Detection in Dynamic Environments", Communications on Applied Nonlinear Analysis ISSN: 1074-133X Vol. 32 No. 1s 2025 .
33. Rayavarapu Veeranjaneyulu, V. Sumathi, C. Sushama, Savanam Chandra Sekhar, P. Neelima, M. Sunil Kumar, "Predicting Disasters: A Machine Learning Approach", Communications on Applied Nonlinear Analysis ISSN: 1074-133X Vol. 32 No. 1s 2025.