International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Improved Harris Hawks Optimization Algorithm for Malware Intrusion Detection in Cloud Storage

Manjushree C. V.*[1], Nandakumar A. N.[2]

Submitted: 06/12/2023 **Revised**: 17/01/2024 **Accepted**: 27/01/2024

Abstract: Defending against malware threats has become a crucial concern in the continually evolving realm of cloud computing. Creative malware has become a rising challenge to cloud data security. Hence, we have proposed a methodology for Cloud Malware Intrusion Detection to strengthen cloud infrastructures against the constant threat of unknown malware attacks. Harris Hawks Optimization (HHO) and the Multilayer Perceptron (MLP) are proposed as a hybrid approach to tackling malware attacks in the cloud using deep learning to detect subtle abnormalities as an indicative solution to identify hidden malware threats. Hence, the MLP model provides part of a vigilant data monitoring system inside the cloud architecture. By modifying the MLP's hyperparameters, HHO serves as an optimization engine, enhancing the MLP's accuracy and efficiency. This hybrid approach has the capacity to safeguard cloud resources against the constantly changing and threatening landscape of malware, which provides an efficient and adaptive defense system, as proved by the implementation process. Accuracy of 98.45%, precision of 98.55%, recall of 99.88%, and F1 Score of 99.21% have been achieved during the experimentation.

Keywords: *Cloud Data Security, Malware Intrusion Detection, Multilayer Perceptron Model, Harris Hawks Optimization, Unknown Malware Attacks.*

1. Introduction

Malware invasions are one of the most hazardous risks that cloud systems have to deal with. Malicious software attacks can severely compromise system functionality and data integrity, endangering both individuals and companies. Cyber-related attacks [1] on the global economy have been rising rapidly in recent years. Researchers estimate that more than a million malicious software files are now produced daily, and the expense of malware attacks, particularly for critical systems and cyber-physical systems (CPS), is also increasing. According to a McAfee analysis, the number of backdoors, financial Trojans, and fraudulent mobile applications has increased significantly. Ensuring the security of cloud assets and preserving confidence in cloud services requires prompt detection and mitigation of these threats.

Malware [2,3,4,5] is any program, including viruses, worms, rootkits, backdoors, and ransomware, that carries out harmful operations on a victim's computer with or without the system owner's knowledge. There have been various alternative methods, both conventional and cutting-edge, proposed for detecting malware. Traditional methods, such as signature-based, heuristic-based, behavior-based, and model-checking-based detecting approaches, have been employed for more than ten years. Advanced methods are based on a variety of methodologies, such as deep learning, edge computing, cloud computing, and machine learning. It is commonly known that the signature-based detection strategy works well with respect to time and memory utilization but fails to catch malware that is not known to it. Table 1 lists the types of malware attacks mitigated by various research.

1.1. Malware Detection Model

Fig. 1 depicts the fundamental architecture of the Cloud-based malware detection model. On a cloud computing system, it has two sides: a client and a server. The client uploads a suspicious file online, and the server runs an analysis and determines if the suspicious file is malware or not. To enhance performance, the server employs a variety of detection agents during the analytic process. Strings, static and dynamic features, system calls, API traces, hybrid features, and application traces are all employed throughout the feature extraction process. According to recent research, cloud-based detection methods improve malware detection rates for both known and undiscovered threats and offer a more in-depth analysis of every malware sample.

[1] *Vemana Institute of Technology (VTU), Bangalore, India*
ORCID ID : 0000-3343-7165-777X
[2] *VTU/City Engineering College, Bangalore, India*
ORCID ID : 0000-3343-7165-777X
** Corresponding Author Email: manjushreecv3@gmail.com, drnandakumarcity@gmail.com*

Table 1. Types of attacks concentrated by various researchers

Study Reference	Types of Attacks
Mazin et al. [6]	Worms
Liu et al. [7]	Anti-malicious attack
Ping et al. [8]	Replay attacks, replacing attacks, forgery attacks
Susilo et al. [9]	Security Attacks
Aslan et al. [10]	IOT, DoS Attacks
Aljumah et al. [11]	Man in the middle (MITM), DoS attacks
Vellela et al. [12]	DoS attacks
George et al. [13]	Cyber attacks
Pramila et al. [14]	Virus, Malicious Attack
Pronika et al. [15]	Cyber attacks
Binod et al. [16]	Malicious, cyber attack
Ravi et al. [17]	Malicious attacks
Carlos et al. [18]	Permission abuse attacks
Song et al. [19]	negligence, malicious attack
Deyannis et al. [20]	Cyber attacks

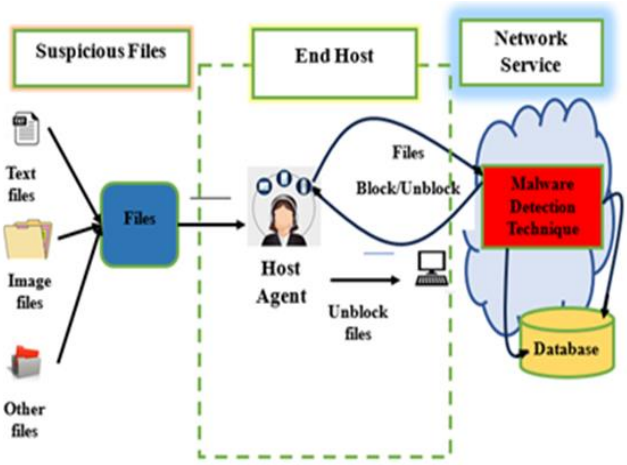

Fig. 1. Cloud Malware Intrusion Detection

1.2. Contributions of the Proposed Work

The contributions of the work are as follows:

- A new hybrid approach of swarm intelligence-based optimization and deep learning approach has been proposed for malware intrusion detection.
- An improved Harris Hawks Optimization approach has been proposed that could recognize malware.
- A new approach to detect unknown or future-created malware is suggested using the combination of the MLP model with the Harris Hawk Optimization technique.

1.3. Organization of the paper

The rest of this paper is organized as follows: In section 2, the related study for insider threat detection framework is discussed. In Section 3, a methodology is proposed that detects malware threats in cloud environments. Section 4 reports the experimental results and observations. Section 5 concludes the paper.

2. Literature Review

The review of the literature identifies several effective detection techniques and strategies designed to defend cloud resources from various threats, such as malware incursions, in order to enhance cloud security.

In 2020, Xianwei Gao *et al.* [21] suggested a novel malware detection system that includes detection, prediction, and transfer components for the cloud that is centered on semi-supervised transfer learning (SSTL). A byte classifier with its detection component built around a recurrent neural network (RNN) was created to identify malware in order to safeguard the confidentiality of users in the public cloud. In 2021, Zahid *et al.* [22] established a scalable multiagent system framework utilizing an approach to guarantee sharing of data on publicly accessible cloud storage and dependability. This work suggested using a cloud host to act as a middleman among the user as well as authorized participants while maintaining the privacy and security of the system. By using the state-of-the-art Gemini approach's very effective power, they have additionally suggested a revolutionary methodology for safeguarding the cloud from malware.

In 2021, Omer *et al.* [23] suggested a cloud environment-based intelligent behavior-based detection method. In order to distinguish between malware and benign samples, the recommended approach first generated a malware dataset on several virtual machines that efficiently identifies distinctive properties. In 2021, Preeti *et al.* [24] suggested an introspection-based security method called *VM Shield* for protecting virtual areas in a cloud-based service system that was made to find malware in cloud architecture.

In 2022, Vinay *et al.* [25] created a system where the most effective classifiers from them were going to be used to gather the best features and apply them, and machine learning techniques would be employed to identify the best features through data set provided by the author and offer an accuracy report. In 2021, Ikram *et al.* [26] suggested and tested a malware classifier that could place each piece of malware into the appropriate group. The author did this by combining a malware visualization method with the multi-

layer perceptron (MLP) method. In 2020, Do Hoang Long *et al*. [27] developed a technique for employing machine learning to recognize harmful indicators based on their atypical behavior. Therefore, in this study, the author would carry out harmful analysis employing static and dynamic analysis techniques to detect aberrant behaviors and integrate them with an MLP to get an idea on malware behavior.

In 2020, Abdulrahman *et al*. [28] presented two-classification models for reliable intrusion detection systems (IDS). The initial model builds a distributed denial of service (DDoS)-based artificial neural network (ANN). In 2023, Sidra Abbas *et al*. [29] offered a machine-learning as well as deep-learning-based method for building an efficient model for the IoMT system to categorize and foresee unforeseeable cyber-attacks/threats. Prior to choosing the optimum feature, the dataset was effectively preprocessed using the Harris Hawk Optimization (HHO) method.

In 2023, Shtwai Alsubai *et al*. [30] designed to create a foundation for malware detection using images. Malware files were transformed into RGB images by the researchers using image conversion as well as enhancement methods.

2.1. Motivation of the Proposed Work

The methodology that has been stated, which combines the Multilayer Perceptron (MLP) with Harris Hawks Optimization (HHO), corresponds with the patterns identified in the literature. An aggressive and flexible strategy toward intrusion detection is required for the continual evolution of cloud malware threats. This methodology is an effective strategy that may improve the cloud's defenses against the constant threat of malware invasions and tie in with the altering cloud security landscape.

2.2. Objective of the Proposed Work

The proposed research aims to complete the research gaps and the objectives of the research work are listed below:

- To develop an optimization approach for detecting unknown threats in a cloud environment.
- To implement the work in a deep learning-based platform.
- To propose an effective detection approach that provides improved accuracy, performance, recall, and F1-score.

3. Proposed Methodology

3.1. Overview

In order to protect cloud environments from malicious software attacks, a sturdy and efficient methodology is required to address

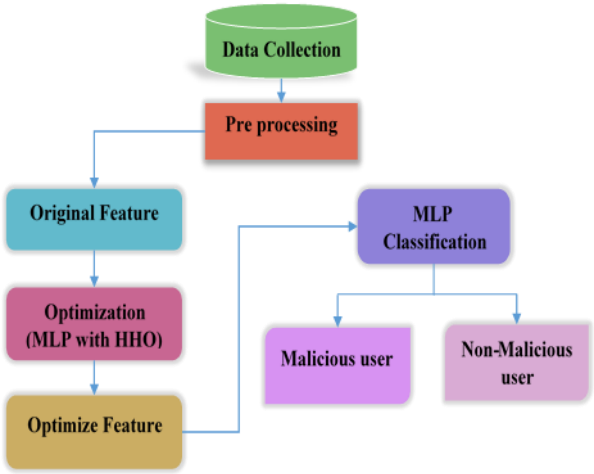

Fig. 2. Cloud Malware Detection with Integrated MLP and HHO Optimization

the vital concern of Cloud Malware Intrusion Detection. By integrating sophisticated methods like Multilayer Perceptron (MLP) and Harris Hawks Optimization (HHO) in a cohesive way, the proposed approach could offer a strong and unique strategy that effectively detects malware threats in cloud environments.

HHO acts as an optimization engine, systematically exploring the vast hyper parameter space of the MLP model. HHO can identify the most effective configurations, which improves the data leak detection system's accuracy and overall performance. HHO intervenes to modify the MLP model's setting and parameters since it is renowned for its ability to optimize complex structures. HHO determines the best potential combination to optimize the model's ability to detect malware intrusions by methodically experimenting with various hyperparameters, including the number of hidden layers, neurons matter, and training rates. By implementing this process, the malware intrusion detection system is ensured to be able to detect new threats and proficient in reducing false positives, thereby offering a strong detection mechanism for the cloud environment.

Fig. 2 shows how the data is pre-processed before feature extraction and is transferred to the optimization process, which yields the optimized features. The two stages of the optimization process are called HHO and MLP, respectively. These two enable the optimized feature to be obtained. The optimized feature is then processed using MLP to categorize users as malicious or benign.

3.2. Optimizing MLP with HHO

The combination of deep learning and optimization features in Cloud Malware Intrusion Detection through MLP and HHO integration provides a highly accurate, flexible, and effective system for detecting and containing malware attacks in cloud environments. An effective defense system against changing cloud security threats is provided by this integrated strategy.

3.2.1. Exploration

Equation (1) illustrates how the two approaches are applied in the search space to imitate the exploration performance of the Harris Hawk.

$$Y(a+1)= \begin{cases} \{Y_{rand}(a)\} - r_1|Y_{rand}(a) - 2r_2Y(a)| & b \geq 0.5\ rule \\ \{Y_{user}(a)\} - |Y_n(a) - r_2(LB + r_4(UB - LB))| & b < 0.5\ rule \end{cases} \quad (1)$$

Where,

Y (a + 1) - Hawk's position in the next iteration of a,

a - Iteration,

Y_{user} - Position of prey,

$Y_{rand}(a)$ - Selection of random solution in the current population,

Y(a) - Hawk's position vector in the current iteration a,

$r1$, $r2$, $r3$, $r4$, and b - Random scaled factor within range of [0, 1] (updated in every iteration),

LB - Lower bound of variables,

UB - Upper bound of variables,

Yn - Solution's average number.

Variety of techniques are provided by exploring different areas of the feature space considering the random scaled component. Based on the average position of solutions, (2) is obtained.

$$Y_n(a) = \frac{1}{M} \sum_{i=1}^{M} Y_i(a) \quad (2)$$

$Y_n(a)$ - Coordinate average of solutions in the current iteration,

M - Whole possible solutions,

$Y_i(a)$ - Location of each solution in iteration a.

3.2.2. Shifting Exploration to Utilization

This stage (3) describes the shift in the Harris Hawk's optimization from exploration to exploitation based on the energy (E) of the user. The HHO takes into account the prey's decreasing energy as a result of the dissipate patterns.

$$E = 2E_0\ (1 - a/\ A),\ E_0 \in [-1,1] \quad (3)$$

Where,

A - Overall iterations,

a - Current iteration.

By employing these tactics, HHO mimics the hawks' attacking approach of fetching the prey as given in (4). These tactics are implemented in accordance with the position, which is determined during the exploratory phase.

$$\begin{gathered} Y\ (a+1) = \Delta Y(a) - E\ |\ Y_{user} - Y(a) \\ \Delta Y(a) = Y_{user} - Y(a) \\ k = 2(1 - r_s),\ r_s \in [0,1] \end{gathered} \quad (4)$$

Where,

k - Prey's jump power,

r_s - Random variables,

Y (a + 1) - Hawk's position in the next iteration of a.

Y(a) - Hawk's position vector in the current iteration a,

E - Energy of prey,

ΔY(a) - Variations between the prey's position vector and current location in iteration a.

Here, the user's energy becomes depleted and exhausted as a result of the mild besiege; the variables' values are $|E| < 0.5$ and ≥ 0.5. We can deduce this event to (5). In the event of a severe besiege, the overall vectors are displayed. In this instance, the hawks barely surround the user in order to execute their last unexpected attack.

$$Y\ (a+1) = Y_{user}(a) - E\ |\ \Delta Y(a)| \quad (5)$$

4. Results and Discussion

The proposed improved Harris Hawks algorithm with MLP model has been implemented in Python Version 3.12, with system configuration being Intel(R) Core (TM) i7-3770 CPU @ 3.40GHz, 8.00 GB RAM and 64-bit operating system with x64-based processor. The Results and Discussion section presents the findings of the proposed approach for Cloud Malware Intrusion

Table 2. Comparison data over performance of proposed model vs other models

Performance (%)	KNN	BPN	SVM	Proposed
Accuracy	91.70	92.72	94.94	98.45
Precision	93.68	96.63	95.65	98.55
Recall	91.43	91.11	94.48	99.88
F1-score	92.78	93.79	95.57	99.21

Detection. By combining the optimization capacities of MLP and

HHO, the methodology produced a synergistic effect that improved the detection system's performance.

In Table 2, our suggested approach is seen to outperform the other models in terms of accuracy with value 98.45%, demonstrating its efficacy in effectively categorizing data instances. We compare the performance of the model with the results of three other models, known as KNN (K-Nearest

Neighbor), BPN (Back Propagation Network) and SVM (Support Vector Machine). The metrics evaluated include accuracy, precision, recall, and F1 score, which are indicative of the model's classification performance.

4.1. Performance Graph

To generate a performance graph for Cloud Malware Intrusion Detection system, let us visualize the evaluation findings and demonstrate how effectively the MLP-HHO system works in particular cloud malware intrusion detection case.

4.1.1. Accuracy

Fig. 3 shows remarkable performance, exhibiting an accuracy of 98.45%, in differentiating between authorized data access and potential intrusion events. This high degree of accuracy highlights the dependability and efficacy of the model in defending against threats to security.

4.1.2. Precision

Precision is a measure of how many of our model's favorable predictions turned out to be accurate. With a precision rating of 98.55%, the proposed model performs excellently in identifying between normal data access and potential intrusion detection systems is shown in Fig. 4.

4.1.3. Recall

The percentage of actual data breaches that our system accurately detects is measured by recall, also known as sensitivity or true positive rate. Fig. 5 shows the system's remarkable 99.88% recall rate. This gauge, which goes by the terms sensitivity and true positive rate, shows how well our system is able to identify nearly all real data intrusions.

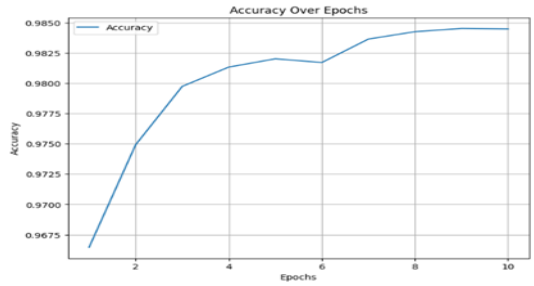

Fig. 3. Performance Graph for Accuracy Prediction

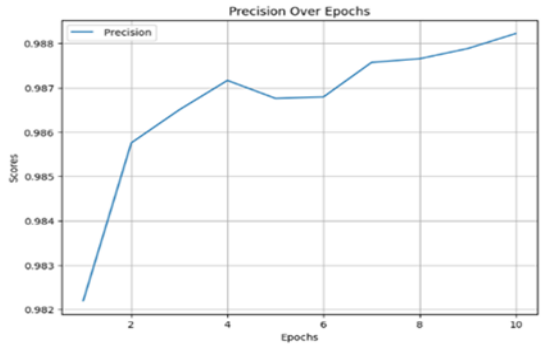

Fig. 4. Performance Graph for Precision Prediction

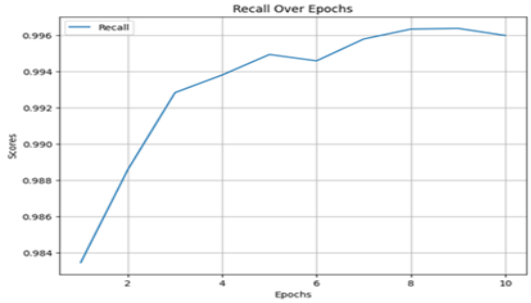

Fig. 5. Performance Graph for Recall Prediction

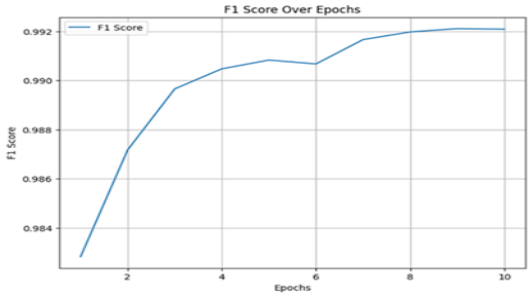

Fig. 6. Performance Graph for F1-score Prediction

4.1.4. F1-score

With a 99.21% F1 score an exceptional result in cloud malware intrusion detection is obtained. Fig. 6 demonstrates the potential to be highly effective in detecting and preventing hazardous attacks in a cloud environment.

4.2. Comparison Graph

Comparing the proposed approach for Cloud Malware Intrusion Detection against other developed deep learning algorithms KNN, BPN and SVM. The comparison graph (Fig. 7) shows the results in terms of several performance metrics (Accuracy, Precision, Recall, and F1-score).

The performance of the proposed method for Cloud Malware Intrusion Detection is shown in Fig. 7 across all evaluated parameters. Our proposed technique provides an effective barrier against malicious intrusions and is highly effective in identifying and addressing malware threats in cloud systems.

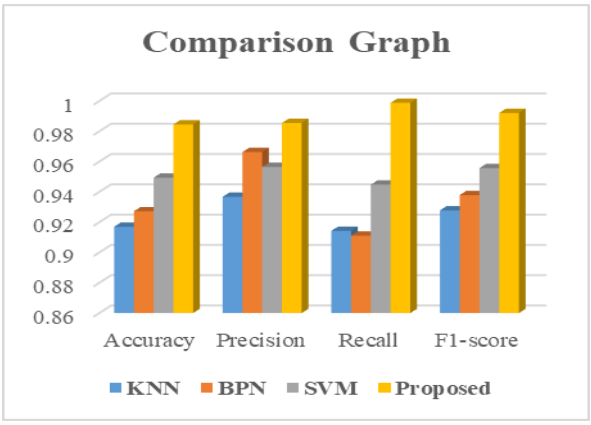

Fig. 7. A comparative graph for the proposed method of cloud malware intrusion detection

5. Conclusion

Hence an effective and innovative approach to addressing the pressing issue of cloud malware intrusion detection is the integration of Multilayer Perceptron (MLP) and Harris Hawks Optimization (HHO). Utilizing an amalgam of dynamic optimization and deep learning approach, this proposed method creates a potent and efficient solution that protects cloud environments against malicious software attacks. Through the implementation of MLP's capabilities, this strategy optimizes the internal parameters of the data monitoring system through HHO. This improves the system's ability to identify abnormalities and departures from expected behavior, which may be signs of malware threats. By methodically examining the MLP model's hyperparameter space, HHO optimizes critical parameters to increase detection accuracy. By using a combined strategy, the method could achieve 98.45% accuracy, 98.55% precision, 99.88% recall and 99.21% F1 Score.

Author contributions

Manjushree C V: Conceptualization, methodology, software, data curation, writing—original draft preparation, **Nandakumar A N**: formal analysis, writing—review and editing, supervision, project administration.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Al-Hawawreh, M., & Moustafa, N., "Explainable deep learning for attack intelligence and combating cyber-physical attacks," *Ad Hoc Networks*, pp. 103329, 2023.

[2] Fascí, L. S., Fisichella, M., Lax, G., & Qian, C., "Disarming visualization-based approaches in malware detection systems," *Computers & Security*, vol. 126, pp. 103062, 2023.

[3] Liu, C., Lu, J., Feng, W., Du, E., Di, L., & Song, Z., "MOBIPCR: Efficient, accurate, and strict ML-based mobile malware detection," *Future Generation Computer Systems*, vol. 144, pp. 140-150, 2023.

[4] Wen, Q., & Chow, K. P., "CNN based zero-day malware detection using small binary segments," *Forensic Science International: Digital Investigation*, vol. 38, pp. 301128, 2021.

[5] Tian, D., Ying, Q., Jia, X., Ma, R., Hu, C., & Liu, W., "MDCHD: A novel malware detection method in cloud using hardware trace and deep learning," *Computer Networks*, vol. 198, pp. 108394, 2021.

[6] Mohammed, M.A., Lakhan, A., Zebari, D.A., Abdulkareem, K.H., Nedoma, J., Martinek, R., Tariq, U., Alhaisoni, M. and Tiwari, P., "Adaptive secure malware efficient machine learning algorithm for healthcare data," *CAAI Transactions on Intelligence Technology*, 2023.

[7] Liu, X., Liu, X., Xiong, N., Luo, D., Xu, G., & Chen, X., "AAJS: An Anti-Malicious Attack Graphic Similarity Judgment System in Cloud Computing Environments," *Electronics*, vol. 12, no. 9, pp. 1983, 2023.

[8] Ping, Y., Zhan, Y., Lu, K., & Wang, B., "Public data integrity verification scheme for secure cloud storage," *Information*, vol. 11, no. 9, pp. 409, 2023.

[9] Susilo, W., Jiang, P., Lai, J., Guo, F., Yang, G., & Deng, R. H., "Sanitizable access control system for secure cloud storage against malicious data publishers," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 3, pp. 2138-2148, 2021.

[10] Aslan, Ö., Ozkan-Okay, M., & Gupta, D., "A review of cloud-based malware detection system: Opportunities, advances and challenges," *European Journal of Engineering and Technology Research*, vol. 6, no. 3, pp.1-8, 2021.

[11] Aljumah, A., & Ahanger, T. A., "Cyber security threats, challenges and defence mechanisms in cloud computing," *IET communications*, vol. 14, no. 7, pp. 1185-1191, 2020.

[12] Vellela, S. S., Balamanigandan, R., & Praveen, S. P., "Strategic Survey on Security and Privacy Methods of Cloud Computing Environment," *Journal of Next Generation Technology*, vol. 2, no. 1, 2022.

[13] George, A. S., & Sagayarajan, S., "Securing Cloud Application Infrastructure: Understanding the Penetration Testing Challenges of IaaS, PaaS, and SaaS Environments," *Partners Universal International Research Journal*, vol. 2, no. 1, pp. 24-34, 2023.

[14] Jadhav, A., & Chawan, P. M., "A System for Detection and Prevention of Data Leak," *International Research Journal of engineering and Technology*, pp: 471-474, 2021.

[15] Pronika, S.S.Tyagi, "Enhancing Security of Cloud Data through Encryption with AES and Fernet Algorithm through Convolutional-Neural-Networks (CNN)", *International Journal of Computer Networks and Applications (IJCNA)*, vol. 8, no. 4, pp. 288-299, 2021.

[16] Roychowdhury, S., & Singh, B. K, "A Hybrid and Multi-objective Approach for Data Leak and Tamper Detection in Healthcare Cloud Data", In *Machine*

Vision and Augmented Intelligence: Select Proceedings of MAI, Singapore: Springer Nature Singapore, pp: 275-285, 2023.

[17] Mottupalli, R. K., "Augmenting the Cloud Environment Security Through Blockchain Based Hash Algorithms", *Journal of Computer Sciences Institute*, vol. 26, pp. 1-6, 2023.

[18] Rubio-Medrano, C. E., Soundrapandian, P. K. D., Hill, M., Claramunt, L., Baek, J., & Ahn, G. J., "DyPolDroid: Protecting against permission-abuse attacks in android," *Information Systems Frontiers*, vol. 25, no. 2, pp. 529-548, 2023.

[19] Song, H., Li, J., & Li, H., "A cloud secure storage mechanism based on data dispersion and encryption," *IEEE Access*, vol. 9, pp. 63745-63751, 2021.

[20] Deyannis, D., Papadogiannaki, E., Kalivianakis, G., Vasiliadis, G., & Ioannidis, S., "Trustav: Practical and privacy preserving malware analysis in the cloud", In *Proceedings of the tenth ACM conference on data and application security and privacy*, pp. 39-48, 2020.

[21] Gao, X., Hu, C., Shan, C., Liu, B., Niu, Z., & Xie, H., "Malware classification for the cloud via semi-supervised transfer learning," *Journal of Information Security and Applications*, vol. 55, pp. 102661, 2020.

[22] Qaisar, Z. H., Almotiri, S. H., Al Ghamdi, M. A., Nagra, A. A., & Ali, G., "A scalable and efficient multi-agent architecture for malware protection in data sharing over mobile cloud," *IEEE Access*, vol. 9, pp. 76248-76259, 2021.

[23] Aslan, Ö., Ozkan-Okay, M., & Gupta, D., "Intelligent behavior-based malware detection system on cloud computing environment," *IEEE Access*, vol. 9, pp. 83252-83271, 2021.

[24] Mishra, P., Aggarwal, P., Vidyarthi, A., Singh, P., Khan, B., Alhelou, H. H., & Siano, P., "VMShield: Memory introspection-based malware detection to secure cloud-based services against stealthy attacks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 6754-6764, 2021.

[25] Vinay J., Zuhair Bilal, Rohit K., Syed Ali Zuhaib, Dr. Mouleeswaran S. K., "Cloud based Malware Detection System," *International Journal of Engineering Research & Technology (IJERT)*, vol. 11, no. 5, 2022.

[26] Ben Abdel Ouahab, I., Elaachak, L., & Bouhorma, M, "Image-based malware classification using multi-layer perceptron", In *Networking, Intelligent Systems and Security: Proceedings of NISS*, Springer Singapore, pp: 453-464, 2021.

[27] Long, Do., "Detecting malware using the MLP algorithm," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, pp. 5640-5644, 2020.

[28] Mohammed, A. J., Arif, M. H., & Ali, A. A., "A multilayer perceptron artificial neural network approach for improving the accuracy of intrusion detection systems," *IAES International Journal of Artificial Intelligence*, vol. 9, no. 4, pp. 609-615, 2020.

[29] Abbas, S., Sampedro, G. A., Abisado, M., Almadhor, A., Yousaf, I., & Hong, S. P., "Harris-Hawk-Optimization-Based Deep Recurrent Neural Network for Securing the Internet of Medical Thing," *Electronics*, vol. 12, no. 12, pp. 2612, 2023.

[30] Alsubai, S., Dutta, A. K., Alnajim, A. M., Ayub, R., AlShehri, A. M., & Ahmad, N., "Artificial intelligence-driven malware detection framework for internet of things environment," *PeerJ Computer Science*, vol. 9, pp. 1366, 2023.