DS Journal of Multidisciplinary
Volume 1 Issue 1, 31-36, Jan - Mar 2024
ISSN: XXXX-XXXX

*Original Article*

# An Optimized Neural Framework to Detect Cryptojacking Malware

**S. David Jebasingh**

*Data Analyst, LatentView Analytics, Tamil Nadu, India.*

djsingh17d13@gmail.com

Received: 27 October 2023; Revised: 22 November 2023; Accepted: 18 December 2023; Published: 22 January 2024;

**Abstract -** Cryptojacking is the process of hacking the user's system to mine cryptocurrencies without the user's acknowledgement through websites. The growing popularity of crypto-currencies and the increasing number of transactions over the internet demand an effective malware detection framework. Hence, a novel hybrid Improved Whale Optimization-based Modular Neural Network model was designed in this paper to detect the network and host-based cryptojacking malware effectively. Initially, the cryptojacking mining dataset was gathered from the standard site and imported into the system. To standardize the raw dataset, it is pre-processed using modular neural features. Then, the whale optimal fitness function is applied in the feature extraction module to track and extract the important data features. In the detection phase, the extracted features are matched with the trained attack features to identify the malicious data. Finally, the results are estimated and compared with the traditional schemes for verification. The performance and comparative analysis show that the presented algorithm outperforms the existing model regarding accuracy, precision, and recall.

**Keywords -** Cryptojacking, Malware detection, Modular Neural Network, Improved Whale Optimization Approach, Crypto-currency.

## 1. Introduction

In recent times, blockchain technologies have utilized the Proof of Work (PoW) approach to ensure immutability in on-chain transactions [1]. This PoW method mainly depends on the computational energy of the system hardware like the Central Processing Unit (CPU), Graphics Processing Unit (GPU), chipsets, etc., [2]. These elements help the crypto miners to resolve complex hash-based problems. However, solving this problem consumes a huge amount of energy and is the reason for the high energy cost in crypto-currency operations [3]. In this ecology, cryptojacking defines the process of utilizing the user's computational power without their acknowledgement [4].

Presently, there are two different ways by which the attackers use the processing power of the users for cryptojacking. The two ways include the injection of script into the website and the extension of mining operation into the host machine. The script's injection and the mining operation extension increase the system vulnerabilities [5].

In the initial phase, the cryptojacking attackers target personal computers by injecting the mining script into famous websites. Then, they start to target the large domains with bigger attacks. In recent times, cryptojacking

attackers have begun to target IoT devices adversely because of their rapid growth and increasing usage in industry, homes, offices, and healthcare [6].

Generally, IoT systems are limited to resource usage and power conservation [7]. Hence, they are not profitable to attackers individually [8]. Hence, the attackers use methods like botnet attacks to take control of the IoT tools to achieve crypto-currency mining. The popular botnet attack approach includes Distributed Denial of Service (DDoS), Mirai, DoS, etc. The attackers using the Mirai botnet attack utilize the network to mine bitcoins and make the botnet system a large cryptojacking mining tool.

Moreover, there are many reasons why the IoT system requires profitable targets compared to the non-IoT systems [9]. The first reason is the wide usage of IoT devices, making them more vulnerable to attackers. The second reason is the restriction of resources and power to the IoT devices. The third is the security flaws of IoT devices. The lack of security functions in IoT networks makes them more vulnerable to cryptojacking malware attacks. Although various malware detection schemes have been implemented in the past to detect browser and host-based cryptojacking malware, they face significant challenges in detection performance [10].

Hence, in this article, a deep learning-based cryptojacking malware detection model was designed to identify both browser and host-based IoT cryptojacking attacks. The key contribution of the proposed framework is described as follows,

- A novel optimized deep learning-based cryptojacking malware detection scheme was designed to identify both browser and host-based cryptojacking malware effectively.
- Initially, the dataset was collected and imported into the system to initialize the detection process.
- Then, the collected dataset was pre-processed using the deep neural features to eliminate the training flaws.
- Further, the features are extracted and tested with the trained attack features for classification purposes.
- Finally, the results are evaluated and compared with the existing techniques regarding accuracy, precision, recall, and f-measure.

The presented paper is arranged as follows: the background of cryptojacking malware detection is illustrated in section 2, the proposed framework is explained in section 3, the proposed model results are analyzed in section 6, and the article's conclusion is described in section 5.

## 2. System Model with Problem Statement

Similar to other security attacks, cryptojacking is the act of hijacking the user's system to mine cryptocurrencies against their will through websites. Cryptojacking attackers use script injection and extension of mining operations to hack the user's system. In recent times, cryptojacking has mainly targeted IoT devices because of their wide usage.

Therefore, to detect this cryptojacking malware, different schemes involving machine learning and deep learning algorithms were proposed earlier. Machine Learning (ML) techniques, such as Random Forest, Support Vector Machine, etc., involve training the system based on the available resources to identify the malware. The ML-based detection mechanism demands huge resources to train the system.

On the other hand, deep learning models like Convolutional Neural Network systems, Recurrent Neural Network systems, etc., include data filtering, feature selection, and classifiers to detect malicious data. However, the optimal selection of features in deep learning is one of the biggest challenges. To overcome these challenges, an optimized neural-based cryptojacking malware detection framework was developed in this paper.

## 3. Proposed IWObMNN for Cryptojacking Malware Detection

In this paper, an optimized deep neural-based cryptojacking malware detection algorithm was developed to identify the browser and host-based malware attacks. This presented scheme integrates the Improved Whale Optimization algorithm and Modular Neural Network system. Initially, the cryptojacking malware detection dataset was collected and imported into the MATLAB system for training purposes. A pre-processing mechanism was designed using the modular neural features to remove the training flaws.

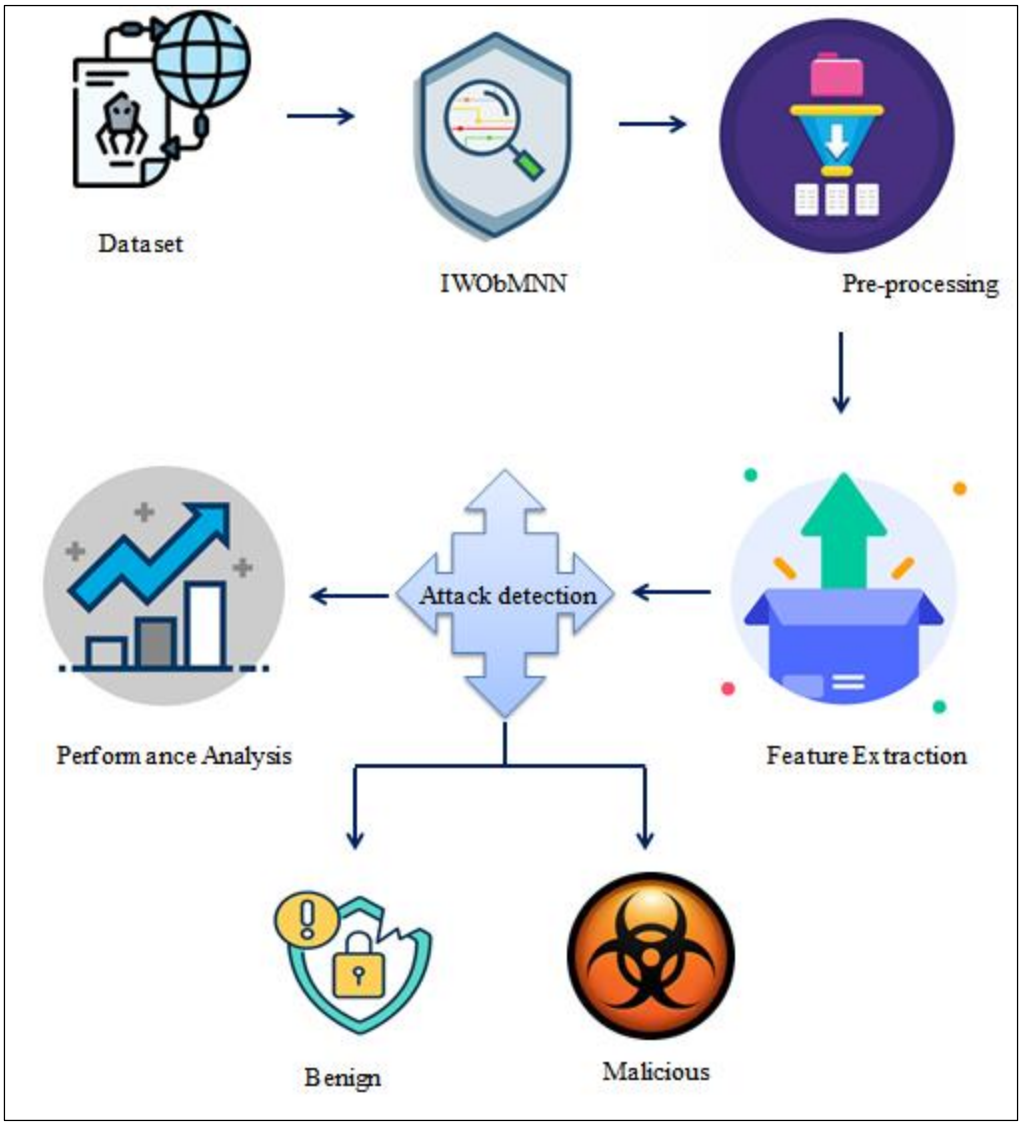


**Fig. 1 Proposed IWObMNN framework**

Further, the important data features are extracted using the whale optimal fitness solution. These extracted attributes are tested with the trained data features for attack detection purposes. Finally, the outcomes of the presented model are estimated and validated with the traditional scheme. The proposed framework is illustrated in Figure 1.

### *3.1. Dataset Pre-Processing*

The cryptojacking malware detection has four phases, namely, Data collection, Pre-processing, Feature extraction, and Malware detection. The cryptography malware dataset was collected from the Kaggle site and

initialized in the system in the initial phase. The dataset contains network and host-based attributes in numerous rows and columns. In the system, the dataset was split into 6:4 ratios for training and testing purposes. Then, the dataset was pre-processed using the modular neural features to eliminate the training flaws and errors present in the dataset. The Modular Neural Network (MNN) system is a type of artificial neural network which is applied to solve problems with less complexity. The main function of MNN is its capability to divide the huge task into sub-tasks. In the proposed framework, the MNN attribute helps separate the errors and null values from the dataset. The pre-processing mechanism is formulated in Equation (1).

$$\chi_F\left[C_{md}\right]=\frac{1}{\vartheta}\sum_{n=1}^{l}\left\|C_{md}-\hat{G}_{md}\right\|^2 \tag{1}$$

Where $\chi_F$ represents the filtering mechanism, $C_{md}$ denotes the dataset, $\vartheta$ refers to the pre-processing variable, $\hat{G}_{md}$ indicates the error and null data present in the dataset, $n$ denotes the iteration, and $l$ refers to the total number of data available in the dataset.

### *3.2. Feature Extraction*

The filtered dataset contains both meaningful and meaningless features. To simplify the detection process and to minimize the complexity of the system, the important features are tracked and extracted. Initially, the features present in the filtered dataset are tracked, and then the important features are extracted. In this process, the meaningless features are eliminated from the dataset. The improved whale fitness is applied to track the important data features in the proposed framework. The whale optimization algorithm is a nature-inspired meta-heuristic approach developed to solve different optimization problems. It is based on the unique characteristics of whales. Here, the unique optimal prey encircling characteristic of the whale is utilized to track the important features. The feature tracking function is expressed in Equation (2).

$$F_{tk}=\left|\sigma.\left(C'_{md},C^{*}_{md}\right)\right| \tag{2}$$

Here $F_{tk}$ , it denotes the feature tracking function, $\sigma$ presents the data tracking variable, $C'_{md}$ indicates the important data features, and $C^{*}_{md}$ refers to the meaningless data features. After feature tracking, the tracked important features are extracted, and the unimportant features are removed. The feature extraction function is represented in Equation (3).

$$G_{xt}\left(C'_{md+1}\right)=\left|C_{md}-\varepsilon.\,C^{*}_{md}\right| \tag{3}$$

Where $G_{xt}$ indicates the feature extraction function and $\varepsilon$ denotes the random variable. The extracted features contain both malicious and benign data. In the malware detection phase, these extracted features are compared with the trained attack features for classification purposes. Thus, the presented model detects the malicious features in the network effectively.

## 4. Results and Discussion

A hybrid malware detection framework was proposed in this paper to detect the cryptojacking malware optimally. The presented algorithm was trained and tested with the cryptojacking mining dataset, which contains 3 CSV files, namely abnormal data, normal data, and complete data. Initially, the dataset was split into 6:4 ratios for training and testing purposes. In the presented framework, the attributes of MNN and IWOA were integrated

to detect the malicious data effectively. The developed scheme was implemented in the MATLAB software, and the results are determined in terms of accuracy, precision, recall, and f-measure. Moreover, a comparative assessment was performed to validate the estimated results. The performance analysis is displayed in Figure 2.

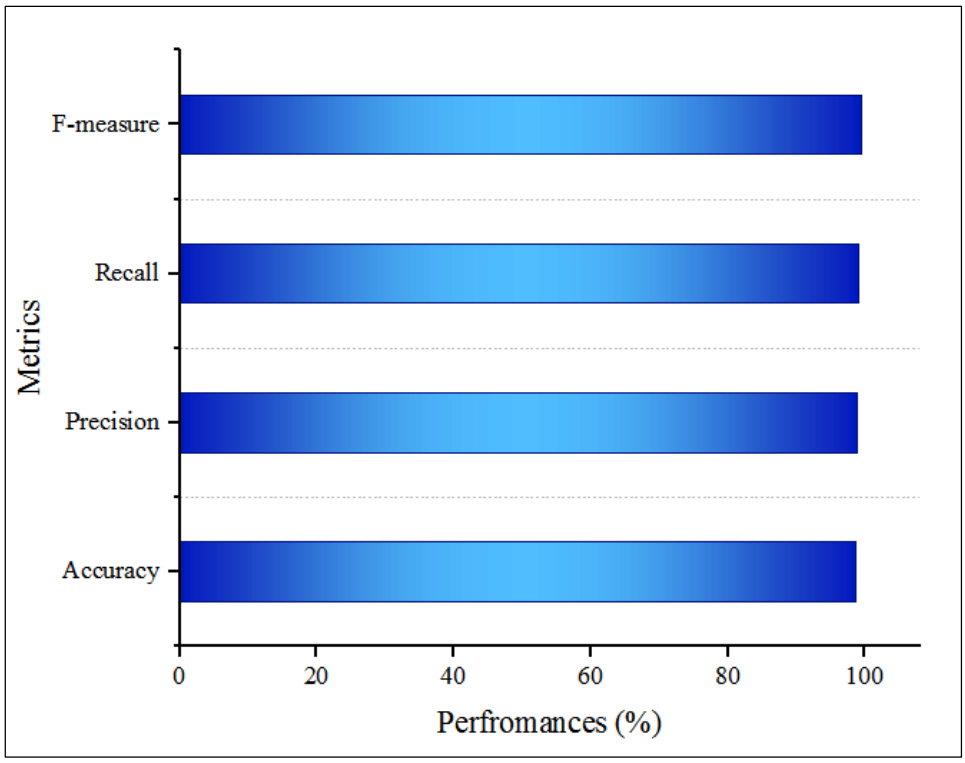


**Fig. 2 Performance analysis**

**Table 1. Comparative assessment**

| Techniques | Accuracy | Precision | Recall | F-Measure |
|---|---|---|---|---|
| CD_DLbHTA | 83.61 | 81.98 | 79.85 | 82.86 |
| CCAM_DS | 79.56 | 76.79 | 67.06 | 81.2 |
| AEbCD | 78.34 | 74.73 | 76.89 | 76.45 |
| HPbCD | 90.43 | 87.77 | 85.19 | 87.56 |
| Proposed | 98.67 | 98.9 | 99.07 | 99.43 |

Finally, the evaluated results are compared with existing techniques like Cryptojacking Detection using Deep Learning based Hardware Tracking Approach (CD_DLbHTA) [11], Cryptojacking Convert Attack Model using Delay Strategy (CCAM_DS) [12], Auto-Encoder-based Cryptojacking Detection (AEbCD) [13], and Honeypot-based Cryptojacking Detection [13]. The overall comparative assessment is tabulated in Table 1. The comparative analysis proves that the presented approach attained greater performance than the existing techniques.

## 5. Conclusion

This paper introduced a novel hybrid cryptojacking malware detection model to effectively detect the host and network-based cryptojacking malware. The presented model hybridizes the features of MNN and IWOA to detect the malware with less computational time. The developed scheme was tested and validated with a cryptojacking mining dataset in the MATLAB software. This detection framework includes data processing,

feature selection, and malware detection modules. The MNN features are applied to filter the input dataset, and the optimal whale fitness is utilized in the proposed framework to track and extract the important data features. Finally, the performances are estimated and compared with the existing malware detection scheme for validation purposes. In addition, the performance enhancement percentage is calculated from the comparative assessment. It is noticed in the proposed model that performances like accuracy, precision, recall, and f-measure are enhanced by 8.24%, 11.12%, 13.9%, and 12.05%, respectively. Thus, the developed scheme accurately detects the cryptojacking malware in the network.

## References


[1] Randhir Kumar, Ningrinla Marchang, and Rakesh Tripathi, "Distributed Off-Chain Storage of Patient Diagnostic Reports in Healthcare System Using IPFS and Blockchain," *International Conference on Communication Systems & Networks,* 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Muhammad Awais Khan et al., "Robust, Resilient and Reliable Architecture for V2X Communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4414-4430, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Jirdehi, Mehdi Ahmadi, and Vahid Sohrabi Tabar, "Risk-Aware Energy Management of a Microgrid Integrated with Battery Charging and Swapping Stations in the Presence of Renewable Resources High Penetration, Crypto-Currency Miners and Responsive Loads," *Energy,* vol. 263, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Ke Ye et al., "Real-Time Detection of Cryptocurrency Mining Behavior," *Blockchain and Trustworthy Systems,* pp. 278-291, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Emanuele Iannone et al., "The Secret Life of Software Vulnerabilities: A Large-Scale Empirical Study," *IEEE Transactions on Software Engineering*, vol. 49, no. 1, pp. 44-63, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Martti Lehto, "Cyber-Attacks against Critical Infrastructure," *Cyber Security*, pp. 3-42, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Christos Xenofontos et al., "Consumer, Commercial, and Industrial IoT (In) Security: Attack Taxonomy and Case Studies," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 199-221, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Maurantonio Caprolu et al., "Cryptomining Makes Noise: Detecting Cryptojacking via Machine Learning," *Computer Communications*, vol. 171, pp. 126-139, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Ege Tekiner et al., "SoK: Cryptojacking Malware," *IEEE European Symposium on Security and Privacy*, pp. 120-139, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Fábio Gomes, and Miguel Correia, "Cryptojacking Detection with CPU Usage Metrics," *IEEE 19th International Symposium on Network Computing and Applications*, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Qianjin Ying et al., "CJSpector: A Novel Cryptojacking Detection Method Using Hardware Trace and Deep Learning," *Journal of Grid Computing*, vol. 20, no. 3, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Aldo Hernandez-Suarez et al., "Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks," *Applied Sciences*, vol. 12, no. 7, pp. 1-28, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Fredy Andrés Aponte-Novoa et al., "On Detecting Cryptojacking on Websites: Revisiting the Use of Classifiers," *Sensors*, vol. 22, no. 23, pp. 1-15, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] Priyank Patel, Ashwini Dalvi, and Irfan Sidddavatam, "Exploiting Honeypot for Cryptojacking: The Other Side of the Story of Honeypot Deployment," *6th International Conference on Computing, Communication, Control and Automation*, pp. 1-5, 2022. [CrossRef] [Google Scholar] [Publisher Link]