International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Machine Learning Approach for Identifying Cryptojacking Attacks

Gunjan Karade[1], Prof. Pooja Hardiya[2]
Research Scholar, Department of CSE, SDBCE, Indore (India)[1]
Asst. Professor, Department of CSE, SDBCT, Indore (India)[2]

ABSTRACT: With the rise of popularity of cryptocurrencies such as Bitcoin, Libra, Ripple, Ethereum etc, more attacks on crypto-currencies have been seen. Crypto-jacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads crypto-mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser. Given the lower-risk/lower effort nature of crypto-jacking, the number of such incidents in 2018 were nearly double of those of ransomware attacks. Apart from the crypto-jackers, web-crypto-mining library providers also enabled benign publishers to use this mechanism as an alternative monetization schema for web in the era of declined ad revenue. The proposed work aims at detecting crypto jacking based on Machine Learning based approaches.

Keywords: Data-mining, Darkweb, Crypto Mining Crypto currency: Bitcoin; Crypto-jacking; Machine Learning

I. INTRODUCTION

Crypto currency is an internet-based medium of exchange which uses crypto graphical functions to conduct financial transactions. Crypto currencies can be sent directly between two parties via the use of private and public keys. These transfers can be done with minimal processing fees, allowing users to avoid the steep fees charged by traditional financial institutions. Examples of crypto currencies: Bitcoin, Libra, Ripple, Ethereum etc. The most important feature of a crypto currency is that it is not controlled by any central authority: the decentralized nature of the block chain makes cryptocurrencies theoretically immune to the old ways of government control and interference. Cryptocurrencies can be sent directly between two parties via the use of private and public keys. These transfers can be done with minimal processing fees, allowing users to avoid the steep fees charged by traditional financial institutions.

Also known as crypto coin mining, altcoin mining, or Bitcoin mining (for the most popular form of cryptocurrency, Bitcoin), cryptocurrency mining has increased both as a topic and activity as cryptocurrency usage itself has grown exponentially in the last few years. Each time a cryptocurrency transaction is made, a cryptocurrency miner is responsible for ensuring the authenticity of information and updating the block chain with the transaction. The mining process itself involves competing with other crypto miners to solve complicated mathematical problems with cryptographic hash functions that are associated with a block containing the transaction data. Cryptojacking is utilizing a host system to illegally mine cryptocurrencies without the knowledge of the host system. Web-based mining is a method of cryptocurrency mining that happens inside a browser, using a script delivered from a website. The first attempts of in-browser such as Bitcoin mining failed due to the increased mining difficulty. However, the rise of alternative crypto-coins (altcoins) that provide distributed mining, increased mining speed and ASICs, has again made it viable to implement crypto mining and cryptojacking.

II. PROBLEMS STATEMENT AND PROPOSED ARCHITECTURE

Typical crypto-attackers try to use the computational power of innocent web users to mine cryptocurrencies illegally (called crypto-jacking). However, it is extremely difficult to detect crypto-jacking attacks because of the following reasons:

1) The attack code is generally very small (compact)
2) The attack doesn't produce any significant effect.
3) Only some common issues like the machine slowing down, more CPU utilization or mild heating can be observed.
4) Hence most attacks go unnoticed.

Typical signs of a crypto-mining operation include increased CPU usage, degraded system performance, and sluggish application responsiveness. Demands imposed by crypto-mining can have serious consequences. "In one instance, crypto-mining software was known to destroy the device that hosted it. Even if signs of crypto-jacking appear on a system, finding the malware can be challenging.

System defenses that depend on software signatures and anomalies, such as modified files or system data, can struggle to identify crypto-mining malware when it lands on a network. Crypto-miners do not modify files, and their anomalous behavior is limited to increased CPU usage or power consumption that can be hard to attribute specifically to a crypto-miner, since there can be other applications—games, for instance—that tend to over-consume the processing capabilities of a system. Increased CPU usage is easier for an individual to recognize than it is for a typical enterprise

The approach would use standard benchmark data sets for testing.

The features are to be selected which are:

1) Temperature
2) Power
3) Network Speed
4) CPU Utilization
5) Memory Utilization
6) Interfering applications (interference)

The features are to be fed to a machine learning based tool to classify detect the attacks. The architecture of the machine learning to be used for the proposed system is shown in the figure below with the data collected from the benchmark datasets.

III. PROPSED METHODOLOGY

After the design of the neural network, it is critical to decide the training algorithm for the same. This is due to the fact that different ANN architectures have different attributes for:

1) Training time or epochs
2) Stability in error
3) Absolute time
4) The rate at which error falls w.r.t. change in weights

The scaled conjugate gradient (SCG) is a training algorithm which has low space complexity which makes it suitable for applications with limited memory and processing power. This can be seen especially in the mobile computing sector. The scaled conjugate gradient approach is based on finding the best gradient for reducing the errors in training. The machine learning algorithm used in this work is a combination of scaled conjugate gradient and K-Nearest Neighbor.

Scaled Conjugate Gradient:

Let there be a data set with 'n' samples. There are multiple ways in which the data and the errors in each iteration can be fed to the neural network to attain stability and reduction in errors. The factor that governs the factor is the weights 'w'. Let us consider that the gradient starts with p0 for the zeroth iteration given by:

$$\boldsymbol{p_0 = -g_0}$$

The negative sign indicates that the gradient moves in such a way the at the error decreases with the weight as well as the iteration. The training rule is:

$$\boldsymbol{x_{k+1} = x_k + \alpha_k g_k}$$

Here,

k is the present iteration

k+1 is the next iteration

α_k is the step size for weights

g_k is the gradient for the kth iteration

x_k is the weight of the present iteration denoted by k

x_{k+1} is the weight of the next iteration denoted by k+1

For any specific iteration k, the gradient vector P is given by:

$$\boldsymbol{P_k = -g_k + \beta_k P_{k-1}}$$

Here p is search direction vector and g is gradient direction vector. The other parameters are given by:

$$\boldsymbol{\beta_K = \frac{(|g_{k+1}|^2 - g_{k+1}{}^T g_k)}{g_k{}^T g_k}}$$

$$\boldsymbol{P_{k+1} = -g_{k+1} + \beta_k P_k}$$

Here,

T represents the transpose operation.

It can be clearly seen that the gradient varies in each iteration to move towards the steepest gradient.

The KNN Approach

KNN stands for the K-Nearest Neighbor. KNN is an effective technique for complex classification problems. The approach works on the following approach which is laid out in the following steps:

1) Receive an unclassified data;
2) consider the classified trained data sets as a standard sample;
3) Obtain new unclassified data;
4) Measure the distance of the unclassified data set from the sample
5) The distance which is least decides the category of the new data sample
6) The classifier learns from the tested data

This is clearly seen that the multivariate distance d decides the category of a particular sample. The new samples create new multi-variate distances and new tested samples.

Sensitivity (Se): It indicates the algorithms ability to correctly detect the samples which test affirmative and belong to a particular category specified by feature values.

Accuracy (Ac): It indicates the algorithms ability to detect correctly whether a sample belongs to a particular data set category or not out of all the possible classification outcomes.
Thus, the above-mentioned parameters help in the evaluation of any proposed algorithm which deals with statistical data and statistical modelling. It is desirable to attain high values of sensitivity and accuracy. The performance metrics are defined as:

1. **True Positive (TP):** It is the categorization of a data sample into positive with correct prediction
2. **True Negative (TN):** It is the categorization of a data sample into negative with correct prediction.
3. **False Positive (FP):** It is the categorization of a data sample into positive with incorrect prediction
4. **False Negative (FN):** It is the categorization of a data sample into negative with incorrect prediction

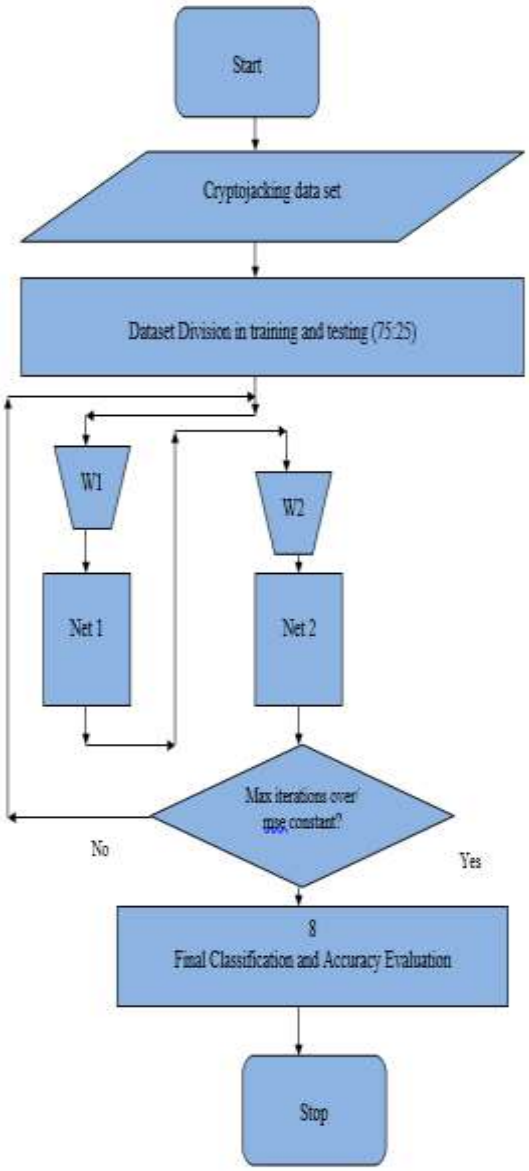

Fig.1 Flowchart of Proposed System

Sensitivity (S_e): It is the comparative positive marker in the data set as how many samples are marked positive. Mathematically:

$$Se = \frac{TP}{TP + FN}$$

Accuracy (Ac): It is a measure of the correctness of classification prediction. It is the ratio of correct classifications to all classifications. Mathematically:

$$Ac = \frac{TP + TN}{TP + TN + FP + FN}$$

The aim would be to hit higher accuracy compared to previously existing systems.

IV. RESULTS

The results have been presented in terms of the following parameters for 2 different datasets:

1) The neural network designed has been deliberately kept devoid of multiple hidden layers so as to reduce the space and time complexity of the system .
2) The above mentioned point is particularly useful for real time critical applications.
3) The evaluation parameters are:
a) Classification accuracy
b) Confusion matrix
c) Neural network training parameters

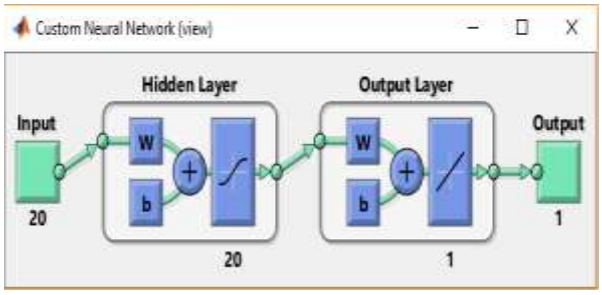

Fig. 2 Neural Network for Classification

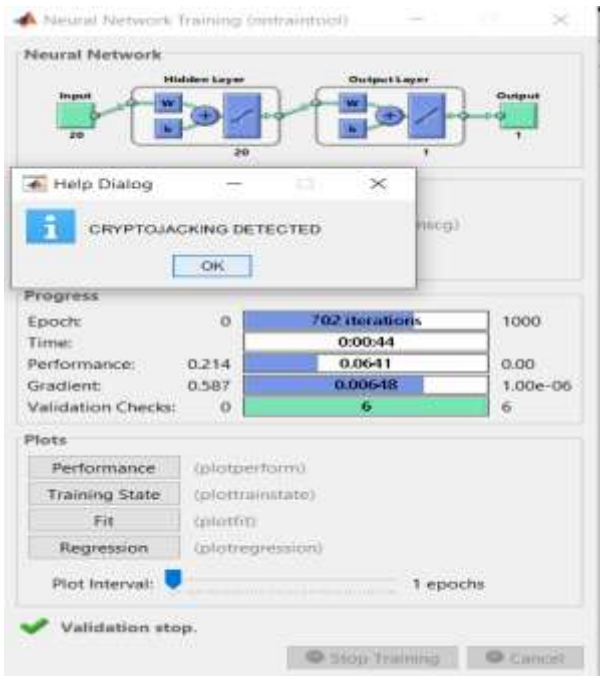

Fig. 3 Cryptojacking Classification by System

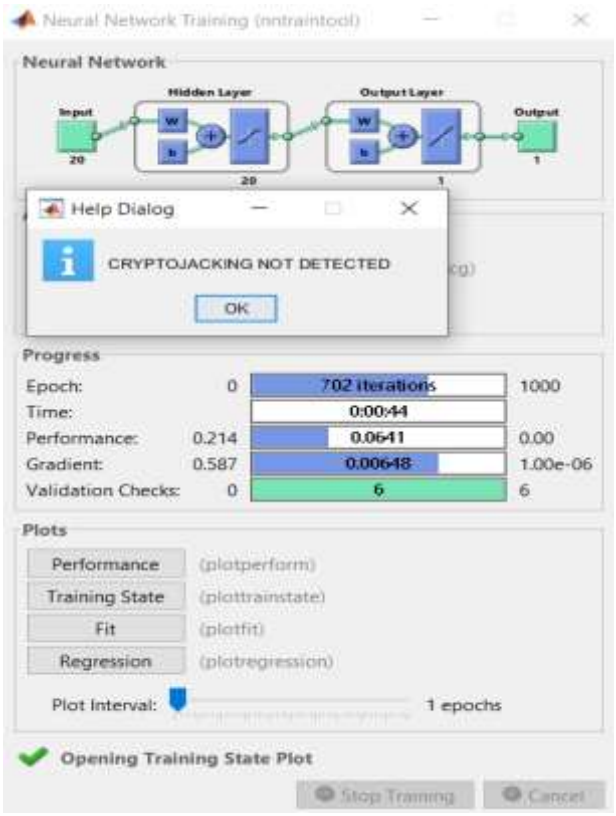

Fig. 4 Non Cryptojacking Classification by System

Fig. 5 Confusion Matrix

CONCLUSION: In this proposed approach, two different data sets have been used for training, validating and subsequently testing the neural

network architecture. The two categories of ANN used for classification using the ada-boost technique in this approach are the scaled conjugate gradient (SCG) approach along with the KNN based classifier. The scaled conjugate gradient if effective in reducing the errors with the steepest gradient approach even for low or limited memory applications specifically suitable for mobile computing applications. The KNN acts as an effective classifier which can effectively classify multi variate data sets. The ada boost approach and its utility can thus be clearly validated from the accuracy of classification of the proposed system. It has been found that the proposed approach attains an accuracy of 97.5% as compared to 93% of the previous work.

References

[1] O Sanda, M Pavlidis, N Polatidis, "A deep learning approach for host-based cryptojacking malware detection", Evolving Systems, Springer, 2023, pp.1-16

[2] Shashank GuptaB. B. Gupta, "XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud", Springer 2022

[3] Patrick Duesse, Christian Gehl ,Ulrich Flegel Sven Dietrich ,Michael Meier, "Detecting zero-day attacks using context-aware anomaly detection at the application-layer", IEEE 2021.

[4] Panagiotis Papadopoulo, Panagiotis Ilia, and Evangelos Markatos, "Truth in Web Mining: Measuring the Probability and the Imposed Overheads of Cryptojacking, Springer 2019

[5] Debabrata Kara, Suvasini, Panigrahib, Srikanth Sundararajan, "SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM", Elsevier 2016

[6] Shashank Gupta B. B. Gupta, "JS-SAN: defense mechanism for HTML5-based web applications against javascript code injection vulnerabilities", Wiley Online Library 2016.

[7] Yen-Lin Chen ; Hahn-Ming Lee ; Albert B. Jeng ; Te-En Wei, "DroidCIA: A Novel Detection Method of Code Injection Attacks on HTML5-Based Mobile Apps", IEEE,2015.

[8] Panagiotis Papadopoulo, Panagiotis Ilia, and Evangelos Markatos, "Truth in Web Mining: Measuring the Probability and the Imposed Overheads of Cryptojacking, Springer 2019

[9] Shashank GuptaB. B. Gupta, "XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud", Springer 2018

[10] Patrick Duesse,Christian Gehl ,Ulrich Flegel Sven Dietrich ,Michael Meier, "Detecting zero-day attacks using context-aware anomaly detection at the application-layer", IEEE 2017

[11] [Roberta PiscitelliEmail authorShivam BhasinFrancesco Regazzoni, Fault Attacks, Injection Techniques and Tools for Simulation, Springer 2017

[12] Debabrata Kara,Suvasini, Panigrahib, Srikanth Sundararajan, "SQLiGoT: Detecting SQL injection attacks using graph of tokens and SVM", Elsevier 2016

[13] Shashank Gupta B. B. Gupta, "JS-SAN: defense mechanism for HTML5-based web applications against javascript code injection vulnerabilities", Wiley Online Library 2016.

[14] Yen-Lin Chen ; Hahn-Ming Lee ; Albert B. Jeng ; Te-En Wei, "DroidCIA: A Novel Detection Method of Code Injection Attacks on HTML5-Based Mobile Apps", IEEE,2015.

[15] Danda B. Rawat ; Chandra Bajracharya, "Detection of False Data Injection Attacks in Smart Grid Communication Systems", IEEE 2015.

[16] Xing Jin, Xunchao Hu, Kailiang Ying, Wenliang Du, Heng Yin and Gautam Nagesh Peri, "Code Injection Attacks on HTML5-based Mobile Apps: Characterization, Detection and Mitigation",IEEE, 2014.