




Cryptojacking Detection Using Genetic Search Algorithm

Ayush Kumar Bar ¹ , Akankshya Rout ¹, Ankush Kumar Bar ²

¹Department of Computer Science Engineering, Techno Engineering College, Banipur, West Bengal, India

²Department of Computer Science Engineering, Coochbehar Government Engineering College, West Bengal, India

Email: ayush.kumar.bar.official@gmail.com

Article History

Received: 10 February 2023

Accepted: 23 April 2023

Keywords:

Logistic Regression;
Decision Tree Classifier;
Random Forest Classifier;
Multi-Layer Perceptron;
Genetic Search;
Cryptocurrency;
Cryptojacking;
SVM

Abstract

Mining cryptocurrency with an unauthorized and unlawful access to a victim's computer's processing power is called cryptojacking. With the rise of cryptocurrency in the markets people took advantage of this new piece of technology through mining it and earning from it. When the need for more performance and money emerged people came out with unlawful activities to mine cryptocurrency using other's devices without their consent. These activities have led people and their devices vulnerable for the sake of greed. This is a distributive approach which uses victim's machine to mine cryptocurrency using all its resources i.e., CPU, GPU etc. This doesn't need any software installation but just to visit sites which are embedded with the malicious scripts that helps accessing user's device. The analogy of this study is not limited to detect the presence of cryptojacking but also to enable users to detect the presence of any kind of suspicious activity is performed on the device. Through Genetic Search algorithm we extracted some of the key metrics used by computers for monitor its resources and further used these metrics to classify the presence of any unauthorized activity and achieved 100% accuracy for classifying these instances. The classification was done using several classification algorithms such as SVM (kernel – "linear"), SVM (kernel – "Radial Bias Function"), Logistic Regression, Decision Tree Classifier, Random Forest Classifier, Multi-Layer Perceptron. The Genetic Search algorithm mentioned earlier is a machine learning iterative technique which is based on natural selection it selects individuals from the current population as parents and uses them to generate the next generation of offspring and all this through a method called CfsSubsetEval which returns a fitness score to the child based on their dependency on other attributes. For comparison we also used several methods which also serves the same objective.

1. Introduction

Cryptojacking is an unauthorized and unlawful mining activity done by the attackers who use the victim's computer's processing capacity to mine cryptocurrency. It is a distributive approach which

causes a significant amount of computational consumption and lowers the victim's computer's processing efficiency. It can take any form, from installing malicious software like Ransome, trojan etc. to Running the mining script if the victim is

active on a website. For e.g., Pirate Bay was using the user's processor in an unauthorized manner till users were active on their page. In comparison to other cyberattacks Crypto jacking is very profitable. First here the attacker uses others' devices to mine bitcoin or digital currency. Second, nowadays there is no need to install any malicious software in the victim's device as much as the victim's device is active on the page, mining can easily be done. Third, for bitcoin mining an extensive amount of computational power is required and as many users are active on the page computational power will increase. According to an article titled "2022 SonicWall Cyber Threat Report" from the cybersecurity bureau SonicWall claims that cryptojacking attacks have increased in the financial sector by 269% year to date, which is nearly five times higher than cyberattacks directed at the retail sector. Also, in the study from SonicWall, the total number of cryptojacking incidents increased by 30% to 66.7 million in the first half of 2022. According to the article published in (India. S, Xavier, and Sahni Chharit) researchers found that the price of Bitcoin has fallen dramatically since January 2022, but the number of crypto jacking incidents has continued to rise, demonstrating that these crimes persist regardless of price changes.

Nowadays attackers use different types of strategies to perform crypto jacking. First is to convince victims to download crypto mining code onto their respective devices. This is accomplished by using social engineering techniques like phishing, in which the targets get an email that appears to be real and instructs them to click a link. The malicious code that the URL executes adds the crypto mining script to the device. The script then continues to execute in the background as the target person works. The second strategy involves inserting a script into a website or advertisement that is then sent to numerous websites. The script is automatically executed as the victim accesses the website or the malicious advertisement displays in their browser. There is no code stored on the victim's machine. In both approaches, the code executes complex mathematical equations on the intended computer and sends the results to the hacker-controlled site. It is the most common approach by the attackers. Third, a new concept or a new way for revenue collection in which the attacker uses the processor of the user

until the user is active on their page, it can be any website.

Numerous crypto jacking businesses are breaking into cloud infrastructure and using an even larger number of compute pools to fuel their mining operations to benefit from the scalability of cloud resources.

In a blog post, senior security researcher for Palo Alto Networks, Guy Arazi, stated that "attackers are targeting cloud services by any means today to mine more and more cryptocurrency, as cloud services can allow them to run their calculations on a larger scale than just a single local machine, whether they're taking over a user's managed cloud environment or even abusing SaaS applications to execute their calculations" (Networks).

Cloud-based assaults are very profitable, according to Matt Muir, security researcher for Cado Security, in a blog post (Cado Security). "The profitability and accessibility of performing crypto jacking at scale makes this type of attack low-hanging fruit," he wrote. If consumers continue to expose services like Docker and Redis to suspicious parties, this is probably going to continue.

As per (nukala) the reason for originating and spreading crypto jacking was with the advent of Bitcoin and many other forms of digital currency, people started preferring decentralized modes of transaction to avoid any involvement of any authority, especially to escape the monopoly and of banks over people's money. And as per the data (CoinDesk) cryptocurrency's price was hitting a milestone and after reaching \$500 billion in late December 2020, Bitcoin (BTC) reached \$1 trillion in February 2021. As a result, ether's market cap is already getting close to that of bitcoin. These headlines caught the attention of people around the world as well as cybercriminals and hence to earn money in an illegal way.

With the help of this research, we will be able to know whether the system is a victim of cryptojacking or not or in simple terms what are the factors to be checked in the system to verify if it is under cryptojacking.

2. Literature Review

In this section, we will highlight those who have worked on this research before. As discussed above with this research, we will try to find out whether the

system is a victim of cryptojacking or not and what are the factors that get affected the most when the system is under the threat of cryptojacking? After going through much research, we found in how many ways cryptojacking can be done has examined the trends of in-browser mining of cryptocurrencies and found that unlike other websites some websites use malicious JavaScript code while visiting without the consent of the user. A study by Google's Cybersecurity Action Team (" [Threat Horizons Executive Snapshot](#) ") reported that 86% of compromised cloud instances are used for crypto mining. A lot of machine learning techniques or algorithms are proposed by many research papers. ([Ganepola and Bandara](#)) compared many existing research papers based on their techniques and highlighted the drawbacks and proposed the technique with an accuracy of 95%. While going through the research papers it was found that most of the papers used pre-existed labelled dataset for e.g. ([Caprolu et al.](#)) used the dataset of Google Play AMD and proposed a classification algorithm with model accuracy of 96%. It was very useful as it was supporting a multi-adversarial profile, but the limitation was it considered a specific crypto client network. Similarly other research papers i.e. ([Miele and Postolache](#)) ([S, Xavier, and Sahni](#)) proposed the solution with a model accuracy 99% and 98%, but the drawback or limitation was the dataset which was considered not general.

Undergoing much research, it was concluded that the major problem is related to the dataset. Most of the datasets were insufficient. To overcome this problem, we proceed with the raw dataset ([Chharit](#)) to get an idea of all factors related to the CPU. The dataset contains records of processing time and all the CPU related attributes in simple terms a total of 82 attributes in various timestamps for 2 months in normal time as well as visiting malicious websites. As per the requirement we attempted Genetic Search Algorithm with `cfsSubsetEval` for extracting all the important attributes. After this the dataset is trained with different algorithms and all the algorithms provide 100% accuracy.

3. Genetic Algorithm Architecture

Genetic search algorithms are methods which are used for solving constrained as well as unconstrained optimization problems based on natural

selection, the process refers to the search heuristic approach inspired by Charles Darwin's theory of natural evolution. The approach iteratively modifies the population of a single result. In every step, it selects individuals from the current population as parents and uses them to generate the next generation of offspring. After completion of each successive generation, the population "evolves" toward the ideal solution. Genetic algorithms are applied to solve various optimization problems which include problems where the objective function is discontinuous, non-differentiable, stochastic, or strongly non-linear or in basic terms the problems which don't go with the standard optimization algorithms. Addition to this Genetic algorithm can deal with mixed integer programming problems where some components are constrained to integers.

Genetic algorithms use three major rules in each step in order to create the next generation from the current population.

- First rule is Selection- In this rule some individuals are selected, called parents, whose work is to contribute to the population of the next generation. It is usually a stochastic approach and calculate on the score of an individual.
- The second rule is Crossover in which two parents are combined to create the next generation.
- Third rule is Mutation rules whose job is to make arbitrary adjustments to each parent to create the following generation.

3.1. Working Architecture of Algorithm

Initialization - The system first generates a random base population. The Genetic Algorithm can find a minimum for the `InitialPopulationRange` even if the choice is suboptimal.

Fitness Check - Since initialization is done, we define a fitness coefficient that indicates how well an individual fits out of the population. Here in our dataset `CfsSubsetEval` is used to evaluate the values of the subset of attributes given by the individual predictive ability of each feature and the degree of redundancy between them.

Termination Condition- There are several conditions used by the algorithm to decide when to stop.

- `MaxGenerations`, `MaxTime`, `FitnessLimit`, `MaxStallGenerations`, `MaxStallTime`, `FunctionTolerance`, `ConstraintTolerance`

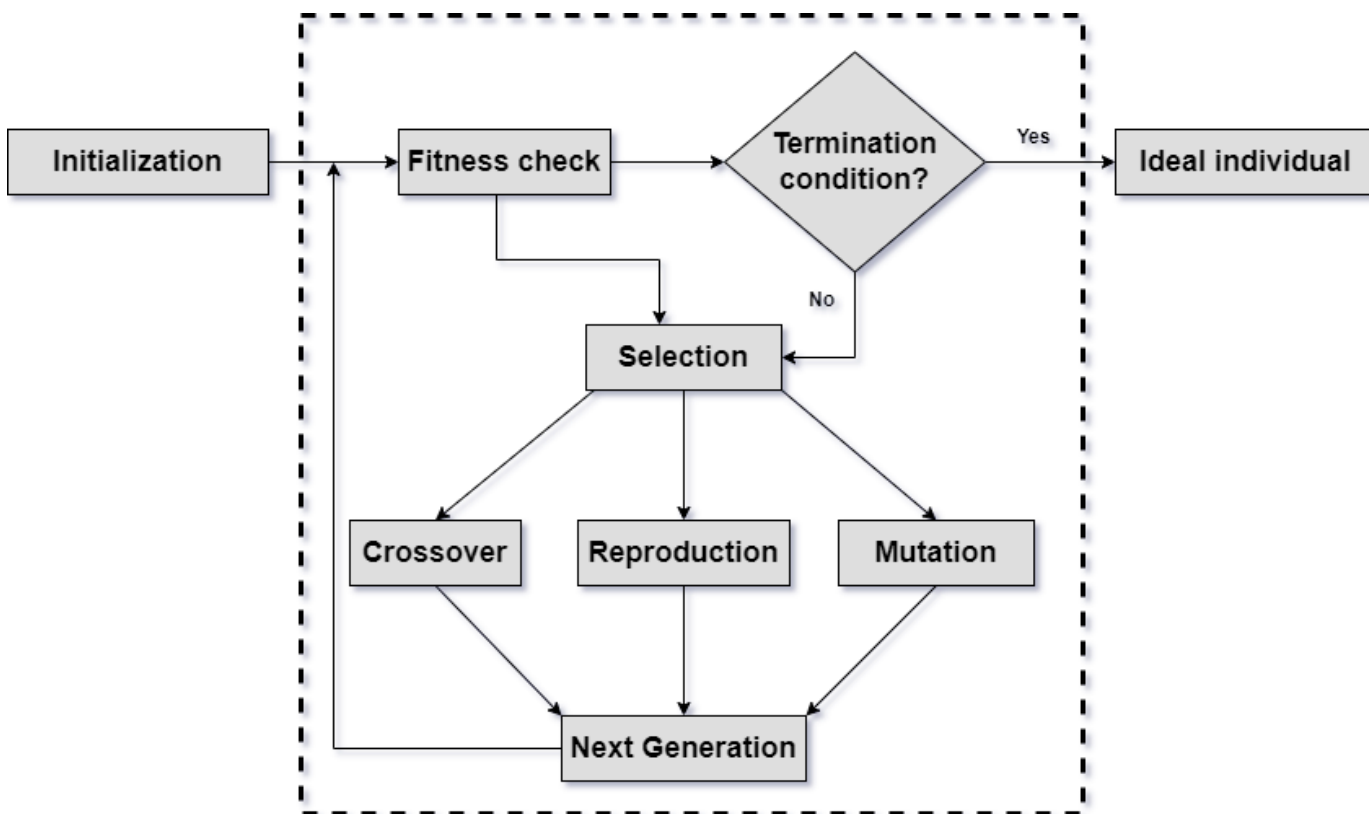


FIGURE 1. Genetic search Algorithm flow diagram

Ideal Individual - In every iteration it will check if the set of attributes are ideal or not. If yes it will return the set, if no it will again iterate.

Selection - As discussed before the selection method selects the next generation parents based on the scaled values from the fitness scaling function. The scaled fitness value is known as expected value. Individuals can be selected as parents’ multiple times; in this case they contribute their genes to multiple children. @selectionremainder is a more deterministic selection option that involves two phases.

- According to the integer portion of everyone’s scaled value, the function deterministically chooses parents in the first step. For example, if a person has a scaling value of 2.3, the function will select that person as her parent twice.

- In the second step, the selection function uses fractions of the scaled values to select additional parents, like probabilistic uniform selection. This function creates a line with sections of varying lengths corresponding to the proportions of the individual scaled values, moving evenly along the line to select the parent. Note that the choice is fully deterministic when the scaled value has all 0s in the fractional part, as is the case with top scaling.

Reproduction - The task of the reproduction method is to control genetic algorithm in creating the next generation. This can be implemented by two ways:

- **EliteCount** — The number of characteristics from the current generation that are guaranteed to persist into the following one. These people are considered privileged children. For each generation, the best fitness score will drop if EliteCount is higher than or equal to 1. It is claimed that this occurs because of the genetic algorithm’s reduction of the fitness function. The population’s concentration of highly qualified people can cause searches to be less successful when EliteCount is set to a high number.
- **CrossoverFraction** - Fraction of the next generation of attributes created by crossover, excluding elite children.

Mutation & Crossover - Genetic algorithms use the current generation of individuals to create the next generation of children. In addition to elite children the algorithm creates

- Crossover children by selecting vector entries or genes from pairs of current generation individuals and combining them to form a single child.
- Children are mutated by making random mod-

ifications to one person from the current generation to create the child.

These procedures are crucial for genetic algorithms because they enable Crossover, which enables algorithms to take the finest genes from several people and mix them to create possibly superior offspring.

Mutations add diversity to the population to increase the likelihood so that the algorithm will generate individuals with better fitness scores.

Next Generation - The selected attributes after each iteration.

4. Methodology

The motivation behind our dissertation is to get a proper knowledge about the metrics of a processor when it is operated at normal state and during attack of cryptojacking. After reviewing and shuffling through many datasets and research materials we went for a dataset which contains all the necessary metrics which can lead us to draw conclusions i.e., memory used by every platform, RAM, Usage time of each app, Storage used, Processing time, IP addresses connected by the server etc.

4.1. Proposed Method

The proposed method is shown in Figure 2.

4.2. Implementation Steps

Step 1: Raw Dataset:

Time-series unlabelled dataset of CPU load, Memory etc. at normal state and during cryptojacking activities performed

Step 2: Data Preparation:

- Classified the data with 'flag' attribute where normal dataset (i.e., data captured at normal state) was flagged to '0' and abnormal dataset (i.e., data captured during cryptojacking) was flagged to '1' and then we combined the data.

- The dataset then was checked for null values. The rows with null or blank values were dropped.

Step 3: Pre-processing:

- Data sampling: Reducing a part of data to use specific data specially for numerical data.
- Data transformation: Sklearn.preprocessing.normalize implemented to scale and normalize the data to remove

biasing caused due to uniform distribution of weights by the data.

- Data segregation: Splitting dataset for train and test.

Step 4 : Feature Selection:

To create the comparative study, we used the learning machine tool Weka (3.7.8). Various feature selection approaches are combined and tested in this work, including BestFirst + CfsSubsetEval, GeneticSearch + CfsSubsetEval, GreedyStepwise + CfsSubsetEval, LinearForwardSelection + CfsSubsetEval, SubsetSizeForwardSelection + CfsSubsetEval, ScatterSearch+CfsSubsetEval.

Implemented GeneticSearch + CfsSubsetEval which resulted in selection of 31 attributes from 83 attributes to proceed further as the genetic search algorithm finds the best suitable attributes on which the whole selection process can rely on.

Step 5: Train the model:

Supervised machine learning methods were implemented i.e., Support Vector Machine (SVM), Logistic regression, Decision Tree classifier, Random Forest Classifier and Multi-layer Perceptron classifier (MLPClassifier) from the neural networks.

Step 6: Analysis:

Checking Accuracy, Precision, Specificity and Sensitivity for the above-mentioned techniques with each classification Algorithm.

4.3. Pseudocode

The Pseudocode for the classification models are shown in figure 4.

5. Results and Discussion

This section describes the results presented in this paper. Our solution turned out to be very effective in finding the most used attributes in cryptojacking. We used Weka software for various feature selection techniques to select the best set of attributes. For the comparison we use various types of classifiers and measure the Accuracy, Precision, Specificity and Sensitivity.

provides the accuracy of each Feature Selection Technique with 6 different Classifiers and as the result shows only the attributes selected by Genetic Search Algorithm can provide 100% accuracy with every classifier. It represents that the model can make correct predictions of the test set provided

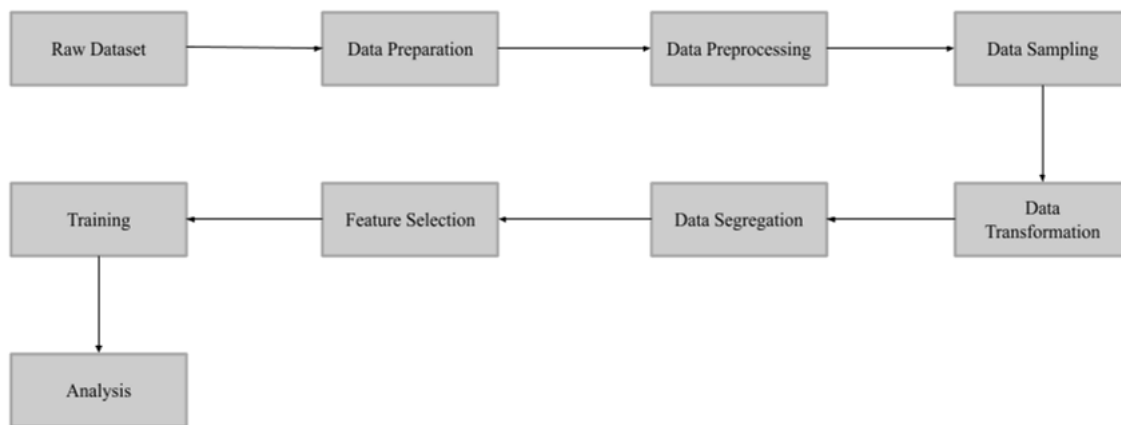


FIGURE 2. Block Diagram

cpu_guest	cpu_guest_nice	cpu_idle	cpu_iowait	cpu_irq	cpu_nice	cpu_softirq	cpu_steal	cpu_system	cpu_total	...	processcount_sleeping	processcount_thread	processcount_total	system_hostname	system_hr_name	system_linux_distro	system
0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	5.0	100.0	--	120.0	155.0	122.0	vm1-graph-analytics	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	5.5	100.0	--	120.0	155.0	122.0	vm1-graph-analytics	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	5.5	100.0	--	120.0	155.0	122.0	vm1-graph-analytics	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
3	0.0	0.0	0.0	0.0	0.0	0.0	0.0	4.3	100.0	--	120.0	157.0	122.0	vm1-graph-analytics	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	5.0	100.0	--	120.0	155.0	122.0	vm1-graph-analytics	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
80846	0.0	0.0	91.7	0.0	0.0	0.0	0.0	2.8	9.9	--	101.0	145.0	103.0	vm4-web-server	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
80847	0.0	0.0	88.4	0.0	0.0	0.0	0.9	4.5	10.0	--	102.0	146.0	104.0	vm4-web-server	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
80848	0.0	0.0	91.7	0.0	0.0	0.0	0.0	2.8	9.1	--	102.0	146.0	104.0	vm4-web-server	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
80849	0.0	0.0	92.6	0.0	0.0	0.0	0.0	2.0	0.3	--	102.0	146.0	104.0	vm4-web-server	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	
80850	0.0	0.0	91.7	0.0	0.0	0.0	0.0	2.8	7.5	--	102.0	146.0	104.0	vm4-web-server	CentOS Linux 7.7.1908 64bit	CentOS Linux 7.7.1908	

FIGURE 3. Data Set

```

model1 = svm.SVC(kernel='linear',gamma='auto', C = 2)
model2 = svm.SVC(kernel='rbf')
model3 = LogisticRegression()
model4 = DecisionTreeClassifier()
model5 = RandomForestClassifier()
model6 = MLPClassifier(solver='lbfgs', alpha=1e-5,hidden_layer_sizes=(10, 10,2), random_state=0)

model1.fit(X_train,y_train)
model2.fit(X_train,y_train)
model3.fit(X_train,y_train)
model4.fit(X_train,y_train)
model5.fit(X_train,y_train)
model6.fit(X_train,y_train)
  
```

FIGURE 4. Classification Models

based on the training set. If there is any change to the splitting function, the model can't provide the exact result.

provides the sensitivity of each Feature Selection Technique with 6 different Classifiers and as the result shows only the attributes selected by Genetic Search Algorithm is able to provide 100% sensitiv-

ity with every classifier. It represents that the dataset doesn't contain any false negative values.

provides the specificity of each Feature Selection Technique with 6 different Classifiers and as the result shows only the attributes selected by Genetic Search Algorithm can provide 100% sensitivity with every classifier. It represents that the dataset doesn't

TABLE 1. Accuracy of different classifiers for different feature selection techniques

Classifiers	Feature Selection Techniques					
	Best-First + CfsSubsetEval	Genetic-Search + CfsSubsetEval	GreedyStepwise + CfsSubsetEval	LinearForwardSelection + CfsSubsetEval	SubsetSizeForwardSelection + CfsSubsetEval	ScatterSearch + CfsSubsetEval
Support Vector Machine (kernel = "linear")	100%	100%	100%	100%	100%	100%
Support Vector Machine (kernel = "Radial Bias Function")	100%	100%	100%	100%	100%	95.05%
Logistic Regression	100%	100%	100%	100%	100%	100%
Decision Tree Classifier	100%	100%	100%	100%	100%	100%
Random Forest Classifier	100%	100%	100%	100%	100%	100%
Multi-layer Perceptron	84.87%	100%	84.87%	84.87%	84.87%	84.84%

contain any false positive values

provides the confusion matrix of Genetic Search Algorithm with 6 classifiers in 3 different split ratios of training and testing dataset. In all the three metrics the value of FP and FN is 0, which means that the test is 100% perfect.

5.1. Area Under the Curve

AUC (Area Under the Curve) is a commonly used measure of classification performance that is preferred for two main reasons. Firstly, it is scale invariant, meaning that it assesses how well the predictions are ranked rather than their absolute values, which makes it more robust and less sensitive to changes in the data. Secondly, AUC is classification-threshold-invariant, meaning that it measures the quality of a model’s predictions irrespective of the specific classification models.

AUC curve of Genetic Search Algorithm is 1 for every classification threshold which represents

That the predictions or the testing are 100% correct.

5.2. Selected Attributes

The attributes selected by Genetic Search Algorithm are shown in Figure 7.

6. Conclusions

As cryptojacking becomes increasingly central with advancements of technology, it is very much important to have good knowledge of websites and different platforms.

1. Avoid visiting pirated websites. Before visiting any website, check whether it is secure or not. A secure URL always begins with “HTTPS” at the start instead of “HTTP”. The ‘S’ in HTTPS is for “SECURE” which shows if a website is SSL certified or not.

2. When browsing through websites, agreeing to cookies is a part of it so whenever browsing a website always go through the description of the cookies permissions manually and select them. Also read the documentation whether it’s performance, preference cookies which helps you to have a better experience on the website and what kind of data it will be using.

3. Use security tools like antivirus to evaluate the site. Do proper research about the company online before selecting an antivirus. One can test with Google Safe Browsing. It has the advantage of using Google’s database, which produces an examination of billions of pages and increases the likelihood of discovering dangerous websites or attempts to steal information from these domains. Installing

TABLE 2. Sensitivity of different classifiers for different feature selection techniques

Classifiers	Feature Selection Techniques					
	BestFirst + CfsSubsetEval	GeneticSearch + CfsSubsetEval	GreedyStepwise + CfsSubsetEval	LinearForwardSelection + CfsSubsetEval	SubsetSize + CfsSubsetEval	ForwardSelection + CfsSubsetEval
Support Vector Machine (kernel = "linear")	100%	100%	100%	100%	100%	100%
Support Vector Machine (kernel = "Radial Bias Function")	100%	100%	100%	100%	100%	95.15%
Logistic Regression	100%	100%	100%	100%	100%	100%
Decision Tree Classifier	100%	100%	100%	100%	100%	100%
Random Forest Classifier	100%	100%	100%	100%	100%	100%
Multi-layer Perceptron	84.87%	100%	84.87%	84.87%	84.87%	49.86%

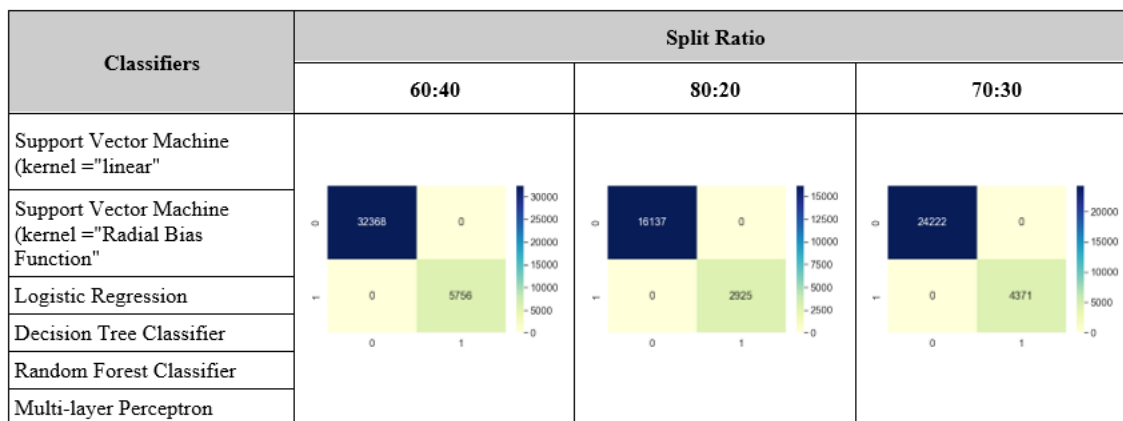


FIGURE 5. Confusion Matrix of different classifiers at different training split

good antivirus helps in preventing data breaching and blocking many malicious websites or pages as many websites try to download corrupted files in the system

4. Analyse if the website has a modern theme. According to an article published by G1 in 2020, over a million WordPress websites may be suscepti-

ble due to some plugins and themes. Avoid using or visiting pirated themes websites. Although it resembles the originals exactly, using them is the same as leaving a door open for the invaders

5. Verify the URL first and learn about how criminals take advantage of people’s lack of attention to detail when using scams. They purposely cre-

TABLE 3. Specificity of different classifiers for different feature selection techniques

Classifiers	Feature Selection Techniques					
	Best-First + CfsSubsetEval	Genetic-Search + CfsSubsetEval	GreedyStepwise + CfsSubsetEval	LinearForwardSelection + CfsSubsetEval	SubsetSizeForwardSelection + CfsSubsetEval	ScatterSearch + CfsSubsetEval
Support Vector Machine (kernel = "linear")	100%	100%	100%	100%	100%	100%
Support Vector Machine (kernel = "Radial Bias Function")	100%	100%	100%	100%	100%	93.90%
Logistic Regression	100%	100%	100%	100%	100%	100%
Decision Tree Classifier	100%	100%	100%	100%	100%	100%
Random Forest Classifier	100%	100%	100%	100%	100%	100%
Multi-layer Perceptron	0.00%	100%	0.00%	0.00%	0.00%	98.45%

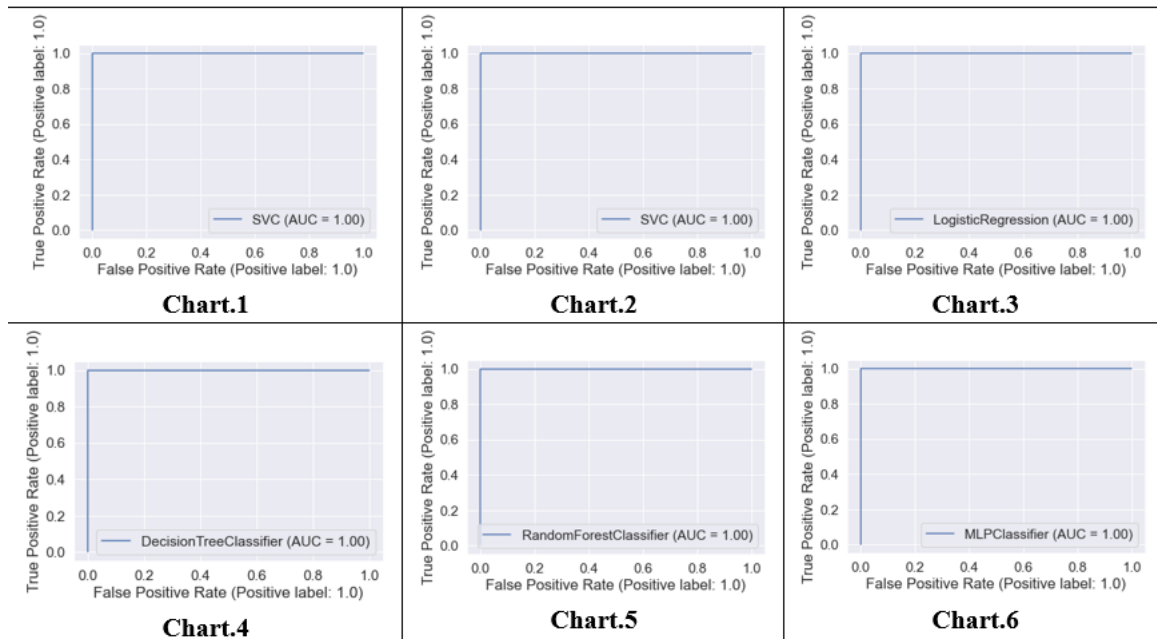


FIGURE 6. AUC of different classifiers for Genetic Search Algorithm

ate fraudulent websites with common spelling errors or grammatical mistakes in the web address that go unnoticed by the consumer, making it easier to deceive and steal from them. For example, changing an "o" to a zero in a web address. The warning specifically mentions the possibility of someone creating a fraudulent website that resembles the real

Google website,

6. Verify the authenticity of security seals on websites. While many companies provide security stamps to certify websites, it is possible for scammers to create fake ones using editing software. To avoid falling for such scams, it is recommended to click on the seal and check if it directs to the com-

- cpu_idle, cpu_iowait, cpu_nice, cpu_softirq, cpu_system, cpu_user
- diskio_sda1_read_bytes, diskio_sda1_time_since_update, diskio_sda1_write_bytes, diskio_sda_read_bytes, diskio_sda_write_bytes
- fs / _device_name, fs / _percent, fs / _size
- load_min1, load_min5
- mem_buffers, mem_percent, mem_shared
- memswap_free, memswap_percent, memswap_sin, memswap_sout, memswap_total, memswap_used
- network_lo_cumulative_cx, network_lo_cumulative_rx, network_lo_cumulative_tx, network_lo_cx, network_lo_rx, network_lo_tx
- percpu_0_cpu_number, percpu_0_guest_nice, percpu_0_iowait, percpu_0_irq, percpu_0_softirq
- processcount_running, processcount_sleeping, processcount_thread
- flag

FIGURE 7. Attributes selected by Genetic Search Algorithm

pany's official website or provides additional information to verify its authenticity. Additionally, one can use the Google badge to verify the legitimacy of the certificate.

7. Escape spam. Some websites use some scams, such as banners that blink ceaselessly, overstated claims, or extremely low product pricing, are common warning signs that a website, email, or advertisement is unsafe. There are still people who disregard features and believe websites that employ these techniques, even though they appear to be from the 1990s and 2000s.

8. Always check system usage regularly to avoid any kind of unknown activities operating on the device. If any unknown application is present on the device, make sure to remove it. Always install software's from genuine sources.

By testing the effect of different types of cryptojacking attacks it is established that it can affect the CPU at a very high level, it can lower down the performance of CPU leading to data loss. Therefore, it is very important to go through the safety measures.

ORCID iDs

Ayush Kumar Bar  <https://orcid.org/0000-0003-3050-6478>

References

- Cado Security. "Tales From the HoneyPot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack." *Tales From the HoneyPot: WatchDog Evolves With a New Multi-Stage Cryptojacking Attack - Cado Security — Cloud Investigation* (2022).
- Chharit. "Cryptojacking Analysis and Problem Clustering". (2019). <https://www.kaggle.com/code/chharit/cryptojacking-analysis-and-problem-clustering/data>.
- CoinDesk. "Ether Touches \$500B Market Cap for First Time, Overtaking JPMorgan and Visa". (2021). <https://www.coindesk.com/markets/2021/05/12/ether-touches-500b-market-cap-for-first-time-overtaking-jpmorgan-and-visa/>.
- Ganepola, Dasuni and Hasini Bandara. "A Systematic Review and Comparative Study of Cryptojacking Detection via Machine Learning". Dec. 2021.
- India., Outlook. "Cryptojacking Cases Are Rising Globally: Why So and Should This Worry You? Outlook India. " (2022). <https://www.outlookindia.com/business/cryptojacking-cases-are-rising-globally-why-so-and-should-this-worry-you--news-212990>.

Miele, Gianfranco and Octavian Postolache. "Special Section on the 2019 IEEE Measurement and Networking Symposium, Catania, Italy, July 8–10, 2019". *IEEE Transactions on Instrumentation and Measurement* 69.10 (2020): 7979–7981.

Networks, Palo Alto. "Stopping Cryptojacking Attacks With and Without an Agent." *Stopping Cryptojacking Attacks With and Without an Agent - Palo Alto Networks Blog* (2018).

nukala, Venkata Sai Krishna Avinash. "Website cryptojacking detection using machine learning". *University of Cincinnati* (2021). https://etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=ucin1627667523933195%5C&disposition=inline.

S, Norman Xavier, and V Sahni. "Machine Learning Approaches to Detect Browser-Based Cryptomining MSc Internship MSc in Cyber Security Machine Learning Approaches to Detect Browser-Based Cryptomining". (2020). <https://www.cyberthreatalliance.org/wp->

"Threat Horizons Executive Snapshot". *Copy of Threat Horizons Executive Snapshot* (2021).



© Ayush Kumar Bar et al. 2023 Open Access.

This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Embargo period: The article has no embargo period.

To cite this Article: , Ayush Kumar Bar, Akankshya Rout , and Ankush Kumar Bar . "Cryptojacking Detection Using Genetic Search Algorithm." *International Research Journal on Advanced Science Hub* 05.04 April (2023): 119–129. <http://dx.doi.org/10.47392/irjash.2023.025>