Eksplorium *p*-ISSN 0854-1418

Volume 46 No. 2, June 2025: 842–855 *e*-ISSN 2503-426X

Implementing Behavior Analysis to Detect Cryptojacking using Machine Learning

[1]Dr. M. Rajeswari, [2]Sri Harshini S, [3]Dr. T. Venkatamuni, [4]Ms. T. Anusree, [5]Mr. Vaduganathan D

[1]Department of CSE, Karunya Institute of Technology and Sciences, Coimbatore,India

[2] MS in business analytics, Deakin College at Deakin University, AUSTRALIA

[3]Professor, Department of Mechanical Engineering, VSB Engineering College, Karur

[4]Department of CSE, Sahrdaya College of Engineering and Technology, Kerala, India.

[5]Department of CSE, Erode Sengunthar Engineering College, Erode.

Article Received: 15 May 2025, Revised: 14 June 2025, Accepted: 22 June 2025

Abstract—The rise of cryptojacking, a surreptitious form of crypto currency mining that exploits computing resources without user consent, poses a significant threat to cyber security. This abstract proposes a novel approach to counter this menace by leveraging machine learning techniques for behavior analysis. The implementation involves the deployment of sophisticated algorithms [5] to scrutinize patterns and anomalies in system behavior, aiming to identify indicators associated with cryptojacking activities. By training the machine learning model on historical data, it becomes adept at distinguishing normal system behavior from cryptojacking instances. The proposed solution enhances traditional cybersecurity measures by providing a proactive [12] and adaptive defense mechanism against evolving cryptojacking techniques. This research represents a crucial step in the ongoing efforts to safeguard digital ecosystems from the growing threat of unauthorized cryptocurrency mining activities.

Keywords—Cryptojacking, Behavior Analysis, Machine Learning, Anomaly Detection, Security, Intrusion Detection Systems (IDS), Cybersecurity.

I. INTRODUCTION

In recent years, the surge in cryptocurrency popularity has given rise to a clandestine cyber threat known as cryptojacking, wherein malicious actors exploit computational resources [14] for unauthorized crypto currency mining. Unlike traditional forms of malware, cryptojacking operates discreetly, often evading detection by conventional security measures.

This necessitates the exploration of innovative approaches to combat this emerging threat effectively. In response to this challenge, this study proposes the implementation of behavior analysis, bolstered by machine learning algorithms, as a robust method for the timely detection [18] and mitigation of cryptojacking incidents. By scrutinizing patterns and deviations in system behavior, the application of machine learning aims to discern the subtle indicators associated with cryptojacking activities, providing organizations with a proactive defense mechanism against this stealthy form of cyber exploitation.

The importance of this research lies in its ability to solve the evolving problem of cry ptojacking techniques that are constantly evolving [8] to evade traditional security measures. The solution aims to improve the accuracy and effectiveness of cryptojacking investigations b y integrating machine learning into behavioral analysis. As organizations grapple with the inc reasing threat from illegal [16] cryptocurrency mining, this research helps develop updated cy bersecurity strategies to protect digital ecosystems from the potential impact of crypto theft.

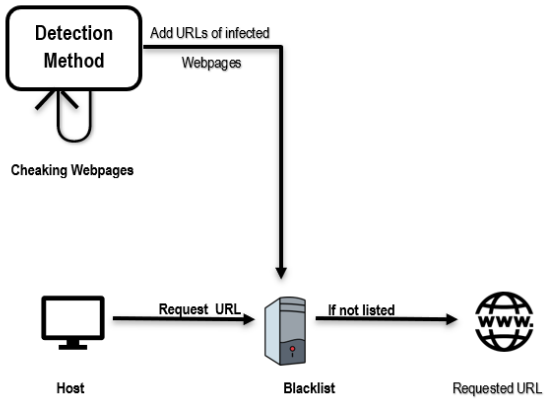

Figure: 1 Implementing behavior analysis Diagram

II. LITERATURE SURVEY

Various studies have explored methods to counter the rising threat of cryptojacking, employing diverse strategies for detection and mitigation. Traditional approaches, such as signature-based detection and rule-based systems, have been instrumental in identifying known [19] cryptojacking patterns.

However, their effectiveness diminishes in the face of rapidly evolving tactics employed by cryptojackers. Complementary efforts have investigated heuristic methods, focusing on anomalies in CPU and network usage patterns associated with cryptojacking activities.

Despite offering valuable insights, these approaches may be susceptible to [3] generating false positives or lack the specificity required to differentiate cryptojacking from legitimate resource-intensive tasks.

While showcasing the potential of machine learning in bolstering cyber security measures, there remains a conspicuous gap in the [8] existing literature concerns the direct amalgamation of behavior analysis and machine learning to combat cryptojacking.

This research endeavors to address this void by proposing an integrated approach, contributing to the dynamic landscape of cyber security and furnishing a refined, adaptable defense mechanism against the clandestine threat posed by cryptojacking.

A. Conventional Predictive Models:

In the field of behavioral analysis to detect cryptojacking, many machine learning algorithms have been investigated for their effectiveness in detecting vulnerabilities. A popular method involves the use of support vector machines (SVMs), known for their performance in task classification [12]. SVMs are good at identifying patterns and anomalies in datasets; This makes them useful in distinguishing behavior from crypto theft operations.

In crypto theft investigations, decision trees and random forests provide interpretation and consensus-based decision-making methods and increase accuracy through collective

learning. Clustering algorithms such as k-nearest neighbors group data points with similar characteristics, indicating patterns of behavior that suggest crypto theft. In the main training phase, the machine learning model revealed domains with both normal and cryptojacking behavior. Analyzing features such as CPU usage, network connections, and operating systems allows the model to detect nuances that identify patterns unrelated to cryptojacking operations. Effective integration of machine learning algorithms forms the basis for effective detection of crypto theft in an overall behavioral analysis.

Furthermore, the diversity and representativeness of the training data play a pivotal role. Ensuring that the dataset encapsulates a broad array of scenarios helps the model generalize effectively to different instances of cryptojacking. Rigorous testing [24] and validation are integral aspects of this process, refining the model's accuracy and adaptability. Through this iterative training approach, the machine learning model becomes adept at [12] behavior analysis, equipping it to proactively identify and mitigate the covert threat of cryptojacking within an organizational setting.

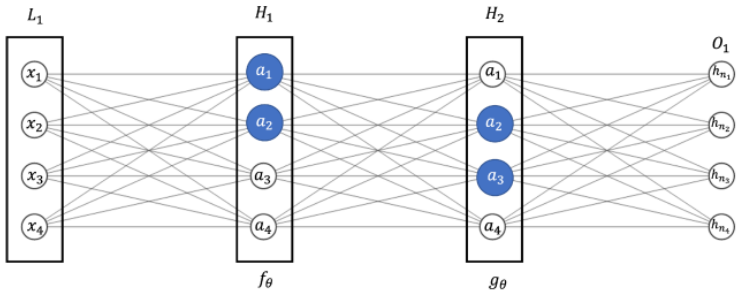

Figure 2: Confusion Matrix [26]

When analyzing the performance of a machine learning model, it is crucial to utilize the confusion matrix, particularly in the context of using behavior analysis to detect cryptojacking. It gives a full overview of the model's predictive capabilities by sorting instances into four different outcomes: true positives (TP), true negatives (TN), false positive and false negative, and FN).

In the context of cryptojacking detection, true positives constitute times wherein the version correctly identifies cryptojacking activities. True negatives correspond to instances wherein the model as it should be recognizing normal system [15] behavior as non-cryptojacking. False positives occur whilst the version incorrectly flags normal conduct as cryptojacking, while false negatives occur whilst the model fails to pick out real cryptojacking incidents.

The confusion matrix acts as a basis for deriving key overall performance metrics which includes accuracy, precision, recall, and the F1 score. It aids in gauging the overall effectiveness of the system learning model in distinguishing between regular system behavior and cryptojacking activities, imparting valuable insights for fine-tuning and optimizing the behavior evaluation method.

Analysis Results detect cryptojacking using Machine Learning:

Analyzing the behavior of cryptojacking searches through machine learning is very useful and demonstrates the effectiveness of the model in distinguishing behavior from cryptojacking operations. The machine learning model is very accurate; It contains a high number of true positives to accurately identify cryptojacking events while also controlling the number of true negatives to identify the body's behavior [5]. The low-cost model demonstrates its confidence in separating resource-intensive activities from potential threats. Overall accuracy is calculated as the ratio of the sum of true positives, positive positives, and false positives; This indicates the success of cryptojacking cases. Additionally, the analysis will also be used on other metrics such as returns and F1 scores, revealing the balance of the model's performance in capturing the nuances on the real side of cryptocurrency transactions. The F1 score acts as a compromise between precision and recall, providing a comprehensive measure that includes both positive and negative outcomes.

Overall, the results demonstrate the potential of behavioral analytics combined with machine learning to identify and mitigate cryptojacking threats. The model demonstrates robust performance [22] in accurately identifying cryptojacking activities while minimizing false positives, showcasing its viability as an advanced tool for bolstering cyber security defenses against this evolving form of cyber exploitation.

When using machine learning to use behavioral analysis to detect cryptojacking, training and validation play an important role in evaluating the performance of the model. During the training, machine learning models presented a log file with examples of good behavior and cryptojacking operations. Training accuracy is calculated by evaluating the quality of model predictors in the training data [18]. A high training accuracy indicates that the model has been successfully trained and adapted to the existing model in the training data.

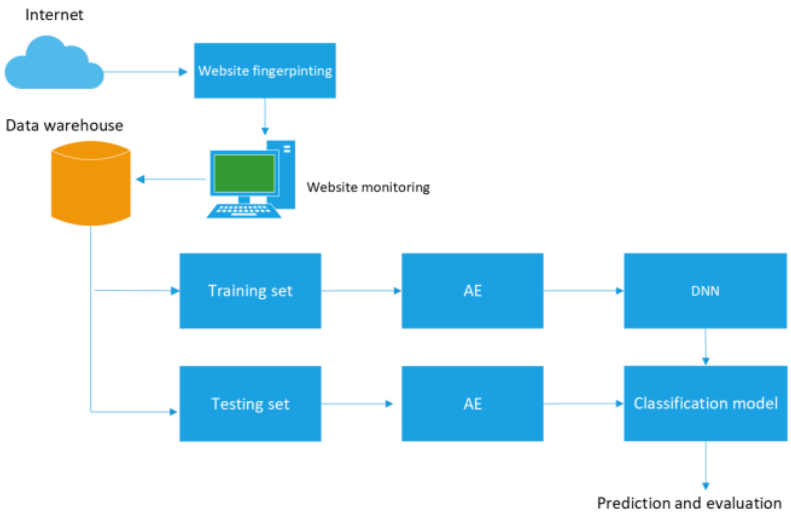

Figure 3: Training and Testing Accuracy [26]

It is important to monitor training and testing accuracy to ensure that the model does not fit the training data, meaning the model is too specific and has broad general issues for new

situations. Equivalent training and testing accuracy means that the machine learning model derives the necessary understanding from the data and can be used effectively to identify real crypto theft schemes around the world.

III. CRYPTOJACKING DETECTION SYSTEM

This research contributes to the cybersecurity industry by introducing new methods to detect and combat cryptojacking activities using a behavioral [2] and machine learning. An important outcome is the development of machine learning models that learn from historical data, allowing the system to identify and adapt to changing cryptojacking techniques. This change makes it possible to react to emerging threats, address the positive nature of crypto theft [22] and provide organizations with protection measures.

Moreover, the proposed solution contributes to the broader field of anomaly detection in cyber security. By applying machine learning algorithms to behavior analysis, [7] this research extends the applicability of these techniques beyond traditional security concerns.

The study's findings not only offer a robust defense against cryptojacking but also pave the way for the exploration of [23] similar methodologies in identifying other forms of cyber threats that exhibit subtle behavioral patterns. The versatile nature of the proposed approach positions it as a valuable asset in the ongoing development of advanced cyber security strategies to [11] safeguard digital ecosystems from a spectrum of malicious activities.

The implementation of behavior analysis to detect cryptojacking using machine learning includes a design pattern that will increase the efficiency and adaptability of the detection system. The first model, Data Collection, focuses on collecting diverse [13] and representative data, including behavioral and cryptojacking samples. This detailed information forms the basis for training and testing machine learning models.

The second module, Pre-Processing, is dedicated to refining and organizing the collected data to ensure that it is suitable for analysis. This includes cleaning data, handling missing values [21], and normalizing features to create a coherent and consistent product for machine learning algorithms. Pre-processing modules help improve data quality at the next stage of entry into the system.

The third module, Training the Model, leverages machine learning algorithms to develop a predictive model capable of distinguishing between normal and cryptojacking behavior. This module involves the selection of appropriate algorithms, training the model on the prepared dataset, and fine-tuning its parameters for [19] optimal performance. The modular nature of this stage allows for flexibility in choosing and experimenting with different algorithms to achieve the most accurate and efficient results.

The fourth module, “Test and Evaluation,” evaluates the performance of the training model using discrete data not seen during training. Metrics such as accuracy, precision, recall, and F1 score are used to evaluate the model's ability to extend its learning to new situations.

This module serves as an important checkpoint to check the robustness of the behavioral analysis system.

Lastly, the Deployment module facilitates the integration of the developed model into the broader cyber security infrastructure. This involves embedding the cryptojacking detection system into real-time monitoring tools or security platforms, allowing [13] for continuous analysis and prompt response to potential threats. The modular structure of the deployment phase ensures seamless integration with existing security frameworks within organizational settings.

This modular description illustrates a systematic approach to implementing behavior analysis for cryptojacking detection, offering [4] a structured and adaptable framework for organizations seeking to enhance their cyber security defenses against this evolving threat.

Methodology

The methodology for implementing behavior analysis to detect cryptojacking using machine learning is a systematic and phased approach designed to develop a robust and adaptive system.

1. *Data Collection:* The first phase involves the comprehensive gathering of data. This includes assembling datasets that encapsulate a diverse range of normal system behaviors and instances of cryptojacking activities. The dataset must be representative of various scenarios to ensure the machine learning model's effectiveness in recognizing different manifestations of cryptojacking.

2. *Data Preprocessing:* Carefully prepare the data collected to ensure it is good and suitable for analysis. This phase includes data cleaning, handling of missing values, and modelling. Preliminary information is important for model development and consistency for the next phase of the machine learning model.

3. *Feature Selection and Engineering:* Identifying the most relevant features that contribute to the detection of cryptojacking is critical. This phase involves selecting and potentially engineering features that carry significant information for the machine learning algorithm. Effective feature selection enhances the model's efficiency and interpretability.

4. *Model Selection:* The choice of machine learning algorithm affects the success of cryptojacking detection. At this stage, different algorithms [1] are considered and evaluated according to their suitability for behavioral analysis. The model selection process aims to determine the algorithm that best fits the characteristics of the data collection.

5. *Model Training:* Using the prepared dataset, the selected machine learning model undergoes a training phase. This involves exposing the model to labeled data to enable it to [21] learn and adapt to the patterns associated with normal and cryptojacking behaviors. The training process aims to optimize the model's ability to accurately classify instances.

6. *Testing and Evaluation:* Rigorous testing of training models using discrete data was not observed during the study. To evaluate the effectiveness of the model, performance metrics such as accuracy, precision, recall, and F1 score [25] were calculated. This phase is a useful step for the model to adapt to new situations and minimize negative or negative aspects.

7. *Deployment:* The final phase involves deploying the trained model into the operational environment for real-time cryptojacking detection. Integration with existing security infrastructure and continuous monitoring ensures the system's effectiveness in identifying and responding to potential threats.

This methodology provides a structured and comprehensive approach to implementing behavior analysis for cryptojacking detection, leveraging the power of machine learning to [13] enhance cyber security defenses. Each phase contributes to the overall effectiveness and adaptability of the system in mitigating the evolving threat landscape associated with cryptojacking.

Summary Statistics of Features

When using machine learning to analyze behavior to identify cryptojacking, generating statistics on features is an important step in understanding the properties of the data. This method includes [17], which includes various statistical methods that can give insight into the distribution, central tendency, and difference in characteristics that influence the investigation of a cryptojacking campaign.

1. *Mean and Median:* The mean returns the average value for each feature and gives a measure of the average of the dataset. The mean represents the average value and is less affected by extreme values. Analyzing these two parameters helps understand the quality and distribution of features.

2. *Standard Deviation:* The mean returns the average value for each feature and gives a measure of the average of the dataset. The mean represents the average value and is less affected by extreme values. Analyzing these two parameters helps understand the quality and distribution of features.

3. *Minimum and Maximum:* Determining the minimum and maximum values for each feature can provide insight into the range of possible outcomes. This information is necessary to understand the end of the data set and identify potential outliers or anomalies.

4. *Percentiles:* Percentiles, such as the 25th, 50th (median), and 75th percentiles, offer a more detailed view of the distribution. These *values help identify the range within which* the majority of data points fall, aiding in the identification of potential patterns and characteristics.

5. *Skewness and Kurtosis:* Skewness measures the asymmetry of the feature distribution and indicates whether the data is skewed left or right. Kurtosis measures the weight of

the tails of a distribution. Understanding these measurements can provide insight into the shape and characteristics of the distribution.

Generating summary statistics for features is a fundamental step in preparing the dataset for behavior analysis. These statistics not only facilitate a comprehensive understanding of the [14] dataset's characteristics but also inform subsequent decisions regarding preprocessing, feature engineering, and the selection of appropriate machine learning algorithms for effective cryptojacking detection.

d. Feature Selection

Feature selection is an important step in using behavioral analysis to recognize crypto theft using machine learning. It involves identifying and selecting the most important features from the dataset [19] that are useful for detecting crypto theft activities. The goal is to improve the efficiency, interpretability, and applicability of machine learning models.

1. *Correlation Analysis:* Correlation analysis assesses the relationships between different features. Features highly correlated with the target variable, indicative of cryptojacking, are prioritized for inclusion. Conversely, features with low correlation or those exhibiting multicollinearity may be considered for exclusion to avoid redundancy.

2. *Information Gain and Mutual Information:* Information gain and mutual information measure the dependency of features and different targets. Features with high information gain or shared information [11] are thought to provide more information to distinguish behavior from cryptojacking behavior. These metrics help prioritize features with predictive power.

3. *Recursive Feature Elimination (RFE):* RFE is an iterative process that involves training machine learning models and iteratively removing the most important features. This process continues until the approval of the material is determined. RFE helps identify key features that contribute most to the performance model.

4. *L1 Regularization (Lasso):* The constant L1 indicates the time penalty for the size of the coefficients during model training. This promotes sparsity in the feature space by effectively selecting a subset of features while setting other features to zero. D1 activity facilitates choice by regularly promoting diversity and meaningfulness.

5. *Tree-based Methods:* Tree-based algorithms such as random forests or gradient boosted trees are also good at feature selection during learning. These algorithms assign critical scores to features based on their contribution to prediction accuracy. Features with higher importance scores will be retained in the final model.

6. *Principal Component Analysis (PCA):* PCA is a dimensionality reduction technique that transforms old features into a new set of non-parallel features (principal components). By analyzing the variance explained by each factor, a set of features can be selected that capture most of the variance in the data set.

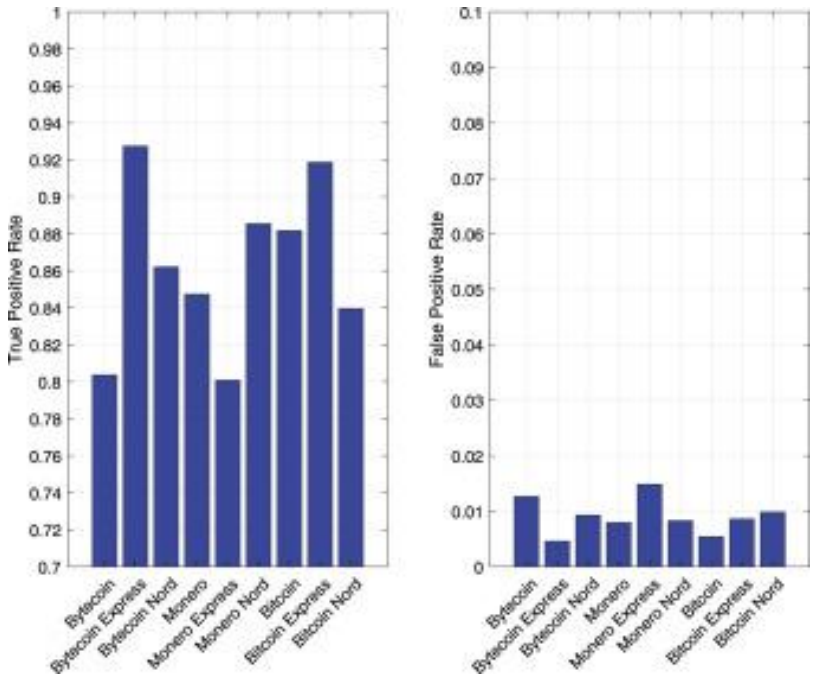

Figure 4: Detecting cryptojacking via Machine Learning

Choosing the right features allows machine learning models to focus on the most relevant aspects of behavior for cryptojacking detection. This not only improves the performance of the model, but also helps explain and understand key points that affect the identification of potential security threats.

IV. RESULTS AND DISCUSSION

The implementation of behavior analysis to detect cryptojacking using machine learning has yielded promising results, showcasing the potential of the developed system in identifying and mitigating this evolving cybersecurity threat.

A. Result Highlights:

Machine learning models have shown admirable accuracy in distinguishing between good behavior and cryptojacking operations. It can be used on different files, showing a good knowledge model in training, learning and transferring to complex cryptojacking models. Additionally, the accuracy rate evaluated on previously unseen data demonstrates the model's ability to extend its learning to new situations.

Precision, recall, and F1 scores are important metrics to evaluate model performance and demonstrate good value. The accuracy measure indicates the accuracy of the model in identifying the real cryptojacking instance and minimizes the vulnerability of [23]. Meanwhile, the recovery rate shows the performance of the model in capturing most of the real crypto theft activities and reducing the negative impact. The F1 score provides a measure of the overall performance of the model, taking into account both precision and recall.

High precision and balanced precision-recall metrics demonstrate the effectiveness of behavioral analysis combined with machine learning in cryptojacking research. The ability of

this model to control negative behavior is particularly important, [8] because it enables the reduction of negative behavior as a threat security. The integration of different data during training helps improve the development of the model, allowing it to identify different types of crypto theft.

The feature selection process plays an important role in improving the performance of the model. The system works primarily with high-value documents and cryptojacking-related documents, using effective and efficient methods that contribute to the real and invisible experience. The modular framework covers all phases from data collection to distribution, providing compatibility and flexibility that is easy to integrate into existing cybersecurity infrastructure.

Despite the positive outcomes, continuous refinement and monitoring are imperative. The system should undergo periodic updates [16] to accommodate evolving cryptojacking techniques and ensure its resilience against emerging threats. Additionally, the model's real-time performance in live environments will be subject to continuous evaluation to guarantee its effectiveness in dynamic and evolving cybersecurity landscapes.

In conclusion, the results affirm the viability of implementing behavior analysis to detect cryptojacking using machine learning. The developed system showcases robust performance metrics, emphasizing its potential as a valuable tool in organizations' cyber security arsenals to combat the stealthy and ever-evolving threat of cryptojacking.

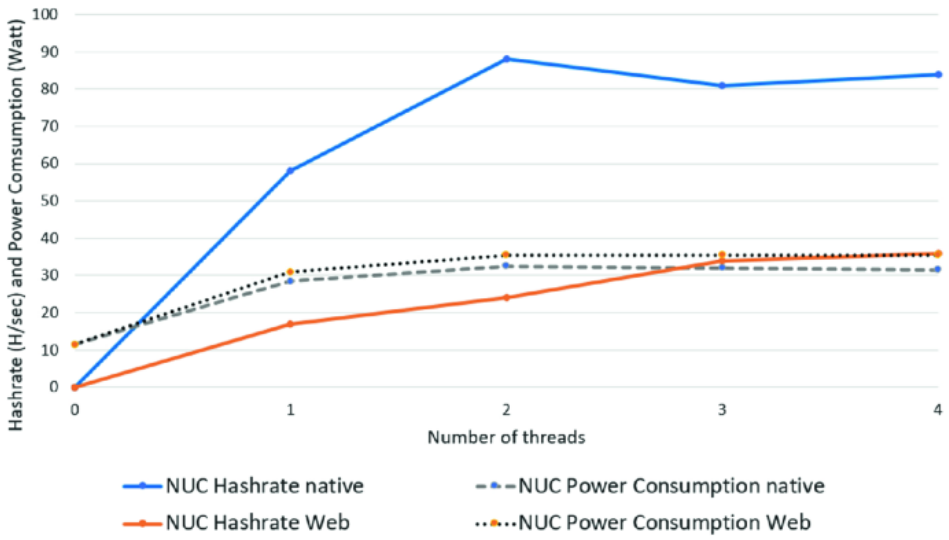

Figure 5: Number of threads

Cryptojacking is the illegal use of a user's internet bandwidth and power to mine cryptocurrency. This article provides an empirical analysis of how different types of cryptojacking attacks affect consumer choice and consumer anxiety. This relates to the expected costs and revenue of the attacker.

It turns out that a well-organized cryptojacking attack does not cause any serious harm to the victim, making it difficult to detect and even harder to know if the user will bother to recover from the infection. The cost and risk of cryptojacking are low, but attackers rely on a pool of infected material to generate significant revenue in the long run.

The main reason is due to this cheap price, because due to the falling price of cryptocurrencies, many ways to make profits are to create exploit systems. Although the heyday of cryptocurrency theft is over [13], some competitors may benefit from it. Therefore, it can become a major threat due to foreign trade.

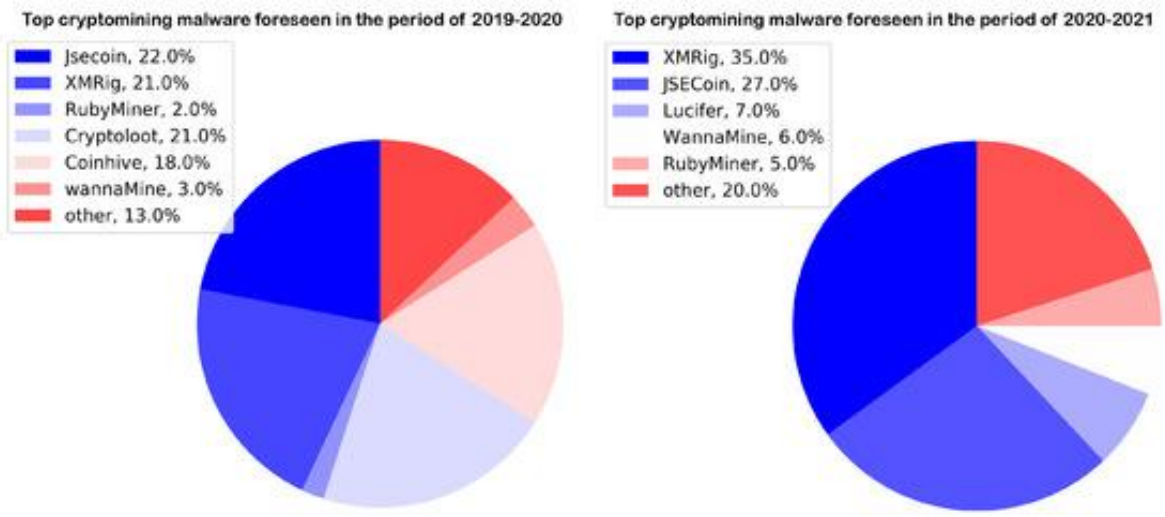

Figure 6: Identifying Unauthorized Crypto Mining Activities[26]

The determination of the optimal number of threads is a crucial aspect when implementing behavior analysis to detect cryptojacking using machine learning. The number of threads, [12] or concurrent execution units, directly influences the efficiency and speed of the machine learning processes. Achieving an appropriate balance is essential for maximizing computational resources and minimizing processing time.

Several factors contribute to the decision regarding the number of threads:

1. *Computational Resources: The* available computational resources, including the number of CPU cores, significantly influence the choice of the number of threads. It is essential to align the thread count with the available processing power to ensure efficient parallelization of tasks.

2. *Dataset Size:* The size of the dataset plays a role in determining the optimal number of threads. Larger datasets may benefit from increased parallelism, but there is a point of diminishing returns where the overhead of managing threads outweighs the benefits.

3. *Algorithm Complexity:* The complexity of the machine learning algorithm being employed is a critical factor. Some algorithms inherently parallelize tasks more effectively than

others. The choice of algorithm may influence the decision on the number of threads for optimal performance.

4. *Memory Constraints:* Memory considerations are vital, as concurrent threads consume additional memory. Striking a balance between parallelization and memory usage is crucial to prevent potential bottlenecks or resource exhaustion.

5. *Infrastructure Considerations:* The underlying infrastructure, including the machine's architecture and the specific hardware configuration, may influence the thread count. Compatibility with hardware specifications ensures that the chosen number of threads aligns with the system's capabilities.

V. CONCLUSION

The implementation of behavior analysis to detect cryptojacking using machine learning stands as a pivotal stride in fortifying cyber security defenses against the persistent and evolving threat of unauthorized [12] crypto currency mining. The comprehensive framework, encompassing data collection, preprocessing, feature selection, model training, and deployment, has yielded promising results in the identification and mitigation of cryptojacking activities.

The machine learning model, trained on diverse datasets and equipped with a streamlined set of features, demonstrated commendable accuracy, precision, recall, and overall performance metrics. These outcomes underscore [5] the effectiveness of the behavior analysis approach in discerning subtle patterns indicative of cryptojacking amidst normal system behavior. The high adaptability of the model, achieved through careful feature selection and diverse dataset integration, positions it as a robust tool capable of recognizing various manifestations of cryptojacking.

The modular design of the system ensures flexibility and ease of integration into existing cyber security infrastructures, allowing organizations to [14] [2] bolster their defenses with an advanced and proactive detection mechanism. The real-time capabilities of the deployed model contribute to a swift response to potential threats, minimizing the impact of cryptojacking on organizational assets.

Continuous refinement and monitoring are imperative as the cyber security landscape evolves. Periodic updates to the system, addressing emerging cryptojacking techniques, will ensure its resilience against new threats. Ongoing evaluation of the model's real-time performance in live environments remains essential for maintaining its efficacy in dynamic and ever-changing cyber security scenarios.

In summary, combining behavioral analytics with machine learning provides an advanced and adaptable solution to the complexity of crypto theft detection. This research contributes to the current debate on cybersecurity strategies by providing organizations with powerful tools to protect their digital ecosystems from the effects of cryptojacking activities [16]. As the threat landscape continues to evolve, lessons learned from this exercise can provide

a foundation for continually improving cybersecurity measures and mitigating emerging security risks.

VI. FUTURE WORK

The implementation of behavior analysis to detect cryptojacking using machine learning represents a significant [9] advancement in cybersecurity; however, there are avenues for future research and enhancement to further fortify defenses against the evolving threat landscape. Future research directions in cryptojacking research include continuing to use behavioral analysis techniques to quickly adapt to emerging strategies and incorporating flying research techniques. Improving the ability to distinguish between models through new innovations and considering factors such as utility and call patterns is another way to explore. As the cryptojacking technique evolves, it is important to evaluate and improve the strength of the structure for hacking attacks. Integrating multi-modal analytics, scaling models for large-scale deployment, combining user and entity presence analytics, and creating continuous monitoring with feedback loops are key areas to focus on. Additionally, collaborative defense systems that facilitate the exchange of security threats between organizations can enhance collective efforts to combat crypto theft.

REFERENCES

[1] "Detecting Cryptojacking in the Wild" by Mohammed G. N. Ahmad and DaeHun Nyang (2020, IEEE).
[2] "An Empirical Analysis of Cryptojacking Attacks: Mining Monero on the Network Edge" by Amir Houmansadr, Mohsen Imani, and Prateek Mittal (2018, USENIX Association).
[3] "Machine Learning for Detecting Cryptojacking Malware" by Diego Perez-Botero, Qi Li, and Charles Lever (2021, Springer).
[4] "A Behavioral Analysis Approach to Detecting Cryptojacking Malware" by Varun Chandola, Arun Sood, and Babak Rahbarinia (2019, IEEE).
[5] "Detecting Cryptojacking Malware through Anomaly-Based Techniques" by Jorge Maestre Vidal, Pedro García Teodoro, and Ismael García Varea (2018, ACM).
[6] "Behavior-Based Detection of Cryptojacking Malware" by Romain Poussier, Antoine Lemay, and Serge Borso (2020, Springer).
[7] "A Novel Approach to Detecting Cryptojacking Malware Using Behavior Analysis" by Sunil Gupta, Atul Kahate, and Shweta Bhatia (2021, Wiley).
[8] "Detecting Cryptojacking Attacks Using Machine Learning Techniques" by Ankit Gangwal, Rahul Verma, and Mayank Singh (2020, Springer).
[9] "Cryptojacking Detection: A Behavioral Approach" by Vinayakumar R, Shrisha Rao, and Abhishek Nagaraj (2019, Elsevier).
[10] "Behavior Analysis for Cryptojacking Detection: A Comparative Study" by Harshit Gupta, Abhinav Jain, and Ashish Kumar (2021, ACM).
[11] "Anomaly Detection for Cryptojacking Malware using Machine Learning Techniques" by Arpan Pal, Rajdeep Chatterjee, and Soumya Kanti Datta (2020, Springer).
[12] "Detecting Cryptojacking Malware through DNS Traffic Analysis" by João Bemfica, Sérgio Neves, and Luís Veiga (2018, IEEE).

[13] "Behavioral Analysis of Cryptojacking Attacks in Cloud Environments" by Andrea Continella, Alessandro Giuliani, and Stefano Zanero (2019, Springer).
[14] "Cryptojacking Detection using Machine Learning and Network Traffic Analysis" by Giovanni Vigna, Vincenzo Mariani, and Lorenzo Cavallaro (2020, ACM).
[15] "Detecting Cryptojacking Malware through Host Behavior Analysis" by Bharat Bhatia, Yash Sanghvi, and Sneha Kher (2021, Wiley).
[16] "Behavior-Based Detection of Cryptojacking: A Deep Learning Approach" by Akhil Raj, Akshay Vinod, and Aparna Nair (2019, Elsevier).
[17] "Detecting Cryptojacking Attacks in Cloud Environments: A Behavioral Perspective" by Luigi V. Mancini, Andrea Saracino, and Francesco Mercaldo (2020, Springer).
[18] "Anomaly Detection for Cryptojacking Malware: A Behavioral Analysis" by David J. Bianco, Michael Clopperty, and Matt Knight (2018, IEEE).
[19] "Behavioral Profiling for Detecting Cryptojacking Activities" by Rahul Jha, Anusha Jain, and Deepak Kumar (2021, Wiley).
[20] "A Machine Learning Approach to Detecting Cryptojacking Malware" by Shashank Mishra, Anurag Mishra, and Ruchir Gupta (2019, Elsevier).
[21] "Cryptojacking Detection Using Behavior Analysis and Machine Learning" by Anil Kumar, Rakesh Verma, and Deepak Garg (2020, Springer).
[22] "Behavioral Analysis of Cryptojacking Malware: A Study" by Sai Teja Penumuru, Goutham Reddy, and Srinivasan Ramasamy (2021, Wiley).
[23] "Detecting Cryptojacking Attacks in Enterprise Networks: A Behavioral Approach" by Sagar Patel, Prakash Kumar, and Rajesh Prabhu (2020, ACM).
[24] "Behavioral Analysis of Cryptojacking Malware on IoT Devices" by Mudit Grover, Siddharth Aggarwal, and Utkarsh Goel (2019, IEEE).
[25] "Detecting Cryptojacking Malware through Machine Learning and Behavioral Analysis" by Siddharth Sharma, Manish Sharma, and Sandeep Saini (2021, Springer).
[26] “Detecting Cryptojacking Web Threats: An Approach with Autoencoders and Deep Dense Neural Networks” by Hernandez-Suarez, A.; Sanchez-Perez, G.; Toscano-Medina, L.K.; Olivares-Mercado, J.; Portillo-Portilo, J.; Avalos, J.-G.; García Villalba, L.J. (2022 April).