Journal of Positive School Psychology
2022, Vol. 6, No. 3, 8611–8622

Detecting Illicit Cryptocurrency Mining Activity in Cloud Computing Platform

Muhammad Azizi Mohd Ariffin[1]; Mohamad Yusof Darus[2]; Abidah Mat Taib[3]; Rozianawaty Osman[4] ; Che Mohamad Anis Che Mat[5]

[1,2,3,4] *Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia*
[5] *Worldline International (APAC), Kuala Lumpur, Malaysia*
[1] *mazizi@fskm.uitm.edu.my*
[2]*yusof@fskm.uitm.edu.my*
[3]*abidah@uitm.edu.my*
[4] *roziana@fskm.uitm.edu.my*
[5] *mchemdanis@gmail.com*

Abstract

Cloud computing adoption in IT infrastructure is one of the key elements in the digital transformation strategy of an organization. The features such as on-demand self-service, resource allocation elasticity and massive scalability that cloud solutions offer have further accelerated adoption during Covid-19 Pandemics. This is because during a lockdown, the organization IT infrastructure must be able to cater for the dynamic requirements while supporting a remote working environment for their employees. Although cloud computing adoption brings many benefits to the organization, cloud users can abuse the cloud platform to conduct illicit cryptocurrency mining activity. The illicit crypto mining activity could be also caused by the spread of malware or security breaches on the cloud computing platform. The unwanted crypto mining activities will cause financial loss to the organization due to increased power consumption because of constant CPU utilization, inflated cooling needs and wasteful computing cycle. To address the problem, this paper proposed a method to effectively detect cryptocurrency mining activity in cloud computing environments. In the method, the cloud's system metrics were collected, pre-processed, and then undergoes features extraction. Then the AD3 algorithm was used to process the values of the features to separate the noise caused by the background process and crypto mining activity for anomaly detection. To evaluate the effectiveness of the proposed method, it was tested on the cloud platform running an OpenStack and the result shows that the proposed method can effectively detect crypto-mining activity and differentiate it from other background activity noise. During mining activity was simulated, the graph of features density values shows a significant drop indicating an anomaly. The method can be further expanded to detect anomalies in a hybrid cloud or container-based environment

Keywords: Cloud Security, System Security, Crypto Mining, Cloud Computing, User Abuse

I. INTRODUCTION

Cloud Computing has been widely adopted in the IT infrastructure of many organizations such as governments, enterprises, universities, financial institutions, and service providers. In many situations, cloud computing has been the technology that drives the digital transformation of the organization (Vu et al., 2020). The flexibility and elasticity of cloud computing technology have made it popular among IT administrators as their core IT infrastructure platform. According to IDC (Yap & Tan, 2020), there is a strong drive among ASEAN's

© 2022 JPPW. All rights reserved

organizations to adopt cloud computing in 2021 due to the Covid-19 pandemic, as it demands scalable and elastic IT infrastructure to support remote working environments.

As cloud computing deployment became popular and common, it can be abused by cloud users or insider IT personnel to run illegals or unauthorized cryptocurrency mining operations (Tahir et al., 2017). One of the common service deployment models for cloud computing is the Infrastructure as a service (IaaS) where users are given a virtual machine (VM) to host their application without managing the underlying physical server infrastructure (Bashari Rad & Diaby, 2017). The service provider or Cloud administrator can assign the user's VM with various virtualized resources such as CPU, Memory, Network Interface, storage, and the user will be given full control of the VM. By giving full control to the cloud user, it is the responsibility of the user to install the operating system and other related system applications which are needed for hosting their services. But the cloud user can abuse the full control privileges given to them to install unauthorized cryptocurrency mining programs on the VM for their gain instead of serving organization IT needs. Based on a report produced by Trend Micro (Alfredo Oliveira, 2019), there have been reported cases where the cloud API resource has been abused by the user for cryptocurrencies mining.

Moreover, illicit cryptocurrency activities on the cloud computing platform can also occur due to the spread of mining malware or hacker compromise on the platform (Zimba et al., 2020). As VM users are given admin rights, the responsibility of securing the assigned VMs are given to the users, but some users failed to properly harden their system which led to malware infection and vulnerability which can be compromised by hackers. The unwanted crypto mining activities will cause financial loss to the organization due to increased power consumption because of constant CPU utilization, inflated cooling needs and wasteful computing cycle (Liebenberg et al., 2018). Detecting such mining activities of the users on the organization cloud platform is difficult as usually there are hundreds or even thousands of running VMs on the cloud platform and it is difficult to differentiate the footprint of legitimate services and illegal mining activities. According to (Tahir et al., 2017), even if administrators can discover such activity, it may be too late as the illegal miners may have fled and shut down their operation. Thus, there is a need for research to find a solution to this problem effectively.

Several works have been conducted regarding the threat of cryptocurrency mining on the IT infrastructure. The work of (Coutinho et al., 2021) identifies the prevalence of illegal cryptocurrency mining in University networks using data collected from the Federal University of Rio de Janeiro (UFRJ) and the work also quantifies the monetary gains which motivate illegal cryptocurrency mining activity. But the work did not propose an effective or novel method to detect mining activity in cloud computing setup. The work of (Zimba et al., 2019) examines the digital forensics trial of three cryptocurrency malware attack vectors which are browser-based crypto-malware, memory resident and crypto viral extortion. But the work did not investigate further whether the digital forensics footprint is also visible during the operation of the cloud platform. Besides that, the paper of (Kharraz et al., 2019), (Hong et al., 2018) investigates the threat of in-browser crypto-jacking where end-users will become unaware that their computer resources have been used for mining activity. But the scope of the work is at the client-side, not at the IT infrastructure perspective. Based on the related work, most of the work examines illegal crypto mining issues due to malware and client perspective and none of the work examines crypto mining issues on cloud computing and proposes a method to effectively detect mining activity running on the cloud computing infrastructure of an organization.

Therefore, to address the gap, this paper proposes a method to effectively detect cryptocurrency mining activity in cloud computing environments. This paper will test

© 2022 JPPW. All rights reserved

the proposed method on a cloud testbed managed by OpenStack which is the most used cloud management software in the market. By providing an effective method to detect cryptocurrency mining, IT administrators will be able to mitigate the issue on their cloud infrastructure which will prevent the organization from significant financial loss. This will also deter external or internal users from abusing the cloud computing resources which has been assigned to them.

II. LITERATURE REVIEW

In this section, the paper will discuss the related topics regarding cryptocurrency mining issues on cloud computing platforms.

A. Crypto Currency Mining

The introduction of blockchain technology has revolutionized computing and business as it introduces the concept of storing transactional data in a distributed ledger. Blockchain has been applied in many areas such as electronic voting, travel booking (Hadzir & Yusoff, 2019), and the most famous blockchain application is the crypto-currency. In decentralized and peer-to-peer cryptocurrency systems such as Bitcoin (Nakamoto, n.d.) or Ethereum (Dannen, 2017) or many others, mining activity is needed to secure and verify the transaction. As an incentive to mine, miners who can solve a problem to verify the transaction will be rewarded with a coin. Thus, coins in cryptocurrency are created as a reward from the mining process. Nowadays, there is strong motivation to engage in cryptocurrency mining activity due to the huge potential of monetary gain. In 2021, Bitcoin price has reached USD 58,083 for 1 Bitcoin, while Ethereum price has reached USD 2,081.29 for 1 Ethereum. Experts forecasted that bitcoin price will continue to rise and reach USD 100,000. Mining is a process which requires enormous computational power and to make mining profitable, miners need mining farms such as in Figure 1.

Figure 1 – Cryptocurrency Mining Farm

Source: (Morgen E. Peck, 2017)

As mining requires huge computational power, it also consumes huge amounts of electricity. According to this research(O'Dwyert & Malone, 2014), the electricity consumption of mining Bitcoin is comparable to the electricity consumption of the whole of Ireland. In 2018, mining bitcoin has become unprofitable unless the mining is conducted in locations where the electricity cost is less than 0.14$/kWh (Delgado-Mohatar et al., 2019). It shows that the profit which has been gained by miners has been offset by the huge electricity cost. Thus, to continue making profits from mining, some miners decide to cut corners by engaging in illegal or illicit mining operations. Some miners make illegal connections to the power grid to steal electricity from the electricity providers (Bernama, 2021), some miners spread malware to steal computing resources from unaware users (Musch et al., 2018) and abuse the cloud infrastructure of other organizations (Tahir et al., 2017).

B. Mining Malware

Crypto Mining malware is a binary executable that becomes the payload of malware. The purpose of the binary program is to use the user's computing resources to mine cryptocurrency without the user being aware of the situation. As other malware infect user's computers, cryptocurrency malware will often disguise itself as legitimate programs such as Pirated software, games, or a script embedded

© 2022 JPPW. All rights reserved

within a website (also known as web crypto-jacking). To spread within the network, cryptocurrency malware also takes advantage of un-patch software vulnerabilities, slow software management cycle and zero-days exploits (Liebenberg et al., 2018). Examples of cryptocurrency malware present on the Internet are KryptoCibule (GRAHAM CLULEY, 2020), AppleJeus(David Bisson, 2021), WaterMiner ("Arbuz") (Zimba et al., 2020) and many more.

C. Cloud Computing Platform

According to National Institute of Standards and Technology (NIST) cloud computing is a computing model which enables suitable on-demand access network to distribute band of configured computing asset such as network, storages, servers, services, and application which precipitously provisioned and released with minimum management effort or interaction from the service provider (Mell & Grance, n.d.). Virtualization is the core technology that enables cloud computing as it allows a single bare-metal physical server to host multiple independent VM and it is also able to assign virtualized resources such as CPU, memory, storage, networking to the VM. Many private cloud infrastructures of an organization follow closely the definition of NIST. For example, there is a new internal IT requirement to develop a new human resource management system. The developer team can request server resources to host the application from the server team via a web dashboard. The request can be fulfilled automatically by the automation process or manually by the server team. A VM (or container) will then be provisioned to the developer team with the requested CPU, Memory, Disk and Networking resource allocation. If later the developer team decides to increase resources of the VM, they can request for VM resizing via a web dashboard.

Cloud Computing Model describes how the services will be deployed to the users, the level of resource abstraction and the essential characteristics which the services should fulfil. There are various cloud computing models have been proposed, but the most widely accepted model is the NIST model as shown in figure 2.

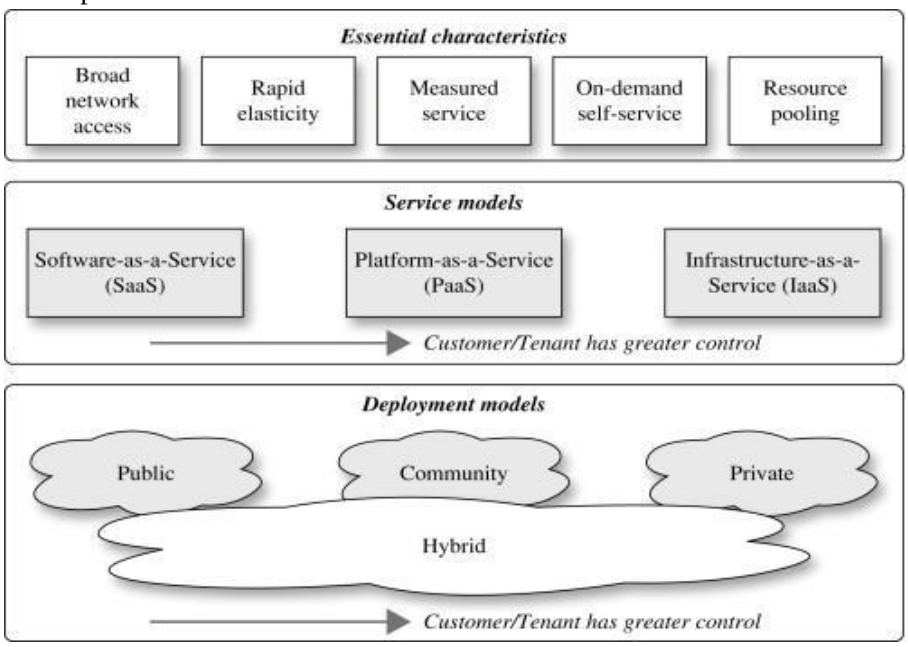


Figure 2 – NIST Cloud Computing Model

Source: (Vic (J.R.) Winkler, 2011)

Based on the NIST cloud computing model, the cloud computing services have 4 types of deployment models: public, community, private and hybrid. A public cloud is a cloud service that is offered by third parties such as Amazon, Microsoft, Google over the Internet, and the infrastructure can be leased by any organization. If there is concern regarding data privacy or sovereignty, organizations can opt in to build their on-demand cloud solution services over their existing on-premises IT

© 2022 JPPW. All rights reserved

infrastructure. Community cloud is several organizations working together to build a shared cloud infrastructure, even though it is multi-tenant and only exclusively shared among the community members. Meanwhile, the hybrid cloud combines public and private cloud. For example, certain applications are hosted on the organization data centre, but when there is a demand to scale resources during peak time, the organization can choose to off-load the demand to the public cloud infrastructure.

Cloud computing services are usually offered to users based on three types of services models: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). The highest level of service abstraction is SaaS, where end-users use the service without concern about the software, hardware or any related elements, examples of SaaS services are Dropbox, Gmail or Canva. PaaS is popular among developers, as developers were given a platform to host and run the code of their application without the hassle of managing a server such as operating system, web server, storage, database. IaaS gives more control to the cloud user without the hassle of managing the physical infrastructure, usually, the user is assigned a VM which the task of managing the server software and security become their responsibility. Moreover, the IT infrastructure must also be able to provide broad network access, rapid elasticity, measured service, on-demand self-service, and resources pooling to be categorized as a cloud computing platform. To allow developers to manage and provision their compute services automatically, the IaaS platform is usually equipped with APIs (Ali et al., 2018).

Operating a cloud computing infrastructure is not easy as it involves multiple components and complex interactions between those components. Thus, to ease the management of daily cloud computing operations, cloud infrastructure is usually deployed using cloud management software such as OpenStack, Cloud Stack, XCP-ng and many more. All of the different cloud components communicate with each other and with cloud management software using a common API, and in some cases, these APIs are vulnerable to different types of network attacks (Ariffin et al., 2020). But among those software, OpenStack is the most commonly deployed as 18% of organizations utilize OpenStack as an infrastructure provider (*OpenStack Services Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)*, n.d.). In this paper, OpenStack was used to set up the experimental testbed.

D Anomaly Detection Method

To detect Illicit crypto mining activity running on the cloud computing platform based on the collected system metrics, some statistical analysis needed to be done on the metrics to filter out the noise and differentiating legitimate and illicit processes to avoid false positives. Table 1 shows a comparison of the different algorithms used for anomaly analysis.

Table 1 –Algorithm for Analyzing Anomaly.

Method/Algorithm	Description	Weaknesses
Support-Vectors Machines (SVM) (Suthaharan, 2016)	Is a supervised learning model which analyzes data based on regression analysis and classification.	Although its ability to accurately classify the metrics, SVM is mathematically complex and computationally expensive. This will drain the computing resources of the cloud control node.
Classifier algorithm and Pearson correlation (Isa et al., 2020)	The work used the classifier algorithm and Pearson correlation to optimized the detection of intrusion on the system.	The proposed method works well with network traffic but did not demonstrate its effectiveness for system or

© 2022 JPPW. All rights reserved

		platform metrics.
Alternating Directions Dual Decomposition (AD3) (Martins et al., 2015)	This method introduces an algorithm with a modular architecture in which different subset values are solved independently.	The method is mathematically complex. But there is the availability of a library for its implementation.
Robust and non-robust statistics for outlier detection (Badarisam et al., 2020)	The detection anomaly in the system can be based on Robust and non-robust statistical analysis. Those statistics can detect multiple and patch outliers and The test statistics are based on the circular median and spacing theory.	The method displays a promising result in detecting an outlier accurately. But it has only been tested on the dataset based series of investigations on the northern cricket frogs homing ability.

III. METHODOLOGY

In this paper, the proposed detection method to detect crypto mining in cloud computing platforms will be tested on a cloud testbed. While the experiment is running, the research will collect the primary data in the form of system metrics and feed it to the detection algorithm. The research methodology used in the paper to achieve its objective is shown in figure 3.

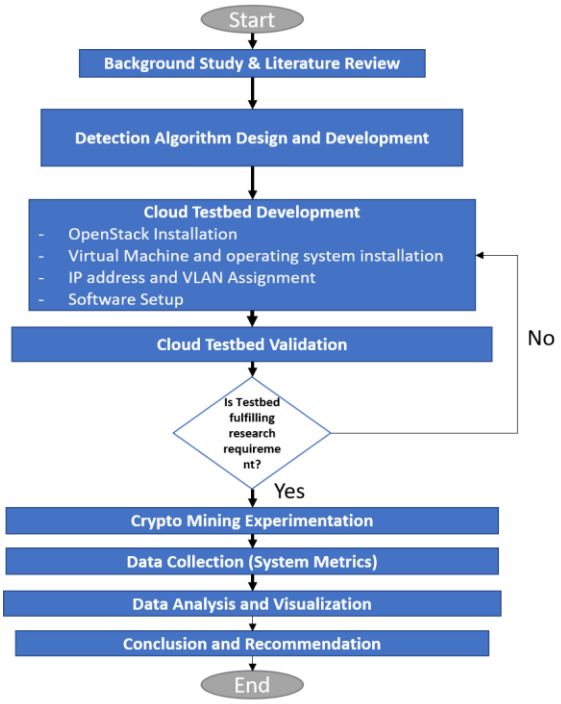


Figure 3 – The Project Research Methodology

Based on the methodology in figure 3, this research starts by conducting background research and literature review. In this stage, this project reviews the topics related to the crypto mining issues and related work regarding the solution to the problem. After that, in the next stage this project develops a detection algorithm based on AD3, the detection algorithm will be developed using Matlab. To detect the crypto mining activity, the developed algorithm needs to feed with system metrics, thus this project develops a cloud testbed for simulating a real-world cloud infrastructure deployment using OpenStack. After finishing configuring the hardware, software, VM, IP address and VLAN for the testbed, the setup will be validated whether it can fulfil the experiment design requirements. Examples of the requirements are the number of running VMs, software running on the VMs and network settings such as VLAN or IP address.

If the testbed fulfils all requirements for the experiment, the experiment will begin based on two scenarios. While the experiment is running, the system and network metrics will be collected using a tool. The data will then be formatted and then fed into the anomaly detection algorithm for analyzing the pattern which may indicate a mining activity. The last stage will discuss the result of the detection

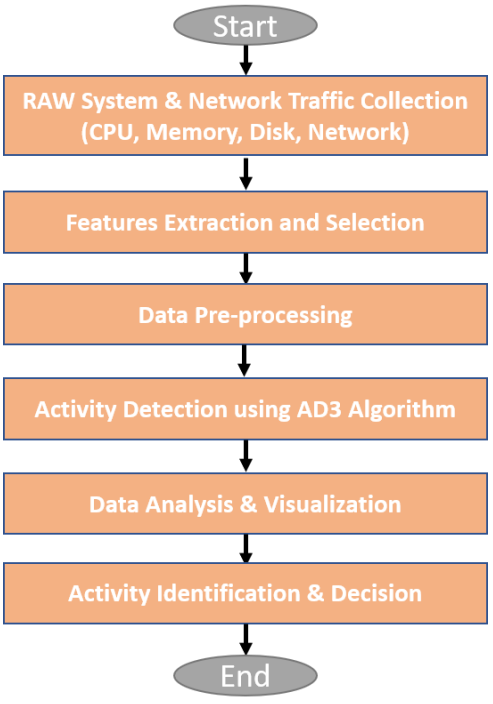
© 2022 JPPW. All rights reserved

algorithm and the effectiveness of the proposed algorithm.

A. Anomaly Detection Algorithm

To detect a cryptocurrency mining activity on the cloud computing platform, the developed algorithm needs to be able to differentiate the pattern caused by background or legitimate process and pattern caused by the illicit mining process, thus this project integrates Alternating Directions Dual Composition (AD3) algorithm (Martins et al., 2015) at the heart of the process for detecting the pattern. AD3 was designed for modularity where each of the local subproblems is processed independently, thus it is suitable for processing different types of metrics and excluding noise from background processes. The AD3 algorithm will calculate the data density values from the given metrics for the bin/time. When we plot the data density values, we can identify anomalies patterns by seeing a line drop in the graph at a particular time. Figure 4 shows the detection process flowchart.

Figure 4 – Anomaly Detection Process Flowchart



The detection of crypto mining processes begins with collecting raw system and network metrics (CPU, memory, disk, and network) data from all the physical machines running the OpenStack node. The system metrics raw data was collected using System Activity Report (SAR) tools (*Sysstat/Sysstat: Performance Monitoring Tools for Linux*, n.d.) while the network metrics were collected using TCP Dump tools. After that, the raw metrics need to undergo a features extraction and selection process because not all metrics collected from the physical machines can reflect an anomaly of malicious operation. For detecting an anomaly caused by crypto mining activity, this research selects CPU users, CPU load, memory utilization, memory commit and network utilization features. SADF tool (B.D. Theelen, 2007) was used to select features from system metrics while for network metrics Caida Coral Reef (Keys et al., 2001) was used.

After the features have been extracted and selected from the raw metrics, it needs to undergo pre-processing to standardize the values of the features so that they can be fed into AD3. This is because the range or scale of multiple metrics features varies differently from each other. To standardize the values, we need to calculate a z-score or standard score for each of the feature metrics. The formula as follows:

$$z = (X - \mu) / \sigma$$

Where z is the z-score, X is the value of the selected features, μ is the features mean, and σ is the standard deviation. The value of the z-score indicates how many standard deviations an element is from the mean (Patro & Sahu, 2015). After the standard score has been calculated for each feature, it then feeds into the AD3 algorithm for calculating the data density of the features to time. The detecting algorithm was implemented using Matlab. Thus, after calculating the density of the features, the values were plotted using Matplotlib. The analysis of the pattern was conducted based on a graph with features density at the Y-axis and Time interval at the X-axis. After analyzing and visualizing the density data, the illicit mining activity can be determined based on the drop pattern on the graph.

B. Experiments Design

There are two scenarios during the experiment which have been conducted on the cloud testbed to test the effectiveness of the proposed detection method. For each scenario, the

© 2022 JPPW. All rights reserved

experiment will be running for 10 minutes. First is the control scenario where the experiment was conducted without any mining process running on any VMs to simulate a mining activity. While the experiment was running, multiple software such as Apache web server, Hadoop and file server were running on different VMs to simulate background processes and legitimate services. The purpose of the control scenario is to get baseline data when the system is operating as normal without any anomalies. The second scenario will involve running the cpuminer-opt 3.8.8.1 program for mining Bitcoin and geth 1.7.3 program for mining Ethereum on the VMs during an experiment to simulate cryptocurrency mining activities. During the second scenario, the mining program will be executed after the experiment has run for 5 minutes.

C. Experimental Cloud Testbed

The cloud testbed for the experiment was built using OpenStack cloud management software, figure 5 shows the topology of the testbed. The server's hardware used for running the cloud controller node and the compute node was equipped with a 3.40GHz i7-2600 CPU, 16GB RAM, 1TB of SATA hard disk and dual gigabit ethernet interface. One gigabit port is connected to the management VLAN while the other gigabit port is connected to the data VLAN. The management VLAN will only carry management traffic such as APIs and dashboards. While the Data VLAN carries the user's traffic from the VMs to other VM or the Internet. All the server's network interfaces are connected to the gigabit switch and to reach the internet the traffic will be routed via a border router which performs network address translation (NAT) on the network packet.

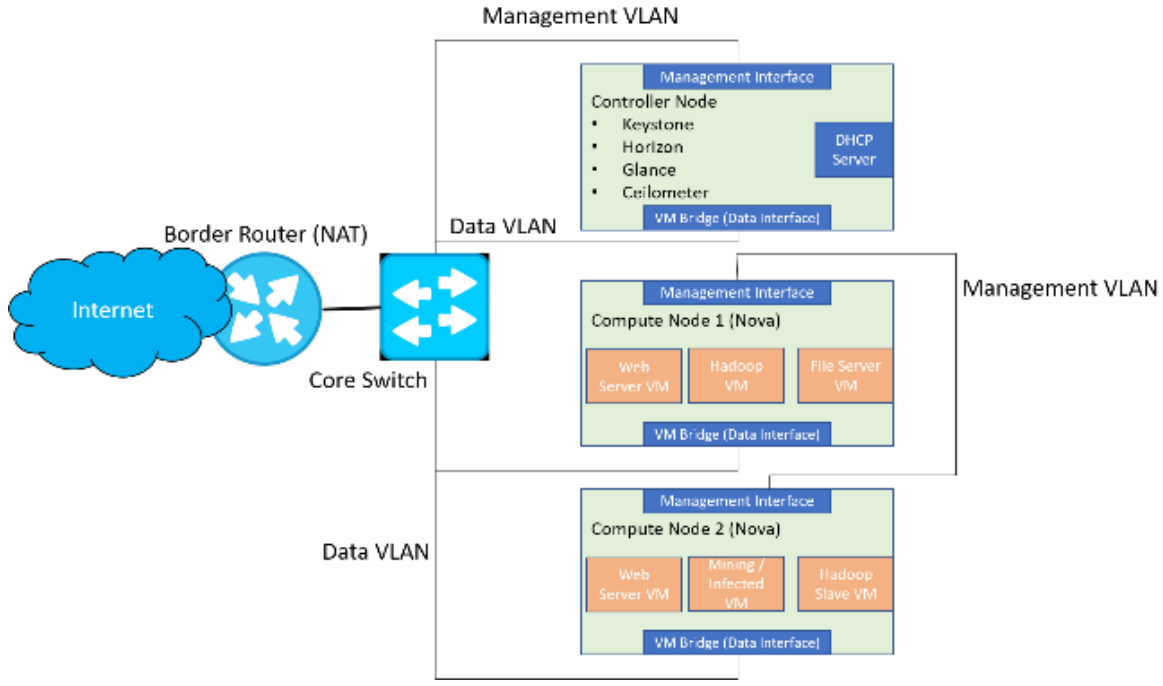


Figure 5 – Cloud Testbed Topology

IV. RESULT AND DISCUSSION

This section will discuss the result of the control experiment and the experiment which simulate cryptocurrency mining activity. For the second experiment, the discussion will involve the graph which highlights the feature density of CPU related metrics during illicit mining activity.

A. Control Result

The graph in figure 6 shows the features metric density produced by the detection algorithm during the control experiment.

© 2022 JPPW. All rights reserved

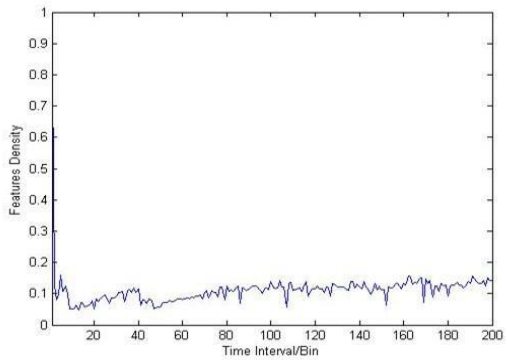


Figure 6 – Control Experiment Metrics Data

The Y-axis of the graph represents the density value of metric features, while the X-axis represents the time interval in which the metric data was collected. The range of the Y-axis is 0 to 1 because of the standardization of metric values. The range of X-Axis is in the range of 0 to 200 because raw data is collected every three seconds, for ten minutes. The graph in figure 6 does not indicate any significant drops indicating there is no anomaly caused by mining activity. There is a slight up and down of the graph due to the noisy nature of the background process. This result was used as a baseline for normal system operation.

B. Crypto Currency Mining Simulation

The graph in figure 7 shows the features metric density produced by the detection algorithm during the simulation of mining activity on the cloud computing platform.

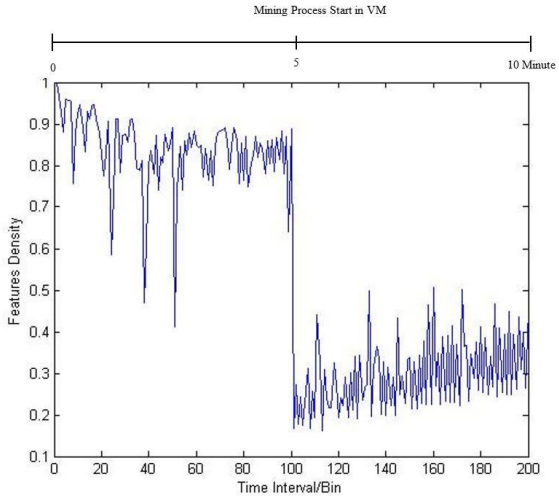


Figure 7 – CPU Metrics During Mining Process

The X and Y-axis of the graph represent the same value as the graph in figure 6 previously. The graph in figure 7 shows a significant line drop in minute 5 which the crypto mining program was running. This indicates an anomaly pattern that was caused by CPU intensive processes such as Cryptocurrency mining. There are other drops in the graph due to other background processes, but the drops are not significant, and the noise has been filtered by the AD3 algorithm. To avoid false-positive detection, during the operation the cloud administrator can set a threshold value on the feature's density. Based on the result shown in figure 7, shows that the proposed detection method of this paper able to effectively detect a crypto mining activity on the cloud computing platform.

V. CONCLUSION

This paper proposed a method to effectively detect illicit cryptocurrency mining activity on the cloud computing platform. The method works by collecting the cloud platform metrics such as CPU, memory and disk utilization values and feed them to AD3 for noise separation and anomaly detection. The proposed method had been tested on the cloud testbed running OpenStack. Based on the result, it shows that the algorithm can detect a malicious pattern from the CPU and memory metrics. This can aid cloud administrators to pinpoint which of many physical server machines in the cloud platform hosted a VM which is running an illicit crypto mining activity and thus saving the organization from potential financial loss. The research can be further expanded on the public or hybrid cloud infrastructure and the container-based cloud infrastructure.

ACKNOWLEDGEMENT

The authors would like to extend appreciation to the research and industrial linkages division of the Faculty of Computer and Mathematical Sciences, UiTM Shah Alam, for supporting this project by providing a grant and facilities needed to complete this research.

© 2022 JPPW. All rights reserved

BIBLIOGRAPHY

1. ALFREDO OLIVEIRA. (2019). Exposed Docker Control API and Community Image Abused to Deliver Cryptocurrency-Mining Malware - TrendLabs Security Intelligence Blog. https://blog.trendmicro.com/trendlabs-security-intelligence/exposed-docker-control-api-and-community-image-abused-to-deliver-cryptocurrency-mining-malware/?_ga=2.148602167.1611177887.1617850113-878262968.1617850113
2. ALI, M., ZOLKIPLI, M. F., ZAIN, J. M., & ANWAR, S. (2018). Mobile Cloud Computing with SOAP and REST Web Services. Journal of Physics: Conference Series, 1018(1). https://doi.org/10.1088/1742-6596/1018/1/012005
3. ARIFFIN, M. A. M., IBRAHIM, M. F., & KASIRAN, Z. (2020). API vulnerabilities in cloud computing platform: Attack and detection. International Journal of Engineering Trends and Technology, 1, 8–14. https://doi.org/10.14445/22315381/CATI1P202
4. B.D. THEELEN. (2007). A Performance Analysis Tool for Scenario-Aware Streaming Applications | IEEE Conference Publication | IEEE Xplore. Fourth International Conference on the Quantitative Evaluation of Systems. https://ieeexplore.ieee.org/document/4338266
5. BADARISAM, F. N., RAMBLI, A., & SIDIK, M. I. (2020). A comparison on two discordancy tests to detect outlier in von mises (VM) sample. Indonesian Journal of Electrical Engineering and Computer Science, 19(1), 156–163. https://doi.org/10.11591/IJEECS.V19.I1.PP156-163
6. BASHARI RAD, B., & DIABY, T. (2017). Cloud Computing: A review of the Concepts and Deployment Models Cloud Computing View project Metamorphic Malware CLassification using MLP Neural Network View project Cloud Computing: A review of the Concepts and Deployment Models. Article in International Journal of Information Technology and Computer Science, 6, 50–58. https://doi.org/10.5815/ijitcs.2017.06.07
7. BERNAMA. (2021). Perak police smashed 24 Bitcoin mining premises since December | The Edge Markets. The Edge. https://www.theedgemarkets.com/article/perak-police-smash-24-bitcoin-mining-premises-december
8. COUTINHO, F. R., Pires, V., Miceli, C., Menasché, D. S., & Menasché, M. (2021). Crypto-Hotwire: Illegal Blockchain Mining at Zero Cost Using Public Infrastructures. http://btc.com
9. Dannen, C. (2017). Introducing Ethereum and Solidity. Berkeley, CA: Apress.
10. David Bisson. (2021). Crypto Malware “AppleJeus” Opens Cryptocurrency Wallets to Thieves. Security Intelligence. https://securityintelligence.com/news/applejeus-crypto-malware-targets-cryptocurrency/
11. DELGADO-MOHATAR, O., FELIS-ROTA, M., & FERNÁNDEZ-HERRAIZ, C. (2019). The Bitcoin mining breakdown: Is mining still profitable? Economics Letters, 184, 108492. https://doi.org/10.1016/j.econlet.2019.05.044
12. GRAHAM CLULEY. (2020). KryptoCibule malware has been stealing and mining cryptocurrency. Tripwire. https://www.tripwire.com/state-of-security/featured/kryptocibule-

© 2022 JPPW. All rights reserved

malware-stealing-mining-cryptocurrency/

13. HADZIR, H. B. M., & YUSOFF, F. H. BIN. (2019). Blockchain Based Data Structure for Travel Entourage Tracking System. 2019 4th International Conference on Information Systems and Computer Networks, ISCON 2019, 538–541. https://doi.org/10.1109/ISCON47742.2019.9036270
14. HONG, G., ZHANG, L., YANG, M., YANG, Z., NAN, Y., ZHANG, Y., DUAN, H., YANG, S., ZHANG, Z., & QIAN, Z. (2018). How you get shot in the back: A systematical study about cryptojacking in the real world. Proceedings of the ACM Conference on Computer and Communications Security, 1701–1713. https://doi.org/10.1145/3243734.3243840
15. ISA, F. M., BUJA, A. G., DARUS, M. Y., & SAAD, S. (2020). Optimizing the effectiveness of intrusion detection system by using pearson correlation and tune model hyper parameter on microsoft azure platform. International Journal of Advanced Trends in Computer Science and Engineering, 9(1.3 Special Issue), 132–138. https://doi.org/10.30534/ijatcse/2020/1991.32020
16. KEYS, K., MOORE, D., KOGA, R., LAGACHE, E., & TESCH, M. (2001). The Architecture of CoralReef: An Internet Traffic Monitoring Software Suite.
17. KHARRAZ, A., LEVER, C., BORISOV, N., MA, Z., MASON, J., ANTONAKAKIS, M., MURLEY, P., MILLER, A., & BAILEY, M. (2019). Outguard: Detecting in-browser covert cryptocurrency mining in the wild. The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019, 840–852. https://doi.org/10.1145/3308558.3313665
18. LIEBENBERG, D., MCFARLAND, C., MARTINEZ, M., & JEROME CRUZ, F. (2018). THE ILLICIT CRYPTOCURRENCY MINING THREAT. https://www.cyberthreatalliance.org.
19. MARTINS, A. F. T., FIGUEIREDO, M. A. T., AGUIAR, P. M. Q., SMITH, N. A., XING, E. P., & JAAKKOLA, T. (2015). AD 3 : Alternating Directions Dual Decomposition for MAP Inference in Graphical Models. In Journal of Machine Learning Research (Vol. 16). http://www.ark.cs.cmu.edu/AD3
20. MELL, P., & GRANCE, T. (n.d.). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145
21. MORGEN E. PECK. (2017). Why the Biggest Bitcoin Mines Are in China - IEEE Spectrum. IEEE Spectrum. https://spectrum.ieee.org/computing/networks/why-the-biggest-bitcoin-mines-are-in-china
22. MUSCH, M., WRESSNEGGER, C., JOHNS, M., & RIECK, K. (2018). Web-based Cryptojacking in the Wild. In arXiv.
23. NAKAMOTO, S. (n.d.). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved April 9, 2021, from www.bitcoin.org
24. O'DWYERT, K. J., & MALONE, D. (2014). Bitcoin mining and its energy footprint. IET Conference Publications, 2014(CP639), 280–285. https://doi.org/10.1049/cp.2014.0699
25. OpenStack Services Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026). (n.d.). Retrieved April 10, 2021, from https://www.mordorintelligence.com/i

© 2022 JPPW. All rights reserved

ndustry-reports/openstack-services-market
26. PATRO, S. G. K., & SAHU, K. K. (2015). Normalization: A Preprocessing Stage. IARJSET, 20–22. http://arxiv.org/abs/1503.06462
27. Suthaharan, S. (2016). Support Vector Machine. Machine Learning Models And Algorithms For Big Data Classification, 207-235. doi: 10.1007/978-1-4899-7641-3_9
28. sysstat/sysstat: Performance monitoring tools for Linux. (n.d.). Retrieved April 12, 2021, from https://github.com/sysstat/sysstat/
29. TAHIR, R., HUZAIFA, M., DAS, A., AHMAD, M., GUNTER, C., ZAFFAR, F., CAESAR, M., & BORISOV, N. (2017). Mining on someone else's dime: Mitigating covert mining operations in clouds and enterprises. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 10453 LNCS, 287–310. https://doi.org/10.1007/978-3-319-66332-6_13
30. VIC (J.R.) WINKLER. (2011). Cloud Deployment Model - an overview | ScienceDirect Topics. Science Direct. https://www.sciencedirect.com/topics/computer-science/cloud-deployment-model
31. VU, K., HARTLEY, K., & KANKANHALLI, A. (2020). Predictors of cloud computing adoption: A cross-country study. Telematics and Informatics, 52, 101426. https://doi.org/10.1016/j.tele.2020.101426
32. YAP, J. J. Q., & TAN, D. (2020). Cloud remains top technology investment priority for ASEAN Organizations. https://www.idc.com/getdoc.jsp?containerId=prAP46702820
33. ZIMBA, A., WANG, Z., CHEN, H., & MULENGA, M. (2019). Recent advances in cryptovirology: State-of-the-art crypto mining and crypto ransomware attacks. KSII Transactions on Internet and Information Systems, 13(6), 3258–3279. https://doi.org/10.3837/tiis.2019.06.027
34. ZIMBA, A., WANG, Z., MULENGA, M., & ODONGO, N. H. (2020). Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security. Journal of Computer Information Systems, 60(4), 297–308. https://doi.org/10.1080/08874417.2018.1477076

© 2022 JPPW. All rights reserved