Journal of Theoretical and Applied Information Technology
15th June 2023. Vol.101. No 11
© 2023 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SECURITY FRAMEWORK PROTECTING VIRTUAL MACHINES AGAINST ATTACKS ON MIGRATION AND PERSISTENCE IN CLOUD COMPUTING ENVIRONMENT

S. MAHIPAL[1] and V. CERONMANI SHARMILA[2]

[1]Research Scholar at the Hindustan Institute of Technology and Science, India

[2]Professor and HOD in the IT Department of Hindustan Institute of Technology and Science, India

E-mail: [1]srmahipal@gmail.com, [2]csharmila@hindustanuniv.ac.in.

ABSTRACT

In a cloud computing environment, Virtual Machine (VM) migration achieves energy efficiency, efficient resource management, and load balancing. VM persistence is another area that leads to increased performance. However, both of them do have security vulnerabilities. There are existing approaches followed by Virtualization technology vendors. However, there is a need for further research to leverage security in the aforementioned areas. Towards this end, in this paper, we proposed a security framework that ensures that VM migration and VM persistence occur without causing cyber-attacks. The framework has two algorithms proposed to realize this objective. Safe Virtual Machine Migration (SVMM) is meant for protecting VM from VM hopping attacks on the VM migration process while another algorithm known as Safe Virtual Machine Persistence (SVMP) focuses on preventing attacks on VM persistence. Both mechanisms are crucial for leveraging cloud performance and Quality of Service (QoS). The proposed framework is realized with a simulation study using CloudSim. The experimental results showed that the proposed approach is capable of handling attacks while VM is being migrated and when VM is being persisted.

Keywords –*Cloud Computing, VM Migration, VM Persistence, Secure VM Migration, Secure VM Persistence*

1. INTRODUCTION

In a cloud computingenvironment, Virtual Machine (VM) migration achieves energy efficiency, efficient resource management, and load balancing. VM persistence is another area that leads to increased performance. Both approaches are found to be associated with virtualization which is linked to cloud computing. Since the cloud is providing scalable resources, virtualization plays its role in realizing sustainable cloud technology. VM live migration and VM persistence are crucial for efficient resource management makespan. VM live migration research is found in [1], [22], and [26]. Narayana and Jayashree [1] investigated different virtualization attacks and found that the VM migration threat is one of the important virtualization threats. They opined that there is a need for protecting the process of VM live migration. VM live migration process is illustrated in [22] with its dynamics in the process of migration. In [26] VM live migration along with security preservation is explored. In the same fashion, some researchers contributed to VM persistence attacks as explored in [2] and [5]. *et al*. [2] proposed a security framework to have the required defense against advanced persistence attacks. It is a threat-intelligent-driven approach to addressing such attacks. From the literature, it is ascertained that there has been significant research carried out on attacks on VM migration and VM persistence. There is a need for an integrated approach that considers the protection of VM migration and VM persistence from malicious attacks. Our contributions to this paper are as follows.

1. We proposed a security framework that ensures that VM migration and VM persistence occur without causing cyber-attacks.
2. We proposed two algorithms proposed such as Safe Virtual Machine Migration (SVMM) is meant for protecting VM from VM hopping attacks on the VM migration process while another algorithm known as Safe Virtual

Machine Persistence (SVMP) focuses on preventing attacks on VM persistence. Both mechanisms are crucial for leveraging cloud performance and Quality of Service (QoS). T

3. he proposed framework is realized with a simulation study using CloudSim. The experimental results showed that the proposed approach is capable of handling attacks.

The remainder of the paper is structured as follows. Section 2 reviews the literature on different techniques of VM migration and VM Persistence. Section 3 proposes a methodology to deal with VM migration and VM persistence attacks. Section 4 presents the empirical study and its results. Section 5 concludes our work and gives possible directions for future work.

2. RELATED WORK

This section reviews the literature on different methods of VM attacks and countermeasures focusing on persistence and migration attacks. Narayana and Jayashree [1] investigated different virtualization attacks and found that the VM migration threat is one of the important virtualization threats. They opined that there is a need for protecting the process of VM live migration. Li *et al*. [2] proposed a security framework to have the required defense against advanced persistence attacks. It is a threat-intelligent-driven approach to addressing such attacks. Alshamrani*et al*. [3] explored different advanced persistence threats (APTs), techniques to address them, and the challenges involved. They illustrated different examples of such threats and possible countermeasures to mitigate attacks. Bahram *et al*. [4] focused on VM introspection as it is important to monitor a VM's functionality. They also presented an attack that could subvert VM introspection to analyze the level of security being provided. Chandra *et al*. [5] proposed an intelligence-based approach to protecting VM from persistent threats. Their solution is based on social engineering where users are educated to prevent attacks.

Li *et al*. [6] characterized and analyzed APTs in VM and cloud environments. They launched different cyber-attacks and evaluated countermeasures and found that APTs are of real threat to different cloud environments. Friedberg *et al*. [7] focused on incident detection through network event correlation to identify APTs and mitigate their effects. Their solution is a fingerprint-based and rule-based approach to detect such attacks. Hildenbrandt*et al*. [8] studied the functioning of Ethereum VM and its role in the growing virtualization-based solutions. Hu *et al*. [9] found that APTs can be launched by insiders as well. To have a defense against such attacks, they proposed a strategy that is dynamic and adaptive. Their system model has different roles to demonstrate the attack and its prevention mechanism. Zhang *et al*. [10] proposed a methodology to protect the integrity and privacy of cloud users with their protection for VMs in the presence of nested virtualization and possible cyber-attacks. Gharehpasha*et al*. [11] proposed a multiverse optimization algorithm for efficient VM placement.

Wang *et al*. [12] investigated on Cloud-Droplet-Freezing attack that causes the collapse of available features in cloud computing. It is a threat to the VM migration phenomenon in distributed system models. The attack has diversified targets such as software and hardware resources. Win *et al*. [13] proposed a methodology for VM securing with a hybrid approach consisting of VM introspection and mandatory access control. There is a hidden monitoring module along with the proposed method to detect security threats. Masdari and Zangakani [14] investigated proactive VM placement to reduce energy consumption in virtualized environments. They proposed a method to this effect to achieve low VM overhead. Zeb *et al*. [15] designed an architecture for VM migration between clouds in a secure fashion. Their architecture illustrates secure VM migration mechanisms between cloud service providers.

Choudhary *et al*. [16] discussed different VM migration approaches. They found that VM migration has advantages such as load balancing, power saving, fault tolerance, resource optimization, and efficient system maintenance. Different kinds of memory are also moved along with VM migration and there is a need for preventing attacks. Ahmad *et al*. [17] explored server consolidation and VM migration mechanisms and the need for VM migration in cloud environments. Shirvani*et al*. [18] also did research in similar areas as that of [17] but used DVFS technology-enabled data centers. Kumara and Jaidhar [19] proposed a system that monitors and detects intrusions made through VM and hypervisor. They have implemented a signature-based and anomaly-based intrusion detection system. Reeba*et al*. [20] proposed a method

based on processor workload prediction for securing VM migration. It has provisions for authentication, load balancing, and secure VM migration for optimal resource utilization.

Other important researches include VM live migration dynamics [21], secure VM placement [22], DDoS attacks in the cloud [23], VM management with security awareness [24], integrity and security prediction model [25], VM lives migration with security preservation [26], VM migration and configuration management using blockchain [27], VM allocation security strategy [28] and VM placement optimization technique. From the literature, it is ascertained that there has been significant research carried out on attacks on VM migration and VM persistence. There is a need for an integrated approach that considers the protection of VM migration and VM persistence from malicious attacks.

3. PROPOSED METHODOLOGY

We proposed a methodology for secure VM migration and secure VM persistence. The dual objective of the proposed method is presented in the following sub-sections.

3.1 Secure Virtual Machine Migration

For secure VM migration considering VM hopping attacks, we designed an architecture that is meant for handling VM hopping attack which is associated with the VM migration process. Figure 1 shows the proposed architecture used to prevent VM hopping attacks that are associated with the VM migration process. The proposed architecture has mechanisms to handle VM hopping attacks. It has mechanisms associated with the hypervisor and also the host OS. There is a monitoring module in the host OS that monitors the control matrix and information for controlling access. The hypervisor part is configured with different mechanisms like a control matrix, information for controlling access, the decision for access, and the access control module.

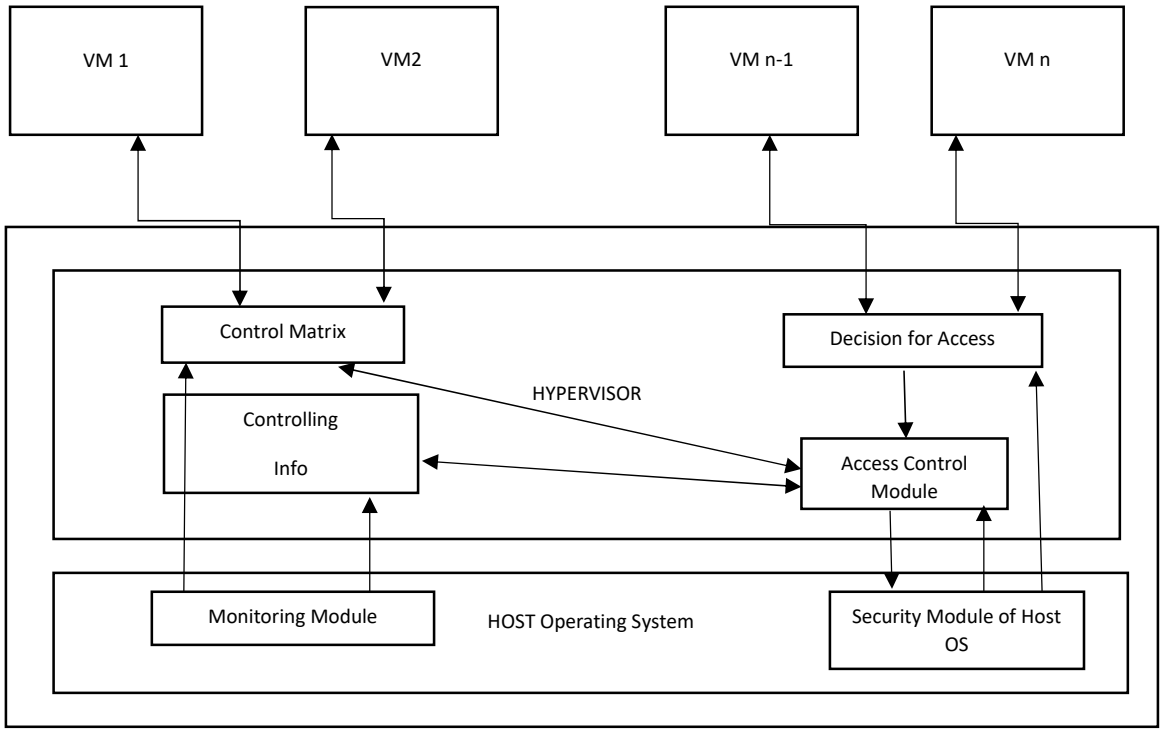

Figure 1: Proposed architecture for preventing VM hopping attack

The monitoring module is associated with the host OS which can be configured by the system admin to deal with the proposed system. At the time of VM creation, the admin has the provision to send a level of confidentiality and integrity based on the needs of the application. It also helps in managing the control matrix and information for controlling as the situation prevails at runtime. The decision for access is meant for checking the request for access by any VM and to know whether the request satisfies access policies. Here requests are filtered to avoid malicious and illegal ones. Only genuine requests are given to the access control module. The access-related matrix is associated with the control matrix. The access control module has an

underlying security implementation with a hook for interfacing with the host OS security module. The information for controlling contains details about VMs at runtime. The host OS security is integrated with the proposed method. As OS starts functioning, the proposed system gets active and monitors for VM hopping attacks.

As presented in Figure 2, the SVMM algorithm takes care of access control and also mandatory requirements to take decisions to allow requests or not. The given request by VM is subjected to multiple checks to avoid a VM hopping attack. After receiving the request, the label associated with the sender and the resource is resolved before processing the request. The initial access control (discretionary) is verified. If this is satisfied, the request is allowed. If not satisfied, mandatory access control is verified. If the condition is satisfied, the request is allowed. If not satisfied, then the sender-level access level is verified. If that is satisfied the access level is updated for

the given sender. If not satisfied, then the resource level access is verified and updated if satisfied. There is an iterative process that continuously verifies the requests given and appropriate decision is made to prevent VM hopping attack.

a. Secure Virtual Machine Persistence

We proposed an algorithm known as Safe Virtual Machine Persistence (SVMP) which exploits machine learning models to detect attacks VMs associated with VM persistence. It recovers attacked VMs automatically. In the process, three ML models are used with and without hyperparameter tuning.

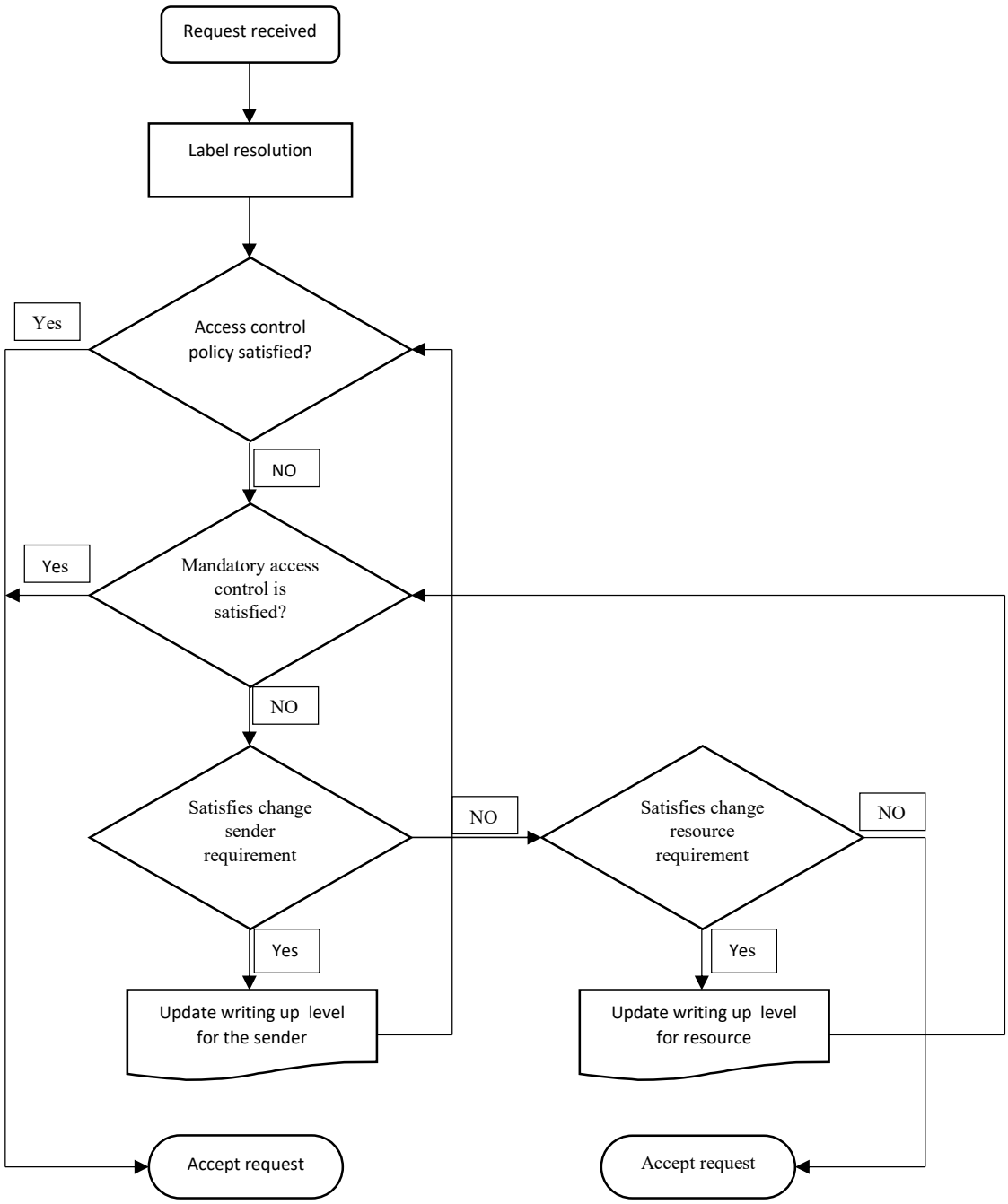

Figure 2:Flow Chart Of The Proposed Safe VM Migration Algorithm

Algorithm: Safe Virtual Machine Persistence (SVMP)

Input:

Virtual machines denoted as M={VM1, VM2, …, VMn}

Machine learning models L

Output: Persistence attack detection and recovery of VM

1. Start
2. For each m in M
3. Monitor the status of m
4. IF status is abnormal Then
5. Find victim VM

```
6.      Stop victim VM
7.    End If
8.    Find all snapshots of victim VM V
9.    For each v in V
10.     For each l in L
11.     Find severity level with l
12.     Find sustained v
13.     Recover v
14.   End For
15.  End For
16. End For
17. End
```

Algorithm 1: Safe Virtual Machine Persistence (SVMP) algorithm

As presented in Algorithm 1, it considers all VMs and identifies attacked VMs. It has a provision for finding severity levels with changes made to the VM state. If there is negligible change, that VM is considered sustained from the attack. If there is a certain level of severity, that VM is recovered and it then functions as usual. There is an iterative process to monitor VMs continuously to prevent VM performance attacks based on the snapshot size.

Performance Evaluation

Two performance metrics such as MAPE and RMSE are used for the evaluation of the SVMP algorithm.

$$MAPE = 1/n \sum_{i=1}^{n} YP_i - Y_i/Y_i \quad (1)$$

$$RMSE = \sqrt{\sum_{i=1}^{n}(YP_i - Y_i)2/n} \quad (2)$$

Table 1: Shows Notations Used

Notation	Description
MAPE	Mean Absolute Percentage Error
RMSE	Root Mean Square Error
YP_i	Predicted data as the output
Y_i	Actual data as output for the ith examination
N	Number of examinations.

4. EXPERIMENTAL RESULTS

The proposed methodology is evaluated with a prototype to know the performance of the proposed algorithms. CloudSim environment is used to simulate the performance of the two algorithms. SVMM and SVMP are the two algorithms whose performance details are presented in this section.

4.1 SVMM Performance

SVMM performance is evaluated in terms of the time taken for migration of the VM. The time is measured without the usage of the proposed SVMM and with its usage. There is significant performance improvement and Quality of Service (QoS) when SVMM is used.

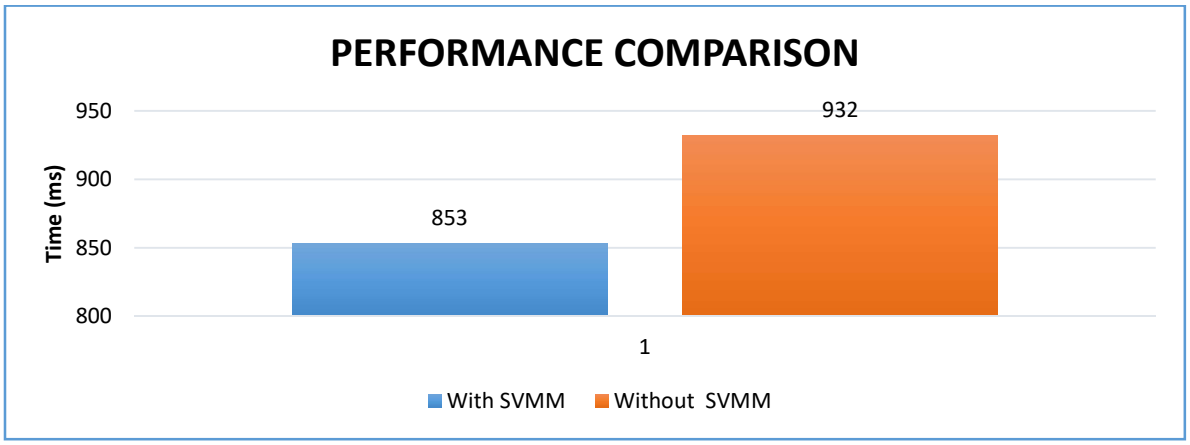

Figure 3:Performance Of SVMM

As presented in Figure 3, the performance of the live migration process is much better with the usage of SVMM as it could prevent live migration attacks. When there is an attack and SVMM is not in place, it took more time for live migration to defeat its underlying benefits.

4.2 SVMP Performance

SVMP performance is evaluated using two performance metrics such as MAPE and RMSE as discussed in the preceding section. As SVMP exploits different ML models, the results are provided for each model.

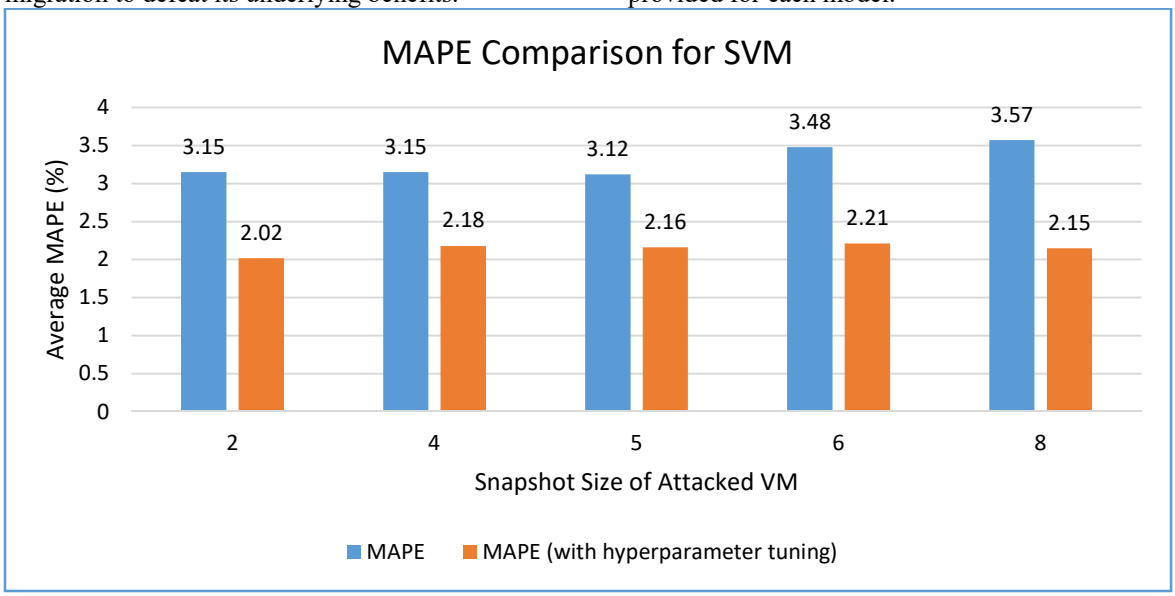

Figure 4:MAPE Performance Comparison When SVM Is Used

As presented in Figure 4, the average MAPE value is observed against the snapshot size of attacked VM. The least MAPE value indicates better performance. The observations are made with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model SVM and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 8, the MAPE value for SVM is 3.57 while the SVM with hyperparameter tuning shows it as 2.15. Thus it is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

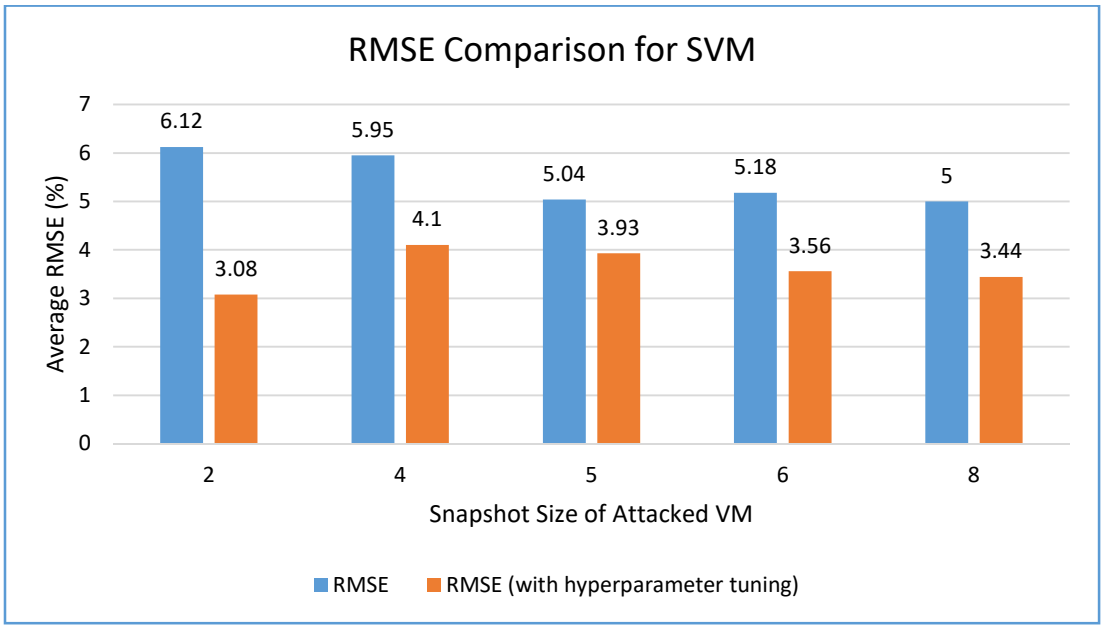

Figure 5: RMSE Performance Comparison When SVM Is Used

As presented in Figure 5, the average RMSE value is observed against the snapshot size of attacked VM. The least RMSE value indicates better performance. The observations are made with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model SVM and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 8, the RMSE value for SVM is 5 while the SVM with hyperparameter tuning shows it as 3.44. Thus it is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

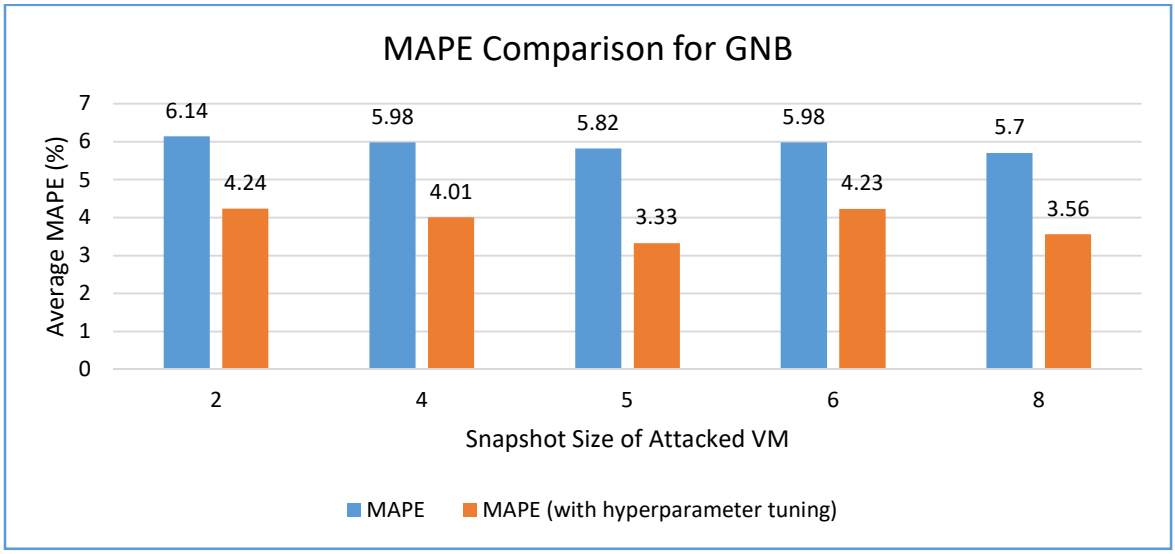

Figure 6: MAPE Performance Comparison When The GNB Model Is Used

As presented in Figure 6, the average MAPE value is observed against the snapshot size of attacked VM. The least MAPE value indicates better performance. The observations are made with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model GNB and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 8, the MAPE value for GNB is 5.7 while the GNB with hyperparameter tuning shows it as 3.56. Thus it is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

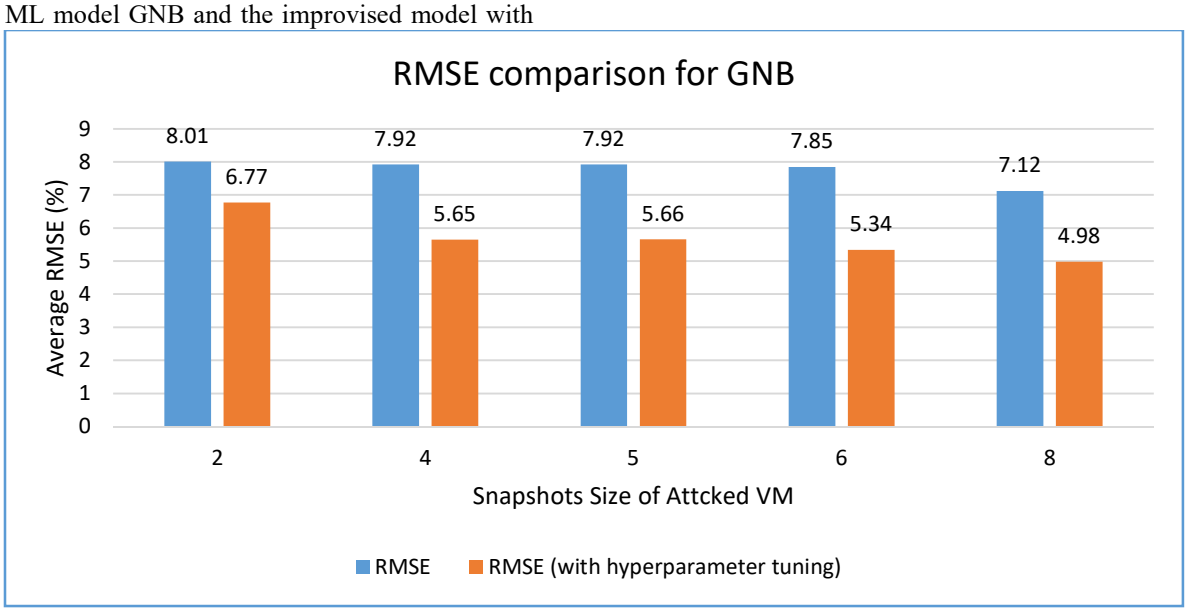

Figure 7: RMSE Performance Comparison When The GNB Model Is Used

As presented in Figure 7, the average RMSE value is observed against the snapshot size of attacked VM. The least RMSE value indicates better performance. The observations are made with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model GNB and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 8, the RMSE value for GNB is 7.12 while the GNB with hyperparameter tuning shows it as 4.98. Thusit is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

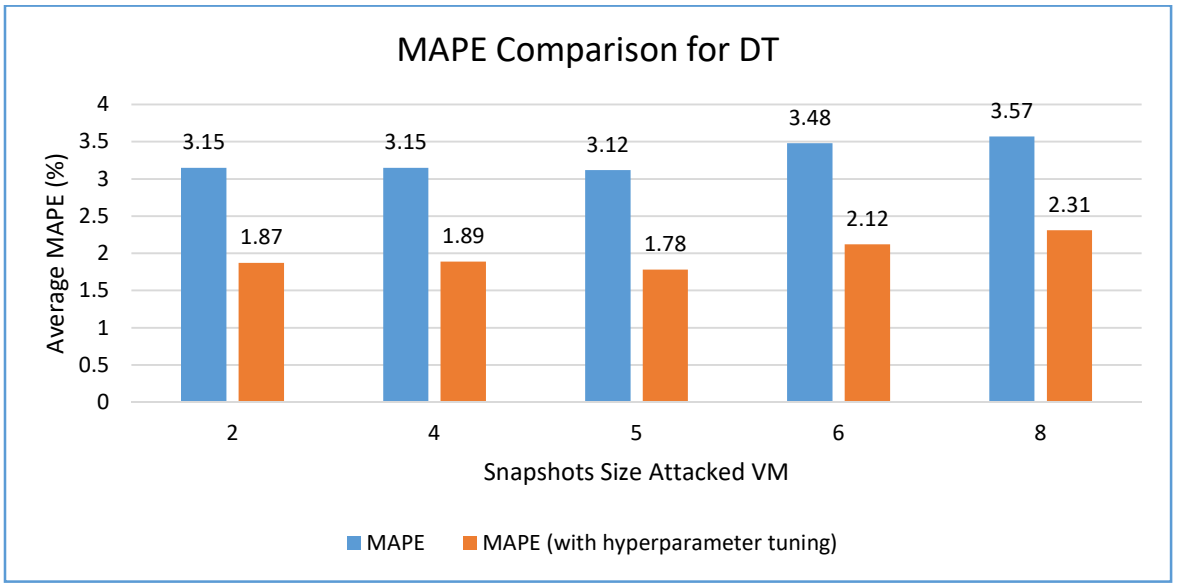

Figure 8: MAPE Performance Comparison When The DT Model Is Used

As presented in Figure 8, the average MAPE value is observed against the snapshot size of attacked VM. The least MAPE value indicates better performance. The observations are made with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model GNB and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 8, the MAPE value for DT is 3.57 while the DT with hyperparameter tuning shows it as 2.31. Thus it is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

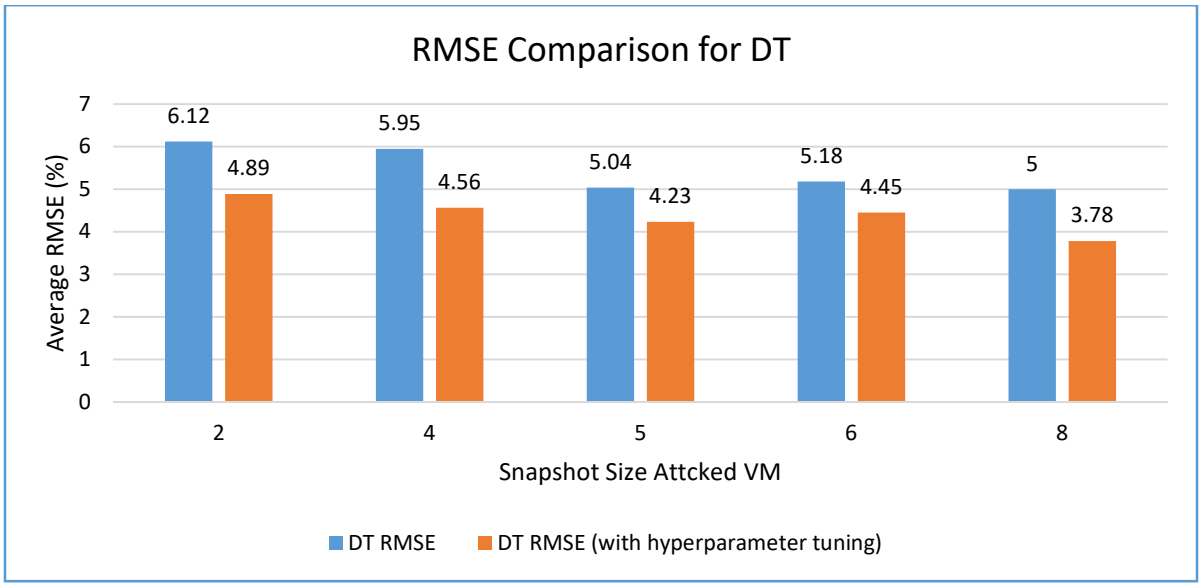

Figure 9: RMSE Performance Comparison When The DT Model Is Used

As presented in Figure 9, the average RMSE value is observed against the snapshot size of attacked VM. The least RMSE value indicates better performance. The observations are made

with different snapshot sizes of attacked VM such as 2, 4, 5, 6, and 8. With every size of snapshot, there is a clear difference between the ML model GNB and the improvised model with hyperparameter tuning. For instance, when the snapshot size of attacked VM is 5, the RMSE value for DT is 3.78 while the DT with hyperparameter tuning shows it as 2.31. Thus it is understood that there is a significant improvement in the persistence attack detection with hyperparameter tuning.

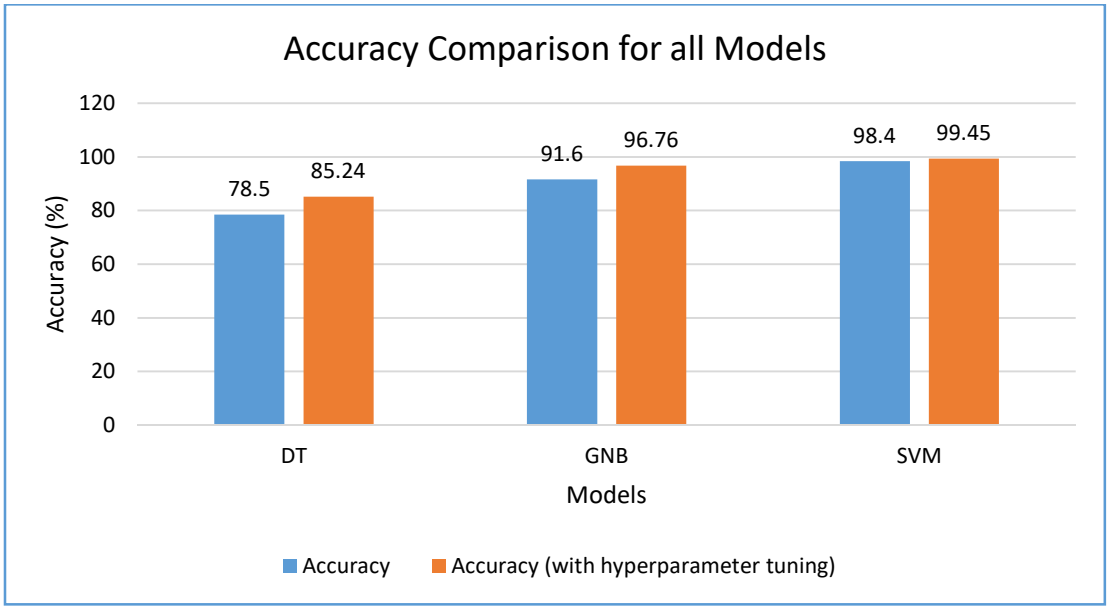

Figure 10: Accuracy Comparison Among All Models

As presented in Figure 10, the accuracy is observed for different ML models such as SVM, GNB, and DT. The accuracy of the models is compared with that of the models when hyperparameter tuning is made in the models associated with the proposed algorithm. It is observed from the results that DT exhibited the lowest accuracy with 78.5% and 85.24% respectively with and without hyperparameter tuning. SVM is the ML model that showed higher performance with 98.4% accuracy and 99.45% accuracy with hyperparameter tuning.

5. CONCLUSION AND FUTURE WORK

In this paper, we proposed a security framework that ensures that VM migration and VM persistence occur without causing cyber-attacks. The framework has two algorithms proposed to realize this objective. Safe Virtual Machine Migration (SVMM) is meant for protecting VM from attacks on the VM migration process while another algorithm known as Safe Virtual Machine Persistence (SVMP) focuses on preventing attacks on VM persistence. Both mechanisms are crucial for leveraging cloud performance and Quality of Service (QoS). The algorithms are implemented and an empirical study is made to evaluate the algorithms. The proposed framework is realized with a simulation study using CloudSim. The experimental results showed that the proposed approach is capable of handling attacks while VM is being migrated and when VM is being persisted. In the future, we intend to propose an integrated framework for preventing variousattacks that are launched through VM and hypervisor in virtualization environments.

REFERENCES

[1] K.E. Narayana;K. Jayashree; (2021). Survey on cross virtual machine side channel attack detection and properties of cloud computing as sustainable material . Materials Today: Proceedings, p1-6.

[2] Li, Yuqing; Dai, Wenkuan; Bai, Jie; Gan, Xiaoying; Wang, Jingchao; Wang, Xinbing (2018). An Intelligence-Driven Security-Aware Defense Mechanism for

Advanced Persistent Threats. IEEE Transactions on Information Forensics and Security, p1–16.

[3] Alshamrani, Adel; Myneni, Sowmya; Chowdhary, Ankur; Huang, Dijiang (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys & Tutorials, p1–25.

[4] Bahram, Sina; Jiang, Xuxian; Wang, Zhi; Grace, Mike; Li, Jinku; Srinivasan, Deepa; Rhee, Junghwan; Xu, Dongyan (2010). [IEEE 2010 IEEE International Symposium on Reliable Distributed Systems (SRDS) - New Delhi, Punjab India (2010.10.31-2010.11.3)] 2010 29th IEEE Symposium on Reliable Distributed Systems - DKSM: Subverting Virtual Machine Introspection for Fun and Profit. , p82–91.

[5] J. Vijaya Chandra1 ,Narasimham Challa2 and Sai Kiran Pasupuleti. (2015). Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform. Indian Journal of Science and Technology. 8 (28), p1-9.

[6] Li, Frankie; Lai, Anthony; Ddl, Ddl (2011). [IEEE 2011 6th International Conference on Malicious and Unwanted Software (MALWARE) - Fajardo, PR, USA (2011.10.18-2011.10.19)] 2011 6th International Conference on Malicious and Unwanted Software - Evidence of Advanced Persistent Threat: A case study of malware for political espionage. , p102–109.

[7] Friedberg, Ivo; Skopik, Florian; Settanni, Giuseppe; Fiedler, Roman (2015). Combating advanced persistent threats: From network event correlation to incident detection. Computers & Security, 48, p35–57.

[8] Hildenbrandt, Everett; Saxena, Manasvi; Rodrigues, Nishant; Zhu, Xiaoran; Daian, Philip; Guth, Dwight; Moore, Brandon; Park, Daejun; Zhang, Yi; Stefanescu, Andrei; Rosu, Grigore (2018). [IEEE 2018 IEEE 31st Computer Security Foundations Symposium (CSF) - Oxford, United Kingdom (2018.7.9-2018.7.12)] 2018 IEEE 31st Computer Security Foundations Symposium (CSF) - KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine. , p204–217.

[9] Hu, Pengfei; Li, Hongxing; Fu, Hao; Cansever, Derya; Mohapatra, Prasant (2015). [IEEE IEEE INFOCOM 2015 - IEEE Conference on Computer Communications - Kowloon, Hong Kong (2015.4.26-2015.5.1)] 2015 IEEE Conference on Computer Communications (INFOCOM) - Dynamic defense strategy against advanced persistent threat with insiders. , p747–755.

[10] Zhang, Fengzhe; Chen, Jin; Chen, Haibo; Zang, Binyu (2011). [ACM Press the Twenty-Third ACM Symposium - Cascais, Portugal (2011.10.23-2011.10.26)] Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles - SOSP '11 - CloudVisor. P1-14.

[11] Gharehpasha, Sasan; Masdari, Mohammad; Jafarian, Ahmad (2020). Virtual machine placement in cloud data centers using a hybrid multi-verse optimization algorithm. Artificial Intelligence Review, p1–37.

[12] Wang, Yichuan; Ma, Jianfeng; Lu, Di; Lu, Xiang; Zhang, Liumei (2014). From high-availability to collapse: quantitative analysis of “Cloud-Droplet-Freezing” attack threats to virtual machine migration in cloud computing. Cluster Computing, 17(4), p1369–1381.

[13] Win, Thu Yein; Tianfield, Huaglory; Mair, Quentin (2014). [IEEE 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC) - London, United Kingdom (2014.12.8-2014.12.11)] 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing - Virtualization Security Combining Mandatory Access Control and Virtual Machine Introspection, p1004–1009.

[14] Masdari, Mohammad; Zangakani, Mehran (2019). Green Cloud Computing Using Proactive Virtual Machine Placement: Challenges and Issues. Journal of Grid Computing, p1-33.

[15] Tian, Jing; Jing, Jiwu; Srivatsa, Mudhakar (2015). [Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering] International Conference on Security and Privacy in Communication Networks Volume 152 || A Secure Architecture for

Inter-cloud Virtual Machine Migration. , 10.1007/978-3-319-23829-6(Chapter 2), p24–35.

[16] Anita Choudhary1, Mahesh Chandra Govil2, Girdhari Singh1, Lalit K. Awasthi3, Emmanuel S. Pilli1* and DivyaKapil. (2017). A critical survey of live virtual machine migration techniques. Journal of Cloud Computing: Advances, Systems and Applications, p1-41.

[17] Ahmad, Raja Wasim; Gani, Abdullah; Hamid, SitiHafizah Ab.; Shiraz, Muhammad; Yousafzai, Abdullah; Xia, Feng (2015). A survey on virtual machine migration and server consolidation frameworks for cloud data centers. Journal of Network and Computer Applications, 52, p11–25.

[18] Hosseini Shirvani, Mirsaeid; Rahmani, Amir Masoud; Sahafi, Amir (2018). A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter: Taxonomy and challenges. Journal of King Saud University - Computer and Information Sciences, p1-20.

[19] Ajay Kumara M.A, ;Jaidhar C.D, (2015). [IEEE 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN) - Kuala Lumpur, Malaysia (2015.5.26-2015.5.28)] 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN) - Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment. , p28–33.

[20] Reeba, P. Jabalin; Shaji, R. S.; Jayan, J. P. (2016). [IEEE 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) - Nagercoil, India (2016.3.18-2016.3.19)] 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT) - A secure virtual machine migration using processor workload prediction method for cloud environment. p1–6.

[21] Ahmad, Naveed; Kanwal, Ayesha; Shibli, Muhammad Awais (2013). [IEEE 2013 2nd National Conference on Information Assurance (NCIA) - Rawalpindi, Pakistan (2013.12.11-2013.12.12)] 2013 2nd National Conference on Information Assurance (NCIA) - Survey on secure live virtual machine (VM) migration in Cloud. , p101–106.

[22]Natu, Varun; Duong, Ta Nguyen Binh (2017). [IEEE 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA) - Kanazawa (2017.11.22-2017.11.25)] 2017 IEEE 10th Conference on Service-Oriented Computing and Applications (SOCA) - Secure Virtual Machine Placement in Infrastructure Cloud Services., p26–33.

[23] Somani, Gaurav; Gaur, Manoj Singh; Sanghi, Dheeraj; Conti, Mauro; Buyya, Rajkumar (2017). DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, p30–48.

[24] Yu, Si; Gui, Xiaolin; Lin, Jiancai; Tian, Feng; Zhao, Jianqiang; Dai, Min (2014). A Security-Awareness Virtual Machine Management Scheme Based on Chinese Wall Policy in Cloud Computing. The Scientific World Journal, 2014, p1–12.

[25] Xu, Xiaolong; Liu, Guangpei; Zhu, Jie (2016). [IEEE 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) - Chengdu, China (2016.10.13-2016.10.15)] 2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) - Cloud Data Security and Integrity Protection Model Based on Distributed Virtual Machine Agents. , p6–13.

[26] Zhang, Fengzhe; Huang, Yijian; Wang, Huihong; Chen, Haibo; Zang, Binyu (2008). [IEEE 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference (APTC) - Wuhan, Hubei, China (2008.10.14-2008.10.17)] 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference - PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. , p9–18.

[27] Alvarenga, Igor D.; Rebello, Gabriel A. F.; Duarte, Otto Carlos M. B. (2018). [IEEE NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium - Taipei, Taiwan (2018.4.23-2018.4.27)] NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium -

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Securing configuration management and migration of virtual network functions using blockchain. , p1–9.

[28]Jia, Hefei; Liu, Xu; Di, Xiaoqiang; Qi, Hui; Cong, Ligang; Li, Jinqing; Yang, Huamin (2019). Security Strategy for Virtual Machine Allocation in Cloud Computing. Procedia Computer Science, 147, p140–144.

[29] Gharehpasha, Sasan; Masdari, Mohammad (2020). A discrete chaotic multi-objective SCA-ALO optimization algorithm for an optimal virtual machine placement in cloud data center. Journal of Ambient Intelligence and Humanized Computing, p1–17.