Scientific Research Publishing

Journal of Information Security, 2024, 15, 419-432
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

An Agent Based Model for Ransomware Detection and Mitigation in a Cloud System

N'golo Konate, Tenan Yeo

UFR Mathematiques et Informatiques, Université Felix-Houphouet Boigny, Abidjan, Cote d'Ivoire
Email: ingngolo@gmail.com

How to cite this paper: Konate, N. and Yeo, T. (2024) An Agent Based Model for Ransomware Detection and Mitigation in a Cloud System. *Journal of Information Security*, **15**, 419-432.
https://doi.org/10.4236/jis.2024.154024

Received: May 29, 2024
Accepted: July 29, 2024
Published: August 1, 2024

Abstract

The increasing trend toward dematerialization and digitalization has prompted a surge in the adoption of IT service providers, offering cost-effective alternatives to traditional local services. Consequently, cloud services have become prevalent across various industries. While these services offer undeniable benefits, they face significant threats, particularly concerning the sensitivity of the data they handle. Many existing mathematical models struggle to accurately depict the complex scenarios of cloud systems. In response to this challenge, this paper proposes a behavioral model for ransomware propagation within such environments. In this model, each component of the environment is defined as an agent responsible for monitoring the propagation of malware. Given the distinct characteristics and criticality of these agents, the impact of malware can vary significantly. Scenario attacks are constructed based on real-world vulnerabilities documented in the Common Vulnerabilities and Exposures (CVEs) through the National Vulnerability Database. Defender actions are guided by an Intrusion Detection System (IDS) guideline. This research aims to provide a comprehensive framework for understanding and addressing ransomware threats in cloud systems. By leveraging an agent-based approach and real-world vulnerability data, our model offers valuable insights into detection and mitigation strategies for safeguarding sensitive cloud-based assets.

Keywords

Cloud Computing, Information Security, Multi-Agent System, IaaS, Malware Propagation

1. Introduction

From the basic software to the full infrastructure, cloud systems provide services

at different levels to support organizational processes. Cloud computing enables organizations to scale their IT resources up or down quickly and easily, without the need for costly hardware upgrades. This can help organizations to respond more quickly to changing business needs and market conditions [1]. Unlike local infrastructures which require a major investment, organizations only pay for the resources needed in a cloud system. However depending on the type of cloud, providers in either organization should invest a lot in security. According to [2], there are four types of cloud computing, as seen in **Figure 1**, which are used in different fields of life with specific rules and respective specifications. Those four types rely on different types of layers and have specific roles:

- **Application layer** directly connected to the end-user defines the commands, responses, data types, and status reporting supported by the protocol.
- **Platform layer** reduces the workload support by the server consists of an operating system and application framework and sits on the top of the infrastructure layer.
- **Infrastructure layer:** Using virtualization technology, this layer establishes a pool of resources for computing and storage resources.
- **Infrastructure layer:** This layer creates a pool of resources for computation and storage through the use of virtualization technologies.

According to Markets and Markets, global public cloud services have a compound annual growth rate of 17.5%. Therefore the cyber security landscape is characterized by the regular emergence of new types of cyber threats and trends which constantly sophisticated and diverse for both individuals and organizations.

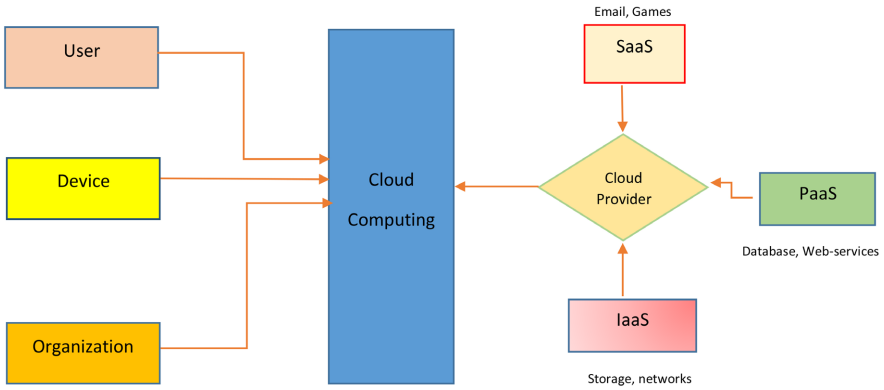

Figure 1. Cloud system environment.

While traditional attacks relied on signature-based detection, which made them easier to identify and counter, newer attacks use artificial intelligence (AI) characteristics like machine learning (ML) and deep learning to make malware more persuasive and easy to spread. With the number of services connected, the attacker can weaponize cyber AI for cyber attacks. [3] define weaponized AI as malicious AI algorithms that can degrade the performance and disrupt the normal functions of benign AI algorithms, while providing technological edge at-

tack scenarios in both cyberspace and physical spaces. Fighting cyber crimes require now a more comprehensive and safer approach [1]. New mathematical models and cyber defense tools are now oriented towards mathematical models [4], and deep learning [5] [6]. This paper is organized as follows. Section II discusses some essential concepts related to the paper as the new trends in cloud computing and the related threats. Section III will be dedicated to the multi-agents model formulation and the rule definitions. Discussions and limitations of the current model are presented in section VI. Finally we conclude the paper in section V.

2. Literature Review

2.1. Cloud Based System

Due to the information systems heterogeneity, cloud systems involve now every component such as end-users, networks, access management, and infrastructures. Therefore before diving into security issues, we need to understand cloud-based systems new trends. The cloud computing services as represented in **Figure 2** have been offered into three common service models including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [7]:

Figure 2. Cloud based architecture.

- **Software as a Service (SaaS):** Software as a Service, is a cloud-based service which can be accessed as an application directly via a web browser [8]. The main advantages of SaaS are accessibility, compatibility and operational manageability. Furthermore, SaaS models offer lower up-front costs than downloading and installing traditional software, making them more accessible to a wider range of businesses.
- **Platform as a Service (PaaS):** Platform as a Service (PaaS) is a complete cloud environment that includes everything developers need to build, run, and manage applications—from servers and operating systems to all the networking, storage, middleware, tools, and more.
- **Infrastructure as a Service (IaaS):** IaaS, is a cloud computing model that provides on-demand access to computing resources such as servers, storage, networking, and virtualization.

Since the malware is more likely to disrupt IaaS, let's dive into its new trends.

The user in an IaaS is in charge of managing the operating system and software applications, while the underlying network in the cloud infrastructure service is controlled by the cloud service provider [9]. As seen in **Figure 3**, IaaS network users can install multiple operating systems on the virtual machine images.

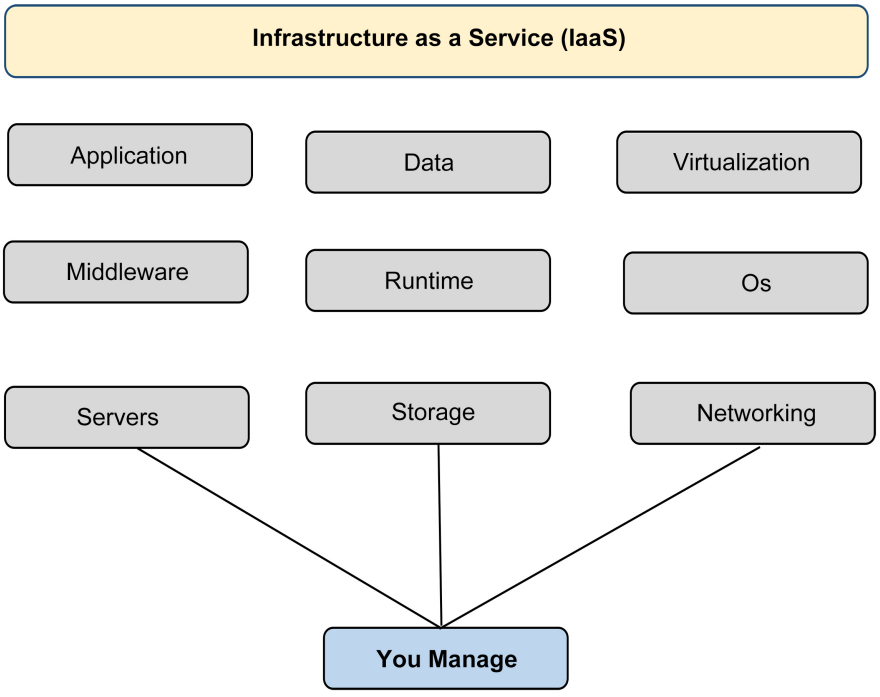

Figure 3. IasS network.

This horizontal view of the cloud system can be segmented into five essential characteristics [10]:

- **On-Demand Self-Service:** This feature enables the user to manage the concerned services

- **Broad Network Access:** This feature refers to the different exploitable breaches. It can also result in system improper configuration.
- **Resources Pooling:** Resources such as VMs, CPU and disk.
- **Rapid Elasticity:** Based on customers requirement. Resources can be scaled up or down.
- **Measure Services:** Resources should be monitored for continuous service.

The connection between the user and IaaS is done through either virtual private servers, a storage or a network. Then the request is sent to the real server through the virtual services resources.

IaaS security model: The security model in IaaS should take into account the three layers in a cloud architecture. Therefore, many components are used to monitor the environment [11].

2.2. Cyber Threats in Cloud System

Since IaaS offers computing capabilities and essential storage as standardized services across the network [12], the infrastructures face threats related to the underlying protocols. Therefore, appropriate safety measures should be taken care of.

A threat is a process whereby an intruder gathers, identifies and determines the risk associated with each area. Each threat identified during this process is analyzed in the exploit database. The threat faced by the cloud environment can emerge either on the user side or the provider side.

Since IaaS inherits data security's features in the SaaS layer [13] and Security concerns associated with SaaS layer are almost data centric. Some concerns about data security are:

- No suitable workload distribution.
- No suitable control for accessing sensitive data.
- Data theft issue due to malware(s).
- No proper view for data analysis.
- No suitable mechanism for controlling security in multi cloud environment.

The last question is a fundamental one, because good safety monitoring and control considerably enhance the third parties' confidence. While discussing security issues, it's important to note the impact of AI on cyber threats. Machine learning and artificial intelligence (AI) can be used to automate many cybersecurity tasks, such as intrusion detection, malware analysis and vulnerability assessment [14]. Since existing cyber defense infrastructures are becoming inadequate to address the increasing speed, and complex decision logic of AI-driven attacks [15]. We will introduce the AI driven propagation metrics to see their impact on the global infrastructure.

2.3. Mathematical Model in Information Security

Mathematical model to perform information system issues is a long problem discussed in the literature under different headings.

3. Methods

3.1. Cloud Architecture

As represented in Figure 3, Cloud physical architecture can be subdivided into provider and tenant parts.

At the provider side: The hypervisor allows each machine to work independently regarding the CPU, memory and NIC. An intruder who targets the hypervisor may be able to corrupt any resource. The runtime space is listed below [11]:

- **Guest VM User-Space:** The attacker could manage to break out from a guest by exploiting a missing check in the QEMU-KVM user-space driver.
- **Guest VM Kernel-Space:** In an IaaS cloud environment, tenants have the flexibility to operate a chosen operating system. Therefore, an intruder could implement a malicious para-virtualized front-end driver and exploit a vulnerability in the back-end driver.
- **Hypervisor Host OS:** Intruder could get into one host and grant the administrator privilege

On the user side: Hypervisor provides a resource isolation to the tenant. Therefore a multi-tenancy occurs. Though it increases the architecture performance, it increases the probability that a legal and malicious user can be located in the same physical machine.

3.2. Security Model

IaaS particularly among clouds offers services that make it difficult to a global model for all the architecture. Therefore, the Model for IaaS Security and Privacy (MISP) is the one retained for this paper [16]. As represented in Figure 4, the security model is organized in cubical form with three planes defined as shown in Figure 4.

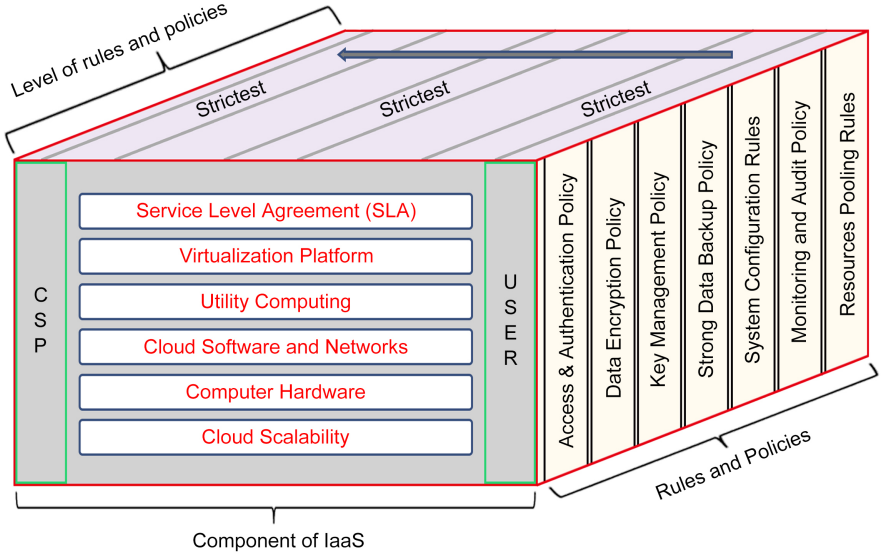

Figure 4. IaaS's security model.

The first plan exhibits aspects of Infrastructure as a Service (IaaS), involving the cloud computing user and the Cloud Service Provider (CSP) as typical stakeholders. They typically collaborate to uphold the security and confidentiality of the infrastructure model.

3.3. Multi Agent System Proposed

3.3.1. General Presentation of the Agents

The agents involved in a system are:

- **Virtual Machine:** Virtual machine represents a virtual implementation of a computer or server through the operating system. A VM can be considered as a node for many users since it can host many shared documents. Therefore, it has the attributes of vulnerability status, infection status, and the data it hosts. VMs are the primary target of ransomware.
- **Computer Agents:** are either virtual or physical machines that interact with the cloud system. They are the endpoints of the global infrastructure. Being manipulated by unaware users makes them the most vulnerable part of our system. Therefore, they are susceptible to various attacks from infectious VMs or users' malicious files.
- **Mobile Phones:** They include all mobile devices. Since they interact directly with the system, they can be vectors for ransomware propagation.
- **Intrusion Detection System:** They assess and evaluate cloud system security policy. Mostly based on signature, anomaly or machine learning algorithms detection systems; it monitors network traffic, file systems, and other activities to identify suspicious behavior indicative of ransomware activity.
- **Attackers:** are the ones who try to disrupt the cloud system using various attackers. They can use misconfigured systems or exploit well-known vulnerabilities.

3.3.2. Representation of the Multi-Agent Model in the Cloud System Value Chain

The critical component of an IaaS cloud architecture is the cloud OS, which manages the physical and virtual structures and controls the supply of virtual resources in line with the needs of the user goods and services [17]. However, the OS cannot be taken in the context of a cloud system without the VM.

The Virtual Machine Agent (VMA) provides virtualized computing resources on-demand. It's in charge of running applications and services, allocating and managing scalability and flexibility in resources allocation, and ensuring isolation and security of a virtualized environment.

The Computer Agents (CA) executes computational tasks and processing data. The computer agent interacts with other agents in the cloud system. Since it hosts applications and launches tasks, it can be the attack source.

The Mobiles Phones Agent (MPA) accesses cloud-based applications and data remotely, ensuring the security and privacy of data transmitted to and from the cloud.

Although IaaS security is an ongoing process, its implementation must correspond to the architecture and security policy. However, the security model retains as much as generic to be implemented in different environments.

The IDS Agent (IDSA) analysis workflow follows those specifications:

- **Customization:** In addition to the known rules defined in public repositories, the IDSs should have their own rules related to our infrastructures (evaluate component criticality, assess the infrastructure propagation using packet, and adopt adaptation actions).
- **Scalability:** The number of deployed SAIDS IDSs should adjust to varying conditions: load of the network trac monitored, number of physical servers in the data center, and number of VMs in the virtual infrastructure [11].
- **Security and Correctness:** This should be achieved with a trust-based definition of false positive and true positive.

3.4. Dynamic Equation of VM

Each agent A_i is represented by a state vector x_i where $i \in 1,\cdots,N$ and t represent the time. The dynamics of resources allocations of VM_i are based on its own resource demand and the resource demands of other agents (VM, CA and PA). The VMi is therefore formulated as:

$$\dot{x}_i(t) = \frac{1}{m_i}\sum_{j\neq i}\alpha_{ij}\left(x_i(t) - x_j(t)\right) \tag{1}$$

where

- $x_i(t)$ represents the resources allocations of VM_i at time *t.*
- m_i is the responsiveness coefficient of VM_i.
- α_{ij} is the interaction strength between VM_i and VM_j.
- The summation term represents the influence of neighboring VM on the resource allocation of VM_i.

Let's denote $\mu_i(t)$, the impact of malware on VM_i at time *t.* The dynamic equation of VM_i can therefore be expressed as

$$\dot{x}_i(t) = \frac{1}{m_i}\sum_{j\neq i}\alpha_{ij}\left(x_i(t) - x_j(t)\right) + \mu_i(t) \tag{2}$$

Since the malware considered will be used in many scenarios, it's formulated as:

$$\mu_i(t) = \beta_i \cdot \delta_i(t) \tag{3}$$

where:

- β_i stand for the impact of malware depending on the VM criticity.
- δ_i represent the impact of malware on VM_i. Considered the VM can be at any time infected by malware $\delta_i(t)$ is expressed using the Dirac delta function.

$$\delta_i(t) = \begin{cases} +\infty & t = 0\,(\text{infected}), \\ 0 & t \neq t_0\,(\text{not infected}) \end{cases} \tag{4}$$

Therefore $\delta_i(t) = \delta_i(t - t_0)$. Incorporating this into the dynamic equations for VM_i, we get

$$\dot{x}_i(t) = \frac{1}{m_i} \sum_{j \neq i} \alpha_{ij} \left(x_i(t) - x_j(t) \right) + \beta_i \delta_i(t - t_0) \tag{5}$$

3.5. Dynamic Equation of Computer Agent

$$\dot{y}_i(t) = \frac{1}{m_i} \sum_{j \neq i} \gamma_{ij} \left(y_i(t) - x_j(t) \right) + \beta_i \delta_i(t - t_0) \tag{6}$$

where

- $y_i(t)$ represents the resources allocations of CA_i over time *t.*
- m_i is the responsiveness coefficient of VM_i.
- γ_{ij} is the interaction strength between VM_i and *CAx.*
- The summation term represents the influence of neighboring *VM* on the resource allocation of the *CA.*
- β_i is the impact of the malware on the *CA.*
- $\delta(t - t_0)$ is the Dirac delta function representing the impact of malware on the *CA* at time t_0.

3.6. Mathematical Formulation of Malware Propagation

The mathematical of malware propagation is formulated as the one in [18] [19]:

$$N = S_1(t) + S_f(t) + S_i(t) + C_a(t) \tag{7}$$

where S_f are susceptible devices undergoing concurrent attacks but not yet infected (victim of attack Type 2), and S_1 are vulnerable devices attacked for the first time (victim of attack Type 1); S_i are vulnerable devices undergoing simultaneous attacks, one of which has already been successful (attack type 3 victim); and $C_a[T]$ are devices that have already contracted an infection and are further attacking the network (attack type 4 victim). Additionally, $C_a[T]$ stands for any device whose state—such as permanently immune devices or malware-inaccessible devices—cannot alter following a malware assault.

4. Results and Discussions

To investigate malware propagation in the clouds the different agents are subdivided as stated in Equation (7) (susceptibles, vulnerables, infected and computer agent). **Figure 5** shows that the malware spread faster in Computer Agent rather than inside the IaaS during a single threat from any part of the system. the computer is used by humans, who are the weakest link in the security chain. Furthermore, security patches are more likely to be applied to core network infrastructures rather than to computer

Moreover, in **Figure 6**, the Cloud's components performances decrease significantly. This is due to the fact that malware consumes cloud's internal resources. And, some particular malware increases file sizes.

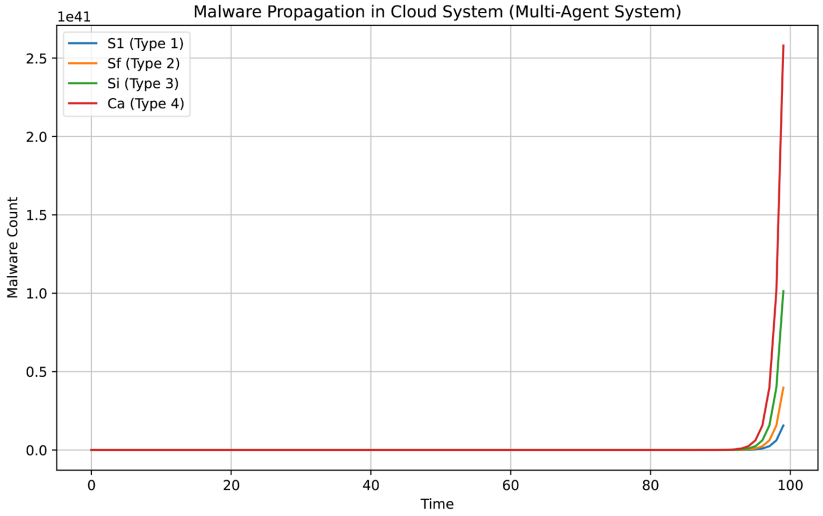

Figure 5. Malware propagation in cloud system.

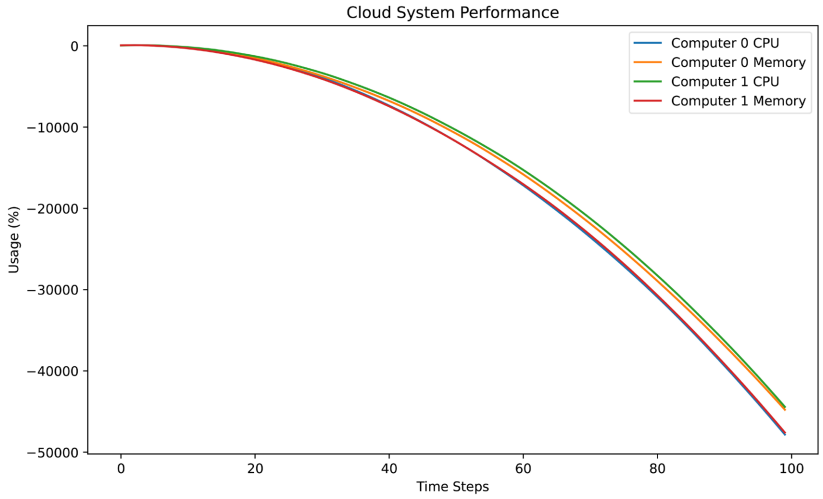

Figure 6. Clouds SYSTEM global performances under multiple infections.

Figure 7 shows the combined effect of responsiveness coefficient, interaction strength, and initial infection points on the mean resource allocation over time. Moreover, higher interaction strengths indicate a stronger influence between VMs and Computer Agents, leading to faster spread of malware. The mesh grid visualizes the combined effect of responsiveness coefficient, interaction strength, and initial infection points on the mean resource allocation over time.

Figure 8 shows that higher interaction strengths indicate a stronger influence between VMs and Computer Agents, leading to faster spread of malware while Lower interaction strengths result in more isolated resource allocation patterns, limiting the impact of malware propagation.

Figure 9 shows that earlier initial infection points lead to quicker initiation of malware propagation. On the other hand later initial infection points delay the onset of malware propagation, giving more time for security measures to be deployed.

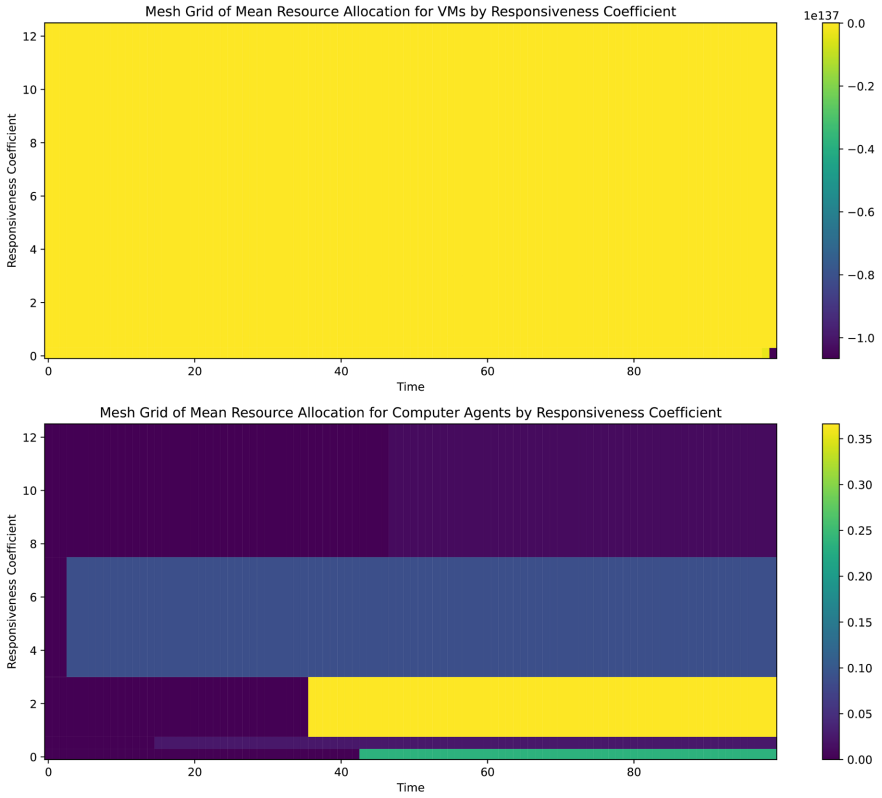

Figure 7. Resource allocations by responsiveness coefficient.

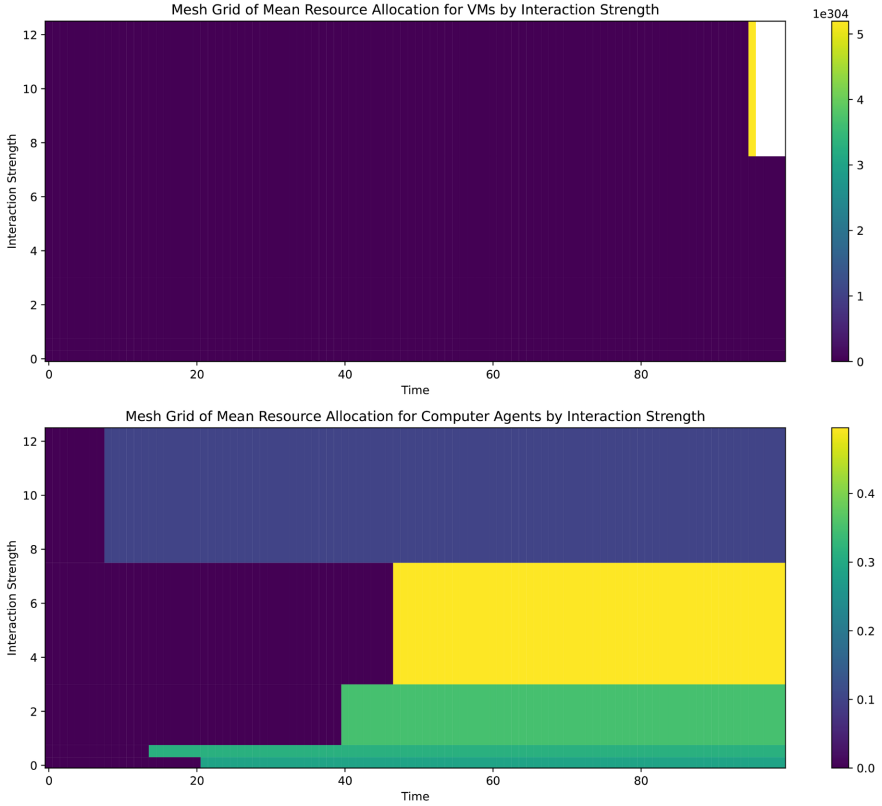

Figure 8. Resource allocations by interaction strength.

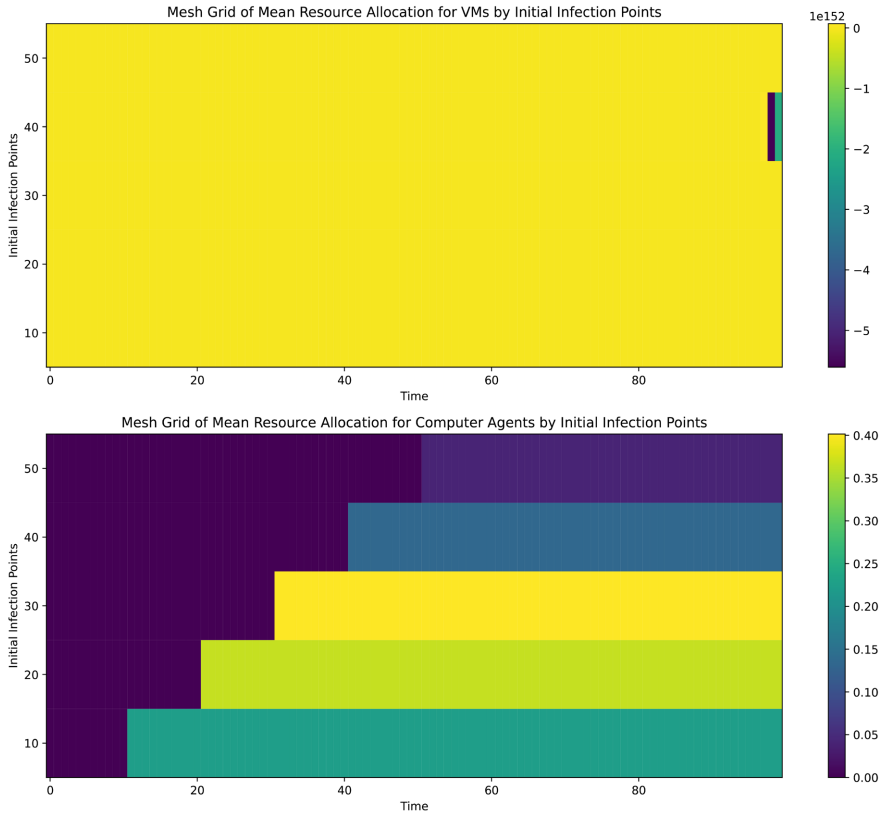

Figure 9. Resource allocation by initial infection points.

5. Conclusion

The formulated model shows malware propagation in a cloud system. Therefore, It can be used to adjust the interaction strength values between the different agents that could significantly impact the overall security posture of the system, with stronger interactions potentially increasing vulnerability to rapid malware dissemination. Moreover the timing of initial infection points can determine the window of opportunity for security defenses to detect and mitigate malware threats. This indicator can be used to select adequate protection tools. Finally Identifying clusters of high resource allocation can guide security practitioners in prioritizing response efforts and implementing targeted security measures to contain malware outbreaks.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Islam, R., Patamsetti, V., Gadhi, A., Gondu, R.M., Bandaru, C.M., Kesani, S.C. and Abiona, O. (2023) International Journal of Communications. Network and System Sciences Scientific Research Publishing. Scientific Research Publishing.

[2] Ullah, A., Nawi, N.M. and Ouhame, S. (2021) Recent Advancement in VM Task

Allocation System for Cloud Computing: Review from 2015 to2021. *Artificial Intelligence Review*, **55**, 2529-2573. https://doi.org/10.1007/s10462-021-10071-7

[3] Yamin, M.M., Ullah, M., Ullah, H. and Katt, B. (2021) Weaponized AI for Cyber Attacks. *Journal of Information Security and Applications*, **57**, Article ID: 102722. https://doi.org/10.1016/j.jisa.2020.102722

[4] Balarezo, J.F., Wang, S., Chavez, K.G., Al-Hourani, A. and Kandeepan, S. (2022) A Survey on DOS/DDOS Attacks Mathematical Modelling for Traditional, SDN and Virtual Networks. *Engineering Science and Technology, an International Journal*, **31**, Article ID: 101065. https://doi.org/10.1016/j.jestch.2021.09.011

[5] Almalaq, A., Albadran, S. and Mohamed, M. (2022) Deep Machine Learning Model-Based Cyber-Attacks Detection in Smart Power Systems. *Mathematics*, **10**, Article No. 2574. https://doi.org/10.3390/math10152574

[6] Aldhyani, T.H.H. and Alkahtani, H. (2023) Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. *Mathematics*, **11**, Article No. 233. https://doi.org/10.3390/math11010233

[7] Gourisaria, M.K., Samanta, A., Saha, A., Patra, S.S. and Khilar, P.M. (2020) An Extensive Review on Cloud Computing. In: Raju, K.S., *et al.*, Eds., *Data Engineering and Communication Technology*, Springer, 53-78. https://doi.org/10.1007/978-981-15-1097-7_6

[8] Laato, S., Mäntymäki, M., Islam, A.K.M.N., Hyrynsalmi, S. and Birkstedt, T. (2022) Trends and Trajectories in the Software Industry: Implications for the Future of Work. *Information Systems Frontiers*, **25**, 929-944. https://doi.org/10.1007/s10796-022-10267-4

[9] Soh, J., Copeland, M., Puca, A. and Harris M. (2020) Microsoft Azure: Planning, Deploying, and Managing the Cloud. Springer.

[10] Sunyaev, A. (2020) Cloud Computing. In: *Internet Computing*. Springer, 195-236. https://doi.org/10.1007/978-3-030-34957-8_7

[11] Giannakou, A., Rillling, L., Pazat, J.-L., Majorczyk, F. and Morin, C. (2015) Towards Self Adaptable Security Monitoring in IaaS Clouds. 2015 15*th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, Shenzhen, China, 2015, 737-740. https://doi.org/10.1109/CCGrid.2015.133

[12] Tabrizchi, H. and Kuchaki Rafsanjani, M. (2020) A Survey on Security Challenges in Cloud Computing: Issues, Threats, and Solutions. *The Journal of Supercomputing*, **76**, 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

[13] Parast, F.K., Sindhav, C., Nikam, S., Yekta, H.I., Kent, K.B. and Hakak, S. (2022) Cloud Computing Security: A Survey of Service-Based Models. *Computers & Security*, **114**, Article 102580.

[14] Admass, W.S., Munaye, Y.Y. and Diro, A.A. (2024) Cyber Security: State of the Art, Challenges and Future Directions. *Cyber Security and Applications*, **2**, Article ID: 100031. https://doi.org/10.1016/j.csa.2023.100031

[15] Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L. and Pospelova, V. (2022) The Emerging Threat of AI-Driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, **36**, Article ID: 2037254. https://doi.org/10.1080/08839514.2022.2037254

[16] Sahu, I.K. and Nene, M.J. (2021) Model for IaaS Security Model: MISP Framework. 2021 *International Conference on Intelligent Technologies* (*CONIT*), Hubli, 25-27 June 2021, 1-6. https://doi.org/10.1109/conit51480.2021.9498375

[17] Hu, V.C., Iorga, M., Bao, W., Li, A., Li, Q.H., Gouglidis, A., *et al.* (2020) General

Access Control Guidance for Cloud Systems, NIST Special Publication, 800-210. https://doi.org/10.6028/NIST.SP.800-210

[18] Carnier, R.M., Li, Y., Fujimoto, Y. and Shikata, J. (2024) Deriving Exact Mathematical Models of Malware Based on Random Propagation. *Mathematics*, **12**, Article No. 835. https://doi.org/10.3390/math12060835

[19] Aslan, O., Ozkan-Okay, M. and Gupta, D. (2021) Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment. *IEEE Access*, **9**, 83252-83271. https://doi.org/10.1109/access.2021.3087316