Modeling the Dynamic Spread of Malware to Enhance Security in Cloud Computing

Sai Ganesh Darbha[1], Dr.K Venkata Nagendra[2]
[1,2]*Department of Computer Science and Engineering, SRKR Engineering College. Bhimavaram, India*

***Abstract*—Cloud computing, particularly in the realms of cloud-fog-edge computing, offers various services globally and is essential to cyber-physical-social systems (CPSS). Virtualization stands out as a key enabling technology in cloud computing, facilitating the dynamic deployment of computing tasks through virtual machine (VM) migration. Consequently, securing the virtual environment in the cloud is of utmost importance. This paper aims to tackle the challenge of malware spread among VMs within infrastructure as a service (IaaS) frameworks. First, a dynamic propagation model is introduced to identify key factors influencing malware transmission, with a particular focus on the role of antivirus software installed in VMs. Following this, a theoretical analysis of the model is conducted using differential dynamics, allowing for a deeper understanding of malware dissemination in an infected cloud environment. Finally, numerical simulations are performed to validate the relevance and effectiveness of the proposed model.**

***Index Terms*—Cloud Computing, Virtual Machine, Infrastructure as a Service, Virtualization, Industrial Internet of Things, Internet of Things**

I. INTRODUCTION

Cyber-physical-social systems (CPSS) are able to make our daily lives more intelligent and convenient through providing forward-looking and personalized services [6]. With the advent of the big data era and the popularity of the Internet of Things in the future, CPSS services will inevitably require various data support including the global historical data and the local real-time data, which will involve many issues such network communication (e.g., [7], [8]), data storage, processing and applications (e.g., [9], [10]). In this context, researchers are vigorously developing cloudfog-edge computing in recent years. Specifically, fog-edge computing has been widely applied to process the local realtime data, which is an important and effective supplement of cloud computing. As a powerful paradigm for implementing the data-intensive applications, cloud computing has an irreplaceable role in storing and processing data. It can offer services such as infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) for users on demand.

As one of the most significant techniques of cloud computing, virtualization breaks the boundaries of time and space. Particularly, it can divide a physical computing device into more virtual machines (VMs) with the same functionality and realize the dynamic deployment of computing tasks through the migration of VMs. There is no doubt that virtualization will greatly improve resource utilization and save system management costs [11]. Unfortunately, virtualization also introduces new vulnerabilities that are becoming the attack target of malware.

The original malware developed to avoid virtual systems, but due to various factors such as profit and benefit, malware makers began to target all computing devices, including physical and virtual machines [12]. Because the Internet has strong propagation ability and is also the most important carrier of computer virus transmission, so once malware appears in a physical or virtual machine, it will spread rapidly in the network, which may cause great damage to human beings, ranging from economic losses to serious threats to human life. Consequently, it is essential to investigate how to protect the virtual environment from malware attack in the cloud.

1.1 Objective**:** This study aims to analyze malware propagation in cloud computing environments, focusing on virtualization within the Infrastructure as a Service (IaaS) model. A dynamical propagation model is developed to assess key factors influencing malware spread, particularly the role of antivirus software in virtual machines (VMs). Using differential

dynamics, the model provides insights into malware dissemination behavior. The research further includes theoretical analysis and numerical simulations to evaluate the model's applicability and effectiveness in securing cloud environments.

1.2 Problem Statement: The dynamic nature of virtualization in cloud computing, particularly virtual machine (VM) migration, increases the risk of malware propagation, making security challenges more complex due to rapid deployment and interaction among multiple VMs.

- Cloud computing, especially under the Infrastructure as a Service (IaaS) model, relies heavily on virtualization, where malware can exploit vulnerabilities, spread rapidly across VMs, and compromise system integrity, posing serious threats to cloud security and reliability.
- Cloud service providers, businesses, and end-users relying on cloud infrastructure are significantly affected, facing risks such as data breaches, service disruptions, and financial losses due to the uncontrolled spread of malware across interconnected virtual environments.
- Malware propagation in cloud computing leads to compromised data confidentiality, reduced system performance, increased recovery costs, potential regulatory non-compliance, and trust issues, ultimately impacting cloud adoption and limiting the full potential of cloud-based cyber-physical-social systems (CPSS).
- To mitigate malware spread, we propose a dynamical propagation model that analyzes key influencing factors, including antivirus implementation in VMs, using differential dynamics and simulations to enhance security strategies in cloud computing environments.

II. LITERATURE SURVEY

Cyber-physical-social systems (CPSSs) [1] represent an emerging paradigm encompassing the cyber world, physical world and social world. One of the main purposes of CPSSs is to provide high-quality, proactive, and personalized services for humans. For CPSSs to realize this purpose, a novel services framework is needed. In this article, we present a tensor-based cloud-edge computing framework that mainly includes the cloud and edge planes. The cloud plane is used to process large-scale, long-term, global data, which can be used to obtain decision making information such as the feature, law, or rule sets. The edge plane is used to process small-scale, short-term, local data, which is used to present the real-time situation. Also, personalized services will be directly provided for humans by the edge plane according to the obtained feature, law, or rule sets and the local high-quality data obtained in the edge plane. Then a tensor-based services model is proposed to match the requirement of users in the local CPSS. Finally, a case study about CPSS services is proposed to demonstrate the application features of the proposed framework.

Recently, the Industrial Internet of Things (IIoT) is attracting growing attention from both academia and industry. [2]. Meanwhile, trust-based communication is widely utilized in various systems. In this article, studying the performance of IIoT, we investigate trust-based communication for IIoT. In particular, devoting attention to sensor- cloud, which is a paradigm of IIoT, we propose three types of trust-based communication mechanisms for sensor-cloud. Furthermore, with numerical results, we show that trust-based communication can greatly enhance the performance of sensor-cloud. Eventually, open research issues with respect to trust-based communication for sensor-cloud are discussed.

Radio frequency identification (RFID) [3] systems, as one of the key components in the Internet of Things (IoT), have attracted much attention in the domains of industry and academia. In practice, the performance of RFID systems rather relies on the effectiveness and efficiency of anti-collision algorithms. A large body of studies have recently focused on the anti-collision algorithms, such as the Q-algorithm (*QA*), which has been successfully utilized in EPCglobal Class-1 Generation-2 protocol. However, the performance of those anti-collision algorithms needs to be further improved. Observe that fully exploiting the pre-processing time can improve the efficiency of the *QA* algorithm. With an objective of improving the performance for anti-collision, we propose a Nested Q-algorithm (*NQA*), which makes full use of such pre-processing time and incorporates the advantages of both Binary Tree (*BT*) algorithm and *QA* algorithm. Specifically, based on the expected number of collision tags, the *NQA* algorithm can adaptively select either *BT* or *QA* to identify collision tags.

Extensive simulation results validate the efficiency and effectiveness of our proposed *NQA* (i.e., less running time for processing the same number of active tags) when compared to the existing algorithms.

The growing volume of network traffic and gradual deployment of SDN devices [4] initiate a new era in which one distinguished feature is the application of big data technology to SDNs for construction of flexible, scalable, and self-managing networks. The primary purpose of this article is to develop a novel tensor-based model for efficient provisioning of QoS in software defined networks. First, a forwarding tensor model is proposed to formalize the networking functions in the data plane; then a controlling tensor model is presented for routing path recommendation in the control plane. Finally, the article introduces a transition tensor model for network traffic prediction and QoS provisioning. The three models can automatically monitor the network state, recommend routing paths and predict network traffic, respectively. A case study to recommend routing paths is investigated in the article.

Telecommunication networks are evolving toward [5] a data-center-based architecture, which includes physical network functions, virtual network functions, as well as various types of management and orchestration systems. The primary purpose of this type of heterogeneous network is to provide efficient and convenient communication services for users. However, the diverse factors of a heterogeneous network such as bandwidth, delay, and communication protocol, bring great challenges for routing recommendations. In addition, the growing volume of big data and the explosive deployment of heterogeneous networks have started a new era of applying big data technologies to implement routing recommendations. In this article, a tensor-based big-data-driven routing recommendation framework, including the edge plane, fog plane, cloud plane, and application plane, is proposed. In this framework, a tensor-based, holistic, hierarchical approach is introduced to generate efficient routing paths using tensor decomposition methods. Also, a tensor matching method including the controlling tensor, seed tensor, and orchestration tensor is employed to realize routing recommendation. Finally, a case study is used to demonstrate the key processing procedures of the proposed framework.

III. SYSTEM ANALYSIS

3.1 EXISTING SYSTEM: Generally, the following three aspects will accelerate the spread of malware in the cloud. Firstly, the migration of VMs will facilitate the diffusion of malware [8], [9]. By using the vulnerabilities of VMs to implant malware, criminals can utilize the migration of VMs to achieve the purpose of malicious attack. Very importantly, the migration of VMs plays a key role in cloud computing, by which the dynamic deployment of computing tasks can be implemented. Secondly, the homogeneity of VMs will also benefit the propagation of malware [10]. Here, the homogeneity mainly means that VMs have the homogeneous structure and settings, and the installed softwares are similar. In practice, there are a large number of VMs in the cloud, if they are configured one by one, it will not only take a lot of time, but also be prone to errors. For convenience, only one of them is usually configured, and then the others are generated by copying it. These operations can now be done automatically.

3.1.1 DISADVANTAGES OF EXISTING SYSTEM:

- VM migration increases malware spread, allowing attackers to exploit vulnerabilities and propagate threats across multiple virtual machines, making security control and isolation more challenging in cloud environments.
- Homogeneity in VM configurations creates a security risk, as malware can exploit identical system structures and installed software, leading to widespread infections with minimal effort from attackers.
- Manual or automated replication of VM settings without proper security considerations can introduce system-wide vulnerabilities, making it easier for malware to penetrate and persist within the cloud infrastructure.
- Lack of an advanced security mechanism to detect and isolate infected VMs in real-time leads to slower response times, increasing the risk of malware propagation before effective countermeasures are implemented.

3.2 Proposed System: Now-a-days Cloud computing provides several advantages to customer to deploy and run their application with lesser cost and without making any infrastructure investments like purchasing hardware's and software's. Customers can deploy their application on cloud by using any service from

available various services such as Platform as a service (PAAS), Infrastructure as a Service (IAAS) and Software As a Service (SAAS). The main advantage of cloud computing is virtualizations where cloud servers can create or destroy virtual machine upon customer requirements. If more requests are coming then cloud may create more number of VM's and if less requests are coming then it will destroy extra VM's and add to available resources pool.

3.2.1 Advantages of proposed system:

1. Cloud computing enhances flexibility by dynamically scaling resources through virtualization, efficiently managing computing demands while ensuring optimized resource utilization without unnecessary infrastructure investments.
2. The automated creation and destruction of virtual machines based on workload demand improve efficiency, ensuring seamless service delivery while reducing the chances of malware persistence in inactive or unused VMs.
3. Cloud services, including IaaS, PaaS, and SaaS, provide customers with secure and cost-effective deployment options, reducing the need for expensive on-premise hardware and software purchases.
4. Virtualization technology improves security management by enabling real-time monitoring, automated threat detection, and rapid VM isolation, reducing malware propagation and enhancing cloud infrastructure protection.

IV. SYSTEM ARCHITECTURE

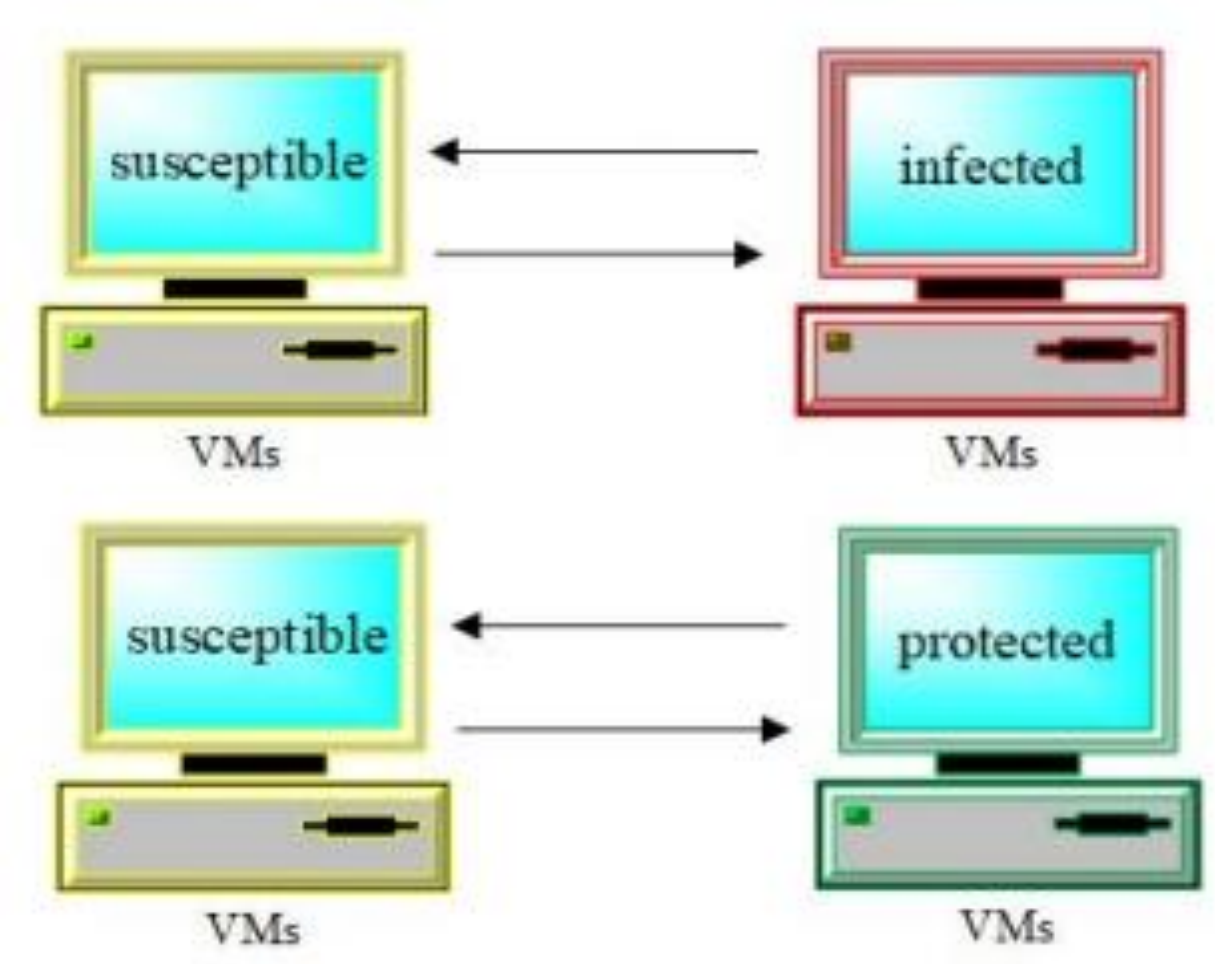
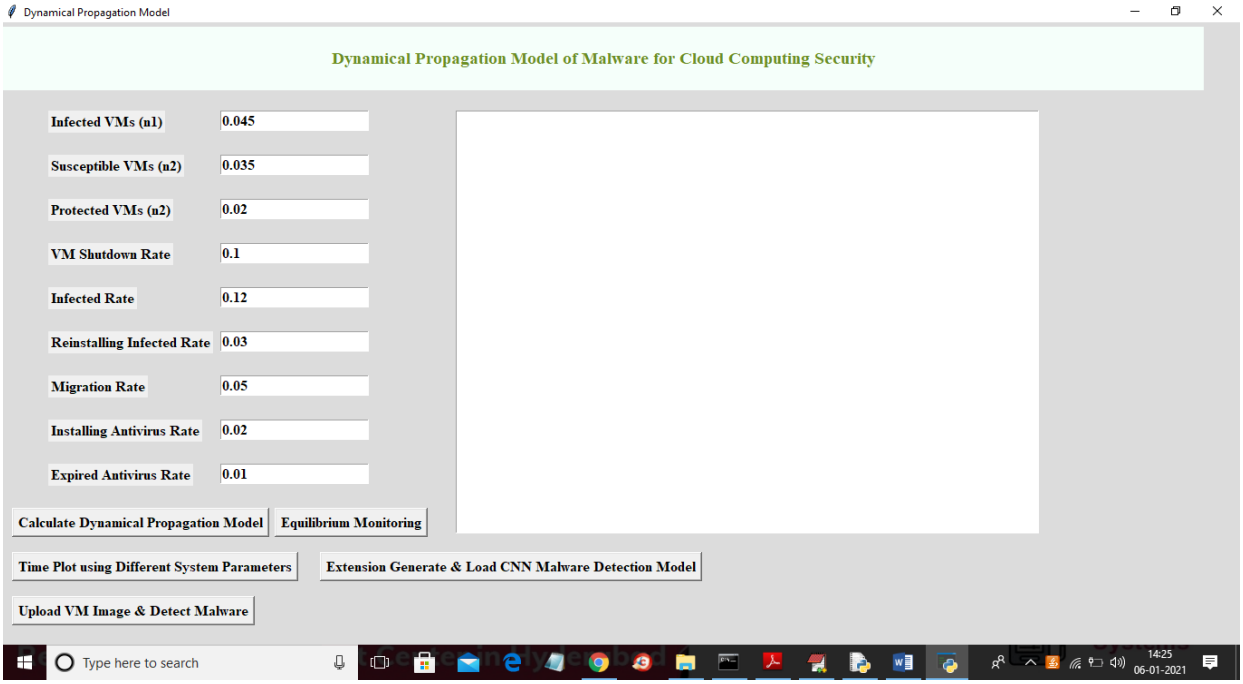


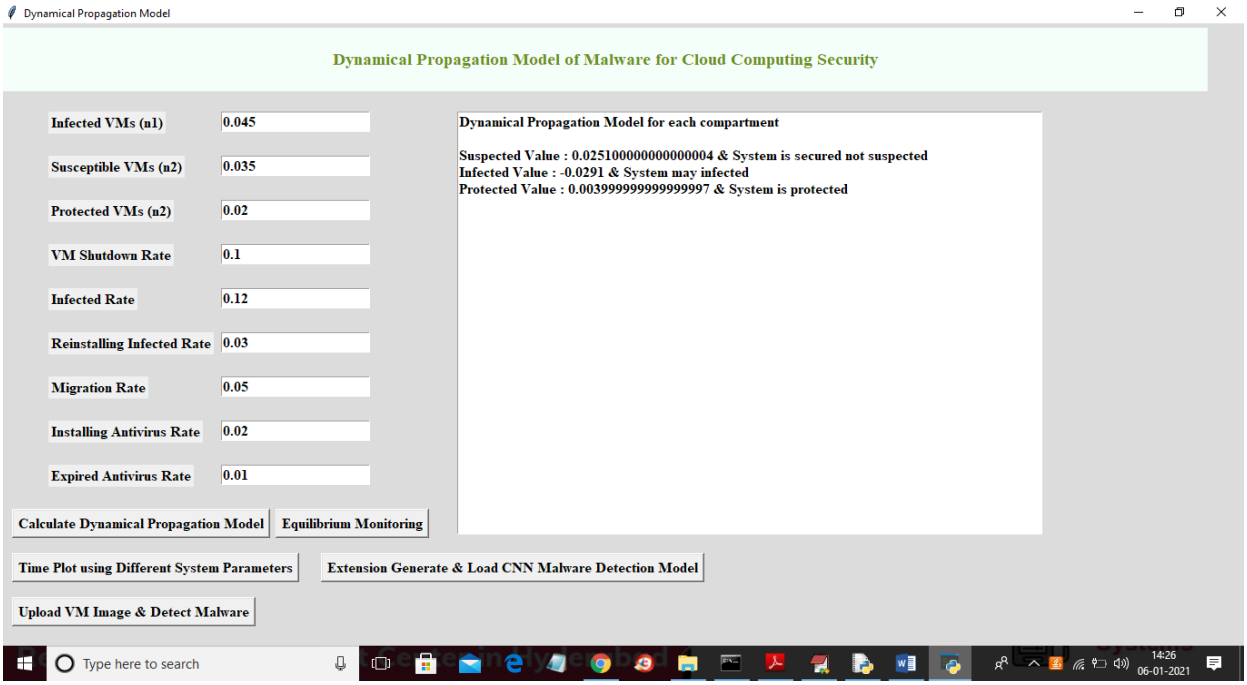
Fig.4.1.1 System architecture

V. RESULTS

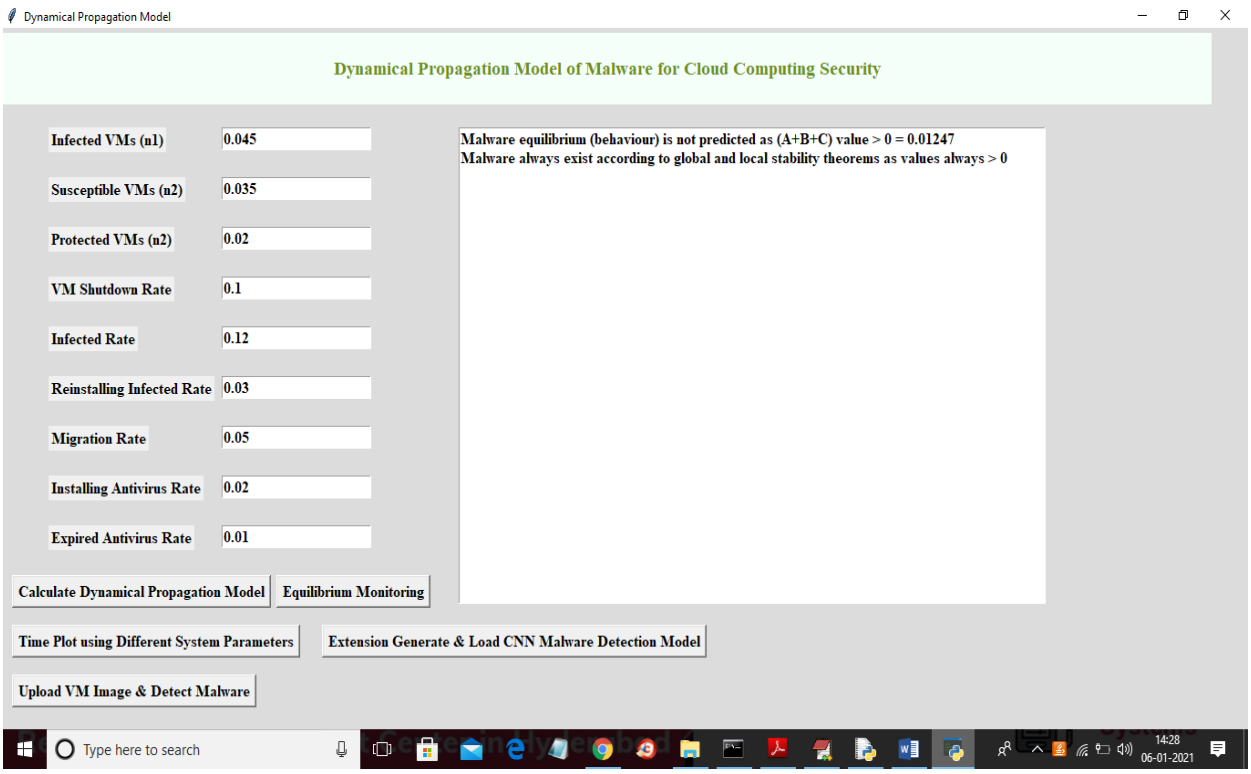
To run project double click on 'run.bat' file to get below screen



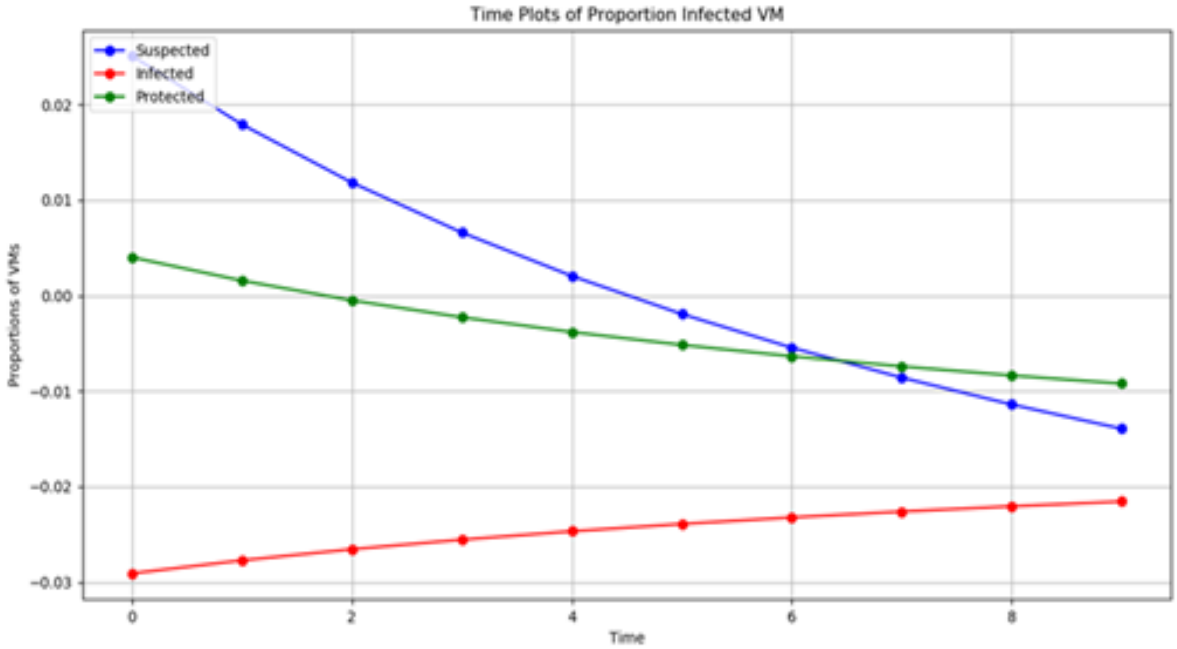
In above screen for experiment we have given SYSTEM PARAMETERS from paper but you change any parameters and then click on 'Calculate Dynamical Propagation Model' button to calculate system SUSPECTED, INFECTED and Protected probability



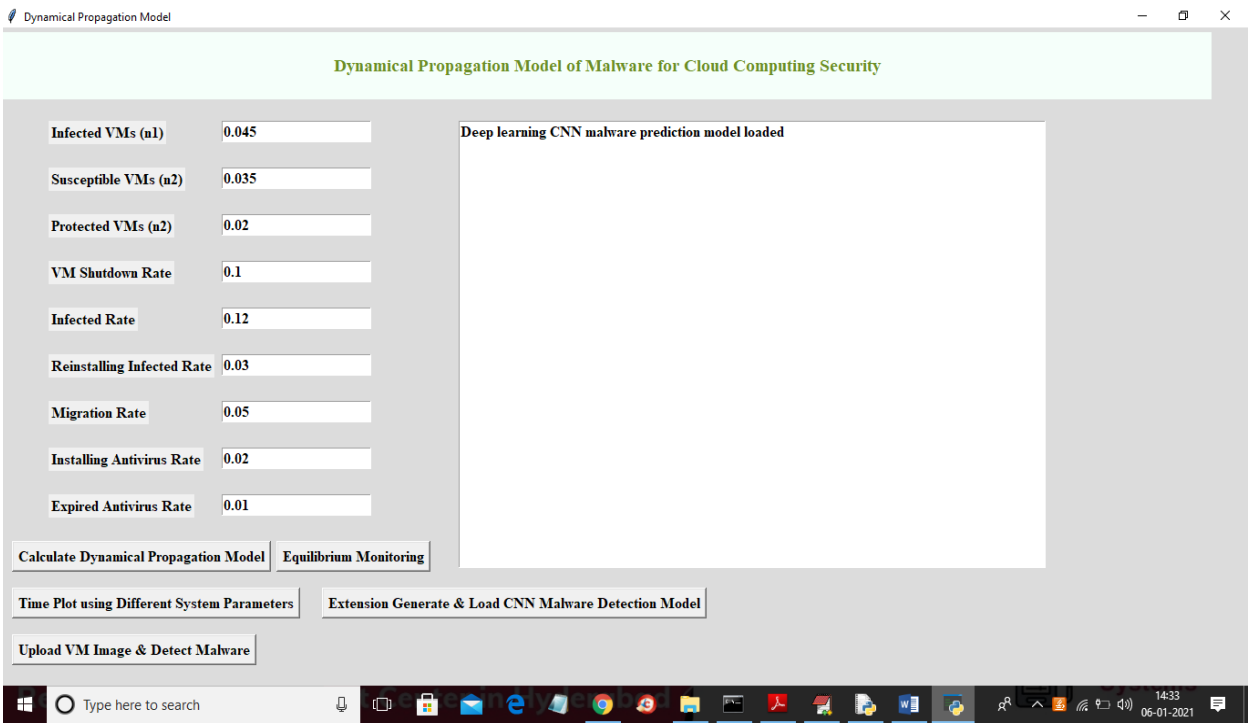
In above screen we calculated Dynamical Propagation model and if value > 0 then system is secure and if value is less than 0 then system may be infected at given time period and now click on 'Equilibrium Monitoring' button to monitoring behaviour of systems under given parameters and if calculated value > 0 then system behaviour is normal else malware detected.



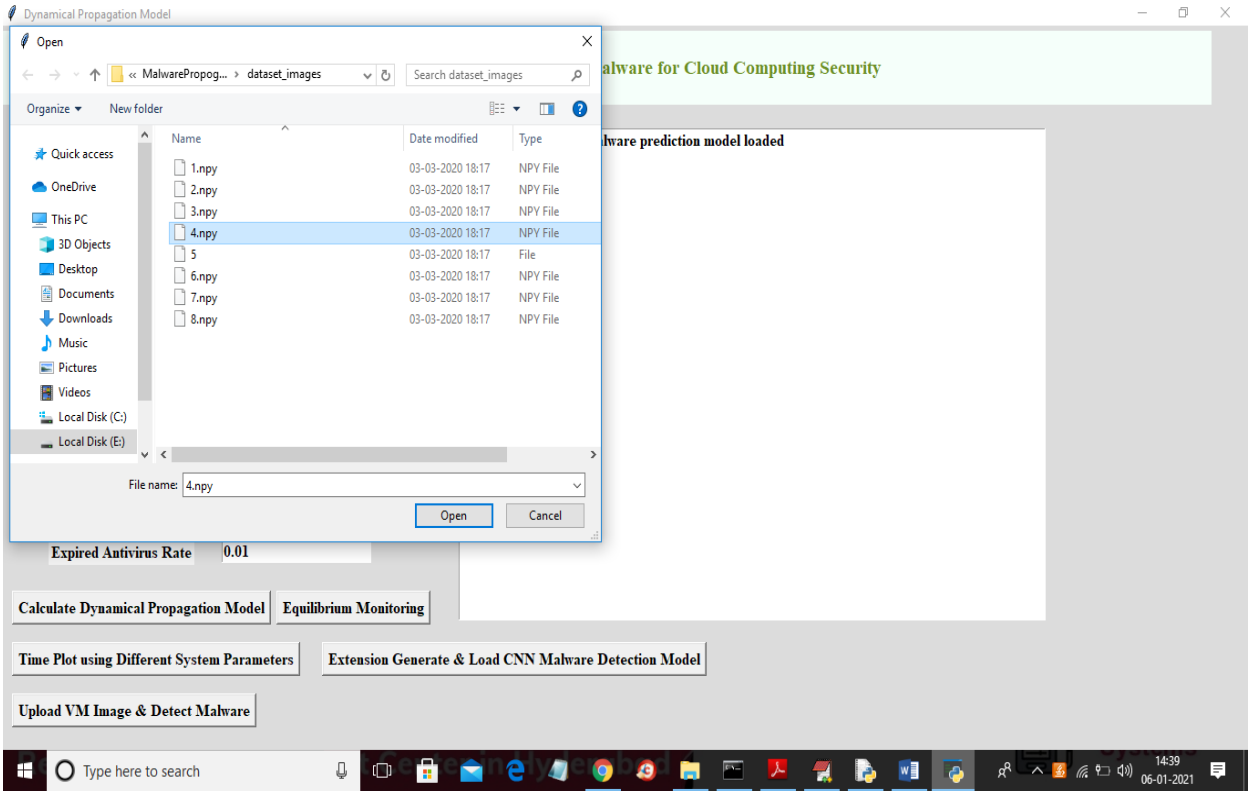
In above screen equilibrium value calculated using constant A,B and C values and if value > 0 then malware is not predicted and may be infected or suspected at different time period and now click on 'Time Plot using Different System Parameters' button to get probability of system suspected, infected and protected probability in graph format.



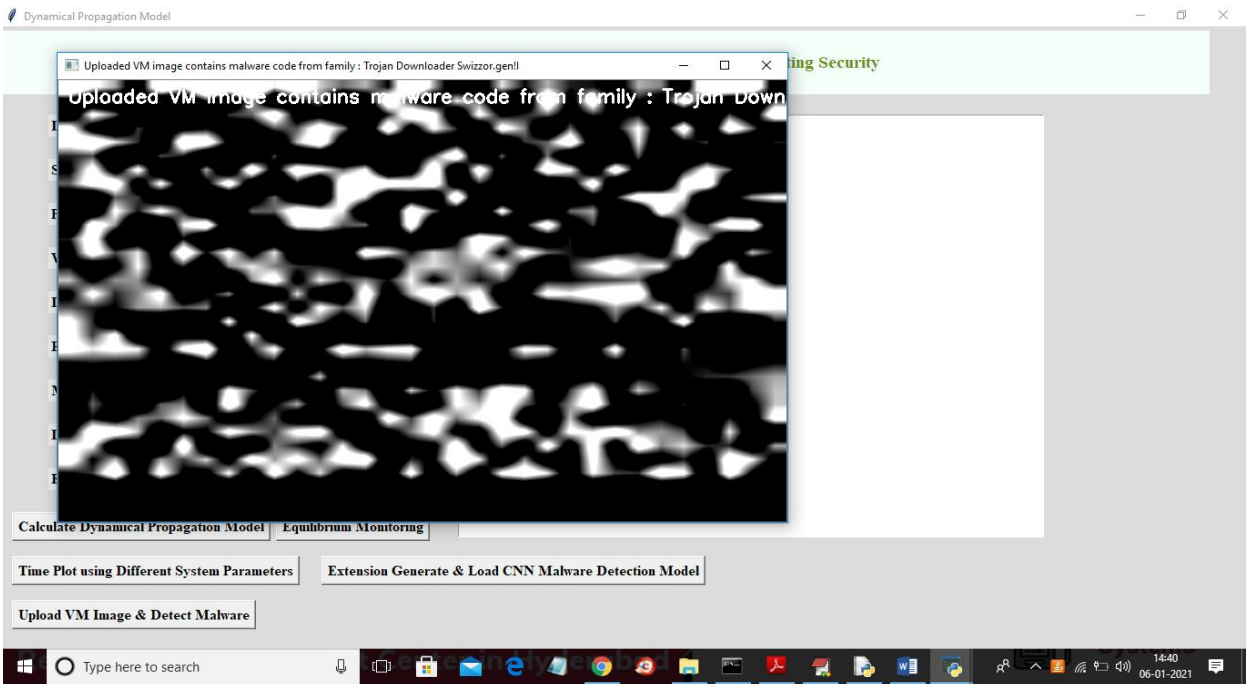
In above graph blue line is for suspected and green for protected and red for infected and x-axis represents different time and y-axis is the VM's probability of malware and from above graph by calculating rules then chances of system getting infected is less compare to protected and suspected. Now click on 'Extension Generate & Load CNN Malware Detection Model' button to generate deep learning malware prediction model



In above screen deep learning model is generated and now click on 'Upload VM Image & Detect Malware' button to upload image and then predict malware family name by applying CNN deep learning model. This image will contains VM internal execution instruction in the form of binary data and if this binary data contains any abnormal or malware instructions then it will be predicted as malware



In above screen selecting and uploading 4.npy file and then click on 'Open' button to get below CNN prediction result



In above screen displaying image of uploaded VM and then displaying VM contains which malware family as the image title. In above image malware name detected as 'Trojan Downloader Swizzor.gen' and similarly u can upload and predict malware from other files

VI. CONCLUSION

This paper presents a dynamic propagation model for malware within the context of cloud computing security. To gain a deeper insight into the spread of malware in an infected cloud setting, a thorough examination of the equilibrium and stability of the proposed model has been performed. The analysis reveals that once malware infiltrates a virtual network, it remains persistent, and complete eradication is unattainable through any method. Nevertheless, by fine-tuning system parameters, the percentage of infected virtual machines (VMs) can be minimized to a manageable level. The paper also includes numerical simulations to demonstrate the primary findings. While our research has yielded some insights into malware propagation in compromised cloud environments, we believe significant further work is necessary. Firstly, our findings indicate that the ultimate infection level is influenced by system parameters, yet there is insufficient exploration into control strategies, which hampers practical application. Thus, it is vital to invstigate targeted control approaches. Furthermore, employing deep learning techniques to analyze malware propagation in the cloud could prove beneficial.

VII. REFERENCES

[1] https://ieeexplore.ieee.org/abstract/document/8114554 (2017)
[2] https://ieeexplore.ieee.org/abstract/document/8291109 [2018]
[3] https://ieeexplore.ieee.org/abstract/document/8291109 [2018]
[4] https://ieeexplore.ieee.org/abstract/document/7389828 [2016]
[5] https://ieeexplore.ieee.org/abstract/document/8610430 [2019]
[6] X. Wang, L. T. Yang, X. Xie, J. Jin, and M. J. Deen, "A Cloud-Edge Computing Framework for Cyber-Physical-Social Services," IEEE Commun. Mag., vol. 55, no. 11, pp. 80-85, Nov. 2017.
[7] C. Zhu, J. P. C. Rodrigues, V. C. M. Leung, L. Shu, and L. T. Yang, "Trust-Based Communication for the Industrial Internet of Things," IEEE Commun. Mag., vol. 56, no. 2, pp. 16-22, Feb. 2018.
[8] X. Wang, L. T. Yang, H. Li, M. Lin, J. Han, and B. O. Apduhan, "NQA: A Nested Anti-Collision Algorithm for RFID Systems," ACM Trans.

Embed. Comput. Syst., vol. 18, no. 4, Article No.: 32, Jul. 2019.

[9] L. Kuang, L. T. Yang, X. Wang, P. Wang, Y. Zhao, "A Tensor-based Big Data Model for QoS Improvement in Software Defined Networks," IEEE Network, vol. 30, no. 1, pp. 30-35, Jan. 2016.

[10] X. Wang, L. T. Yang, L. Kuang, X. Liu, Q. Zhang and M. J. Deen, "A Tensor-based Big Data-Driven Routing Recommendation Approach for Heterogeneous Networks," IEEE Network Magazine, vol. 33, no. 1, pp.64- 69, Jan. 2019.

[11] C. Dong, H. Wang, Y. Li, W. Wang, and Z. Zhang, "Route Control Strategies for Autonomous Vehicles Exiting to Off-Ramps," IEEE Trans. Intell. Transp. Syst., pp. 1–13, 2019.

[12] D. H. Ni, "Determining traffic-flow characteristics by definition for application in ITS," IEEE Trans. Intell. Transp. Syst., vol. 8, no. 2, pp. 181–187, Jun. 2007.

[13] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles," IEEE Trans. Intell. Transp. Syst., vol. 16, no. 2, pp. 546– 556, Apr. 2015.

[14] C. Y. Dong, H. Wang, Q. Chen, D. H. Ni, and Y. Li, "SimulationBased Assessment of Multilane Separate Freeways at Toll Station Area: A Case Study from Huludao Toll Station on Shenshan Freeway," Sustainability, vol. 11, no. 11, Jun. 1 2019.

[15] C. Wang, C. C. Xu, J. X. Xia, Z. D. Qian, and L. J. Lu, "A combined use of microscopic traffic simulation and extreme value methods for traffic safety evaluation," Transp. Res. Part C Emerg. Technol., vol. 90, pp. 281–291, May 2018.

[16] Y. Li, H. Wang, W. Wang, L. Xing, S. W. Liu, and X. Y. Wei, "Evaluation of the impacts of cooperative adaptive cruise control on reducing rear-end collision risks on freeways," Accid. Anal. Prev., vol. 98, pp. 87–95, Jan. 2017.

[17] D. H. Ni, J. D. Leonard, C. Q. Jia, and J. Q. Wang, "Vehicle Longitudinal Control and Traffic Stream Modeling," Transp. Sci., vol. 50, no. 3, pp. 1016–1031, Aug. 2016.

[18] F. Chen and S. Chen, "Injury severities of truck drivers in single- and multi-vehicle accidents on rural highways," Accid. Anal. Prev., vol. 43, no. 5, pp. 1677–1688, Sep. 2011.

[19] Y. Li, Z. B. Li, H. Wang, W. Wang, and L. Xing, "Evaluating the safety impact of adaptive cruise control in traffic oscillations on freeways," Accid. Anal. Prev., vol. 104, pp. 137–145, Jul. 2017.