

A Strategic Anti-Virus Model for Preventing Virus Attacks in a System using a Heuristic Checkpoint Approach in mitigating Cyberthreats

Ibeneme-Sabinus I. L.¹, Ezeh I. H.², Ewunonu T. C.³, Okoloegbo C. A.⁴, Amaka E. N.⁵, Nworuh G. E.⁶, Okon I. A.⁷, and Ugbor I. C.⁸
^{1,2,3,4,5,6,7,8}Department of Cybersecurity, Federal University of Technology Owerri, Nigeria.

Date of Submission: 04-02-2026

Date of Acceptance: 15-02-2026

Abstract: Attacks involving viruses have grown over the years as cybercriminals work harder to mislead victims into downloading infected files, email messages, advertisements, devices and apps in order to steal sensitive organization's Information as same is now on the increase. This has called for an urgent attention of researcher and different bodies alike to develop mobile techniques and tools to fight against these deadly occurrences and bring to an end these ugly activities of virus threats. This study examines several techniques and methods while suggesting a combination of Checkpoint Monitors (M1, M2, and M3) technique to mitigate the activities of viruses as known cyber threats in our business organizations today.

Key Words: Virus threats, Checkpoint, Heuristic approach, Monitors.

I. Introduction

Virus is a type of malware threat which has been in operation for ages causing damages to organization's systems, disrupting businesses and rendering transactions hopeless. As one of cybersecurity threats usually causing tremendous negative effects on any device it comes in contact with and its presence can be noticed through its

common mode of operations such as organization's computer system running slower than usual, unwanted and unusual pop-up menu including advertisements, computer programs unexpectedly closing down by themselves, customer's accounts being logged out when specific applications are affected, crashing of systems, fraudulent emails, websites, or social media messages which are used to luring individuals into downloading and installing viruses into devices.[2].

Its operations pose a significant threat as they are designed to disrupt computer systems and propagate through networks or Internet connections [3]. Detecting its spread effectively has become increasingly difficult because of the complexity of modern viruses and the volume of data being generated [6].

The presence of most cybersecurity threats paves ways for viruses, endangering user security, privacy, and their financial security [1]. Traditional antivirus systems have relied on signature-based detection methods for a long time [5]. But the spread of virus is increasing by the day as many computer systems run very slow and equally shut down at ease, business not moving smoothly as it used to in the previous days. Hence, this clarion call for effective and efficient model to mitigate their ugly operations.

Viruses work in different phases and one of such phases of occurrence is shown in figure 1 below.

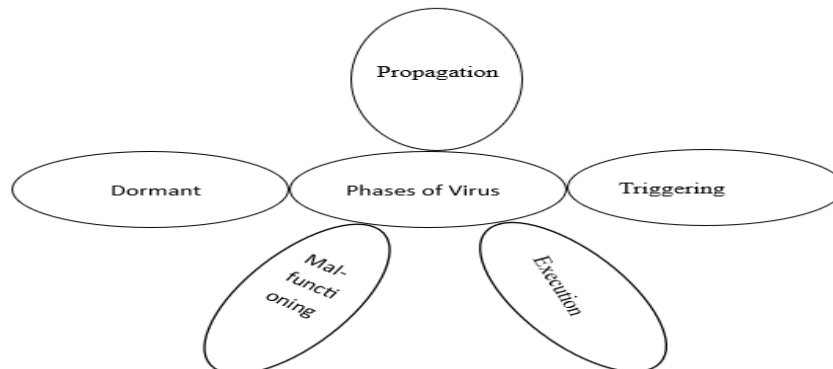


Figure 1: Different occurrence phase of a virus threats.

They work in the following four distinct phases:

- Dormant Phase: In this phase virus sneaks into the system, it hides itself without immediate exploit. this behavior doesn't call for prompt initial detection.
- Propagation Phase: The virus in this stage began to move and spread itself into files, folders, and programs across the system and can comfortably move into other systems through external devices and shared files.
- Triggering Phase: This phase is usually activated when user click on already downloaded files from visited sites, click on applications and programs the actions activate the virus.
- Execution Phase: Immediately after the triggering phase elapses, the virus starts

running its malicious code in the system and this is where the damages begin. Systems start slowing down and disrupting day-to-day activities, data being compromised and sensitive information stolen.

This is when most organizations start seeking the services of a cyber security experts to eradicate the occurrence and possibly opting for a more secured and reliable security measures to mitigate the activities of cyber threats within the organization. The security of data and information over the internet is one of the top challenges facing most businesses today [4]. This research paper is proposing a Heuristic Checkpoint model for its water-tight mitigation and the proposed model architecture is shown in figure 2 below.

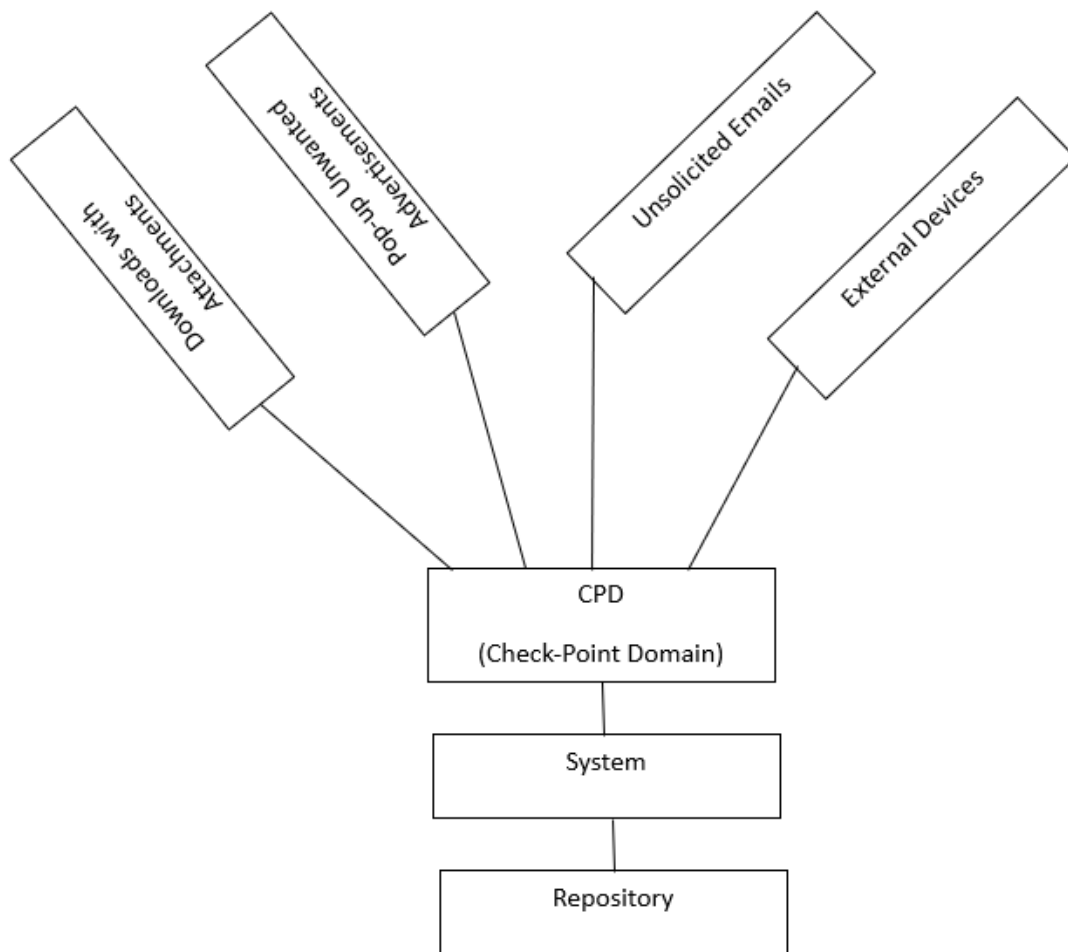


Figure 2: Proposed Model Architecture

In this proposed model, all activities and entrance routes into organization system is scrutinized using some self-generated tools, these checkpoints consist of the combinations of three (3)

monitors. These monitors operate using 3D operational technique that mimics the Malwarebytes, Kaspersky and Bit defenders' technologies in eliminating viruses in organization's system. The

first Monitor {M1} scans for virus codes, downloaded files with attachments, Pop-up advertisements, unsolicited emails and inserted external devices as request are made into the system, M2 monitors and removes suspected virus behaviour from source (its hiding place which could be files) to its destination as it moves round the entire network

environment and M3 uses destination stack to remove virus at its endpoint which may occur as a result of interruption from network or other services as the repository stores and manages different types of data and all activities conducted on the organization system while also focusing on collaboration and version control scheme.



Figure 3; A simulated Environment showing how the Monitors (M1, M2, M3) navigates.

A simulated environment (fig 3) that demonstrated how the different monitors move and navigate through the organization's system in search of suspected virus behaviour which might have resulted through user's activities. These operations suggested that by the combination of these techniques' virus can be totally eradicated from source to destination within the organization's structure.

II. Conclusion

In an effort to provide an everlasting solution in mitigating the occurrence of viruses, a thorough review was made by understanding the rapid development of the subject matter. We x-rayed the performance of the techniques and analyze their capacities appropriately. The result of the simulation showed that these combinations worked perfectly as virus enters into a system through downloads, emails, advertisements and injecting malicious codes into the system. The monitors navigate through the system from the source where the virus is hidden as a result of the activities of the users to destination where the virus plans to execute and explodes.

References

[1]. Sharma, M., Kaul, A., & Kumar Gondhi, N. (2025). An enhanced hybrid architecture for detecting malware in android apps using machine learning and deep learning

techniques. *Academy of Marketing Studies Journal*, 29(3), 1-21.

[2]. Gulshan and Neetu Sharma (2025). Malware Analysis and Detection using ML tools: Current State and Challenges. *International Journal of Engineering Trends and Technology* Volume 73 Issue 1, 371-384, January 2025 ISSN: 2231-5381 /<https://doi.org/10.14445/22315381/IJETT-V73I1P132> © 2025 Seventh Sense Research Group®.

[3]. Unnimaya M U (2025). A Comprehensive Review on Malware Detection Techniques. *International Journal on Science and Technology (IJSAT)* E-ISSN: 2229-7677. Volume 16, Issue 1, January-March 2025.

[4]. Ibeneme-Sabinus I.L, Agbakwuru O.A and Elebiri L.E (2025) Multiagent antimalware model,a paradigm shifts from mere detection to prevention of cyber threats.*Iconic Research Engineering Journals*. Vol.9, issue 5. IRE 1712391.

[5]. Gautam Karat, Jinesh M. Kannimoola, Namrata Nair, Anu Vazhayil, Sujadevi V G and Prabakaran Poornachandran (2024). CNN-LSTM Hybrid Model for Enhanced Malware Analysis and Detection.5th International Conference on Innovative Data Communication Technologies and

- Application (ICIDCA 2024), Procedia Computer Science 233 (2024) 492–503.
- [6]. Hussain A, Abdulrahman A, and Mounir F (2025) Imbalance Datasets in Malware Detection: A Review of Current Solutions and Future Directions. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 16, No. 1, 2025.