IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025

MidBrain Antivirus

Mr. Aditya Jamage, Mr. Krushna Manore, Mr. Kulkarni Omkar,
Mr. Patil Piyush, Mr. R. A. Kautkar
Guru Gobind Singh Polytechnic, Nashik, India

Abstract: *The "MidBrain" antivirus project focuses on developing an intermediate-level antivirus software that offers essential protection against malware and system threats. The project utilizes techniques such as hash-based malware detection, folder and deep scanning to identify and eliminate malicious software. Additionally, it incorporates real-time protection to safeguard the system by continuously monitoring and blocking threats in real time. System optimization features like a RAM booster and junk file remover are included to enhance overall performance. The project is designed with upgradability in mind, allowing for future enhancements in malware detection algorithms and database updates. Built using Python and Tkinter, or PyQt for the graphical user interface (GUI), the "MidBrain" antivirus provides a user-friendly, efficient, and adaptable solution for everyday system protection.*

Keywords: MidBrain

I. INTRODUCTION

In the contemporary digital environment, when malware attacks become very widespread, the role of antivirus software is highly important in computer security. However, designing an integrated antivirus package is quite complex and calls for profound knowledge regarding malware behavior and techniques of its detection. The paper presents "MidBrain," a simple antivirus project designed and developed by students as part of their diploma courses. Our MidBrain Antivirus comes with some key features, including hash comparison for malware detection, scan of a directory, and real-time protection. For the above project, the language used in programming is Python.

The plan for MidBrain is not to be one of the industry players in the league of Quick Heal, McAfee, or AVG but rather to be a training tool to teach students the basics of what needs to be done in an AV implementation. It's practical, and it keeps things grounded in reality; the most basic antivirus will not work on all advanced features or even some of the complicated malware scenarios.

Instead, it's an experiential learning experience in the form of a project not complete in all the senses of the word, with detailed learning pathways both via online resources as well as academic researches. As we keep growing, it will add new features assigned based on learning, but for now, it is purely about how the antivirus works.

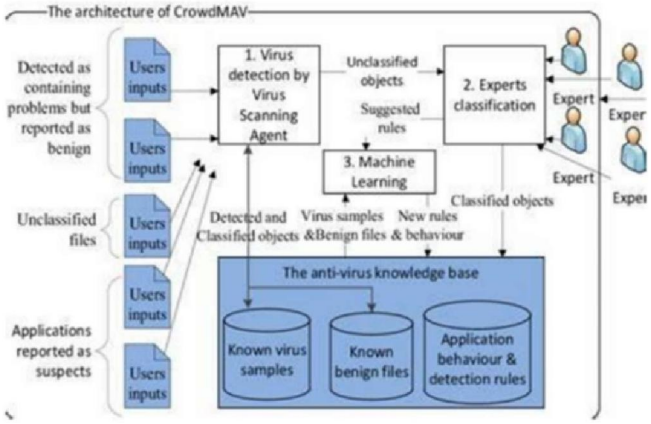
II. LITERATURE SURVEY

The literature highlights various approaches to antivirus and malware detection. Signature-based methods [1] are efficient for known threats but fail against novel malware. Heuristic-based techniques [2] detect unknown threats through patterns but suffer from high false-positive rates. Behavior-based detection [3] analyzes runtime behaviors for sophisticated threats but is computationally intensive. Cloud-based detection systems [4] offer scalability and real-time updates but depend on network reliability. Recent advancements leverage machine learning [5] for adaptive and intelligent detection, enhancing accuracy while addressing evolving cybersecurity challenges.

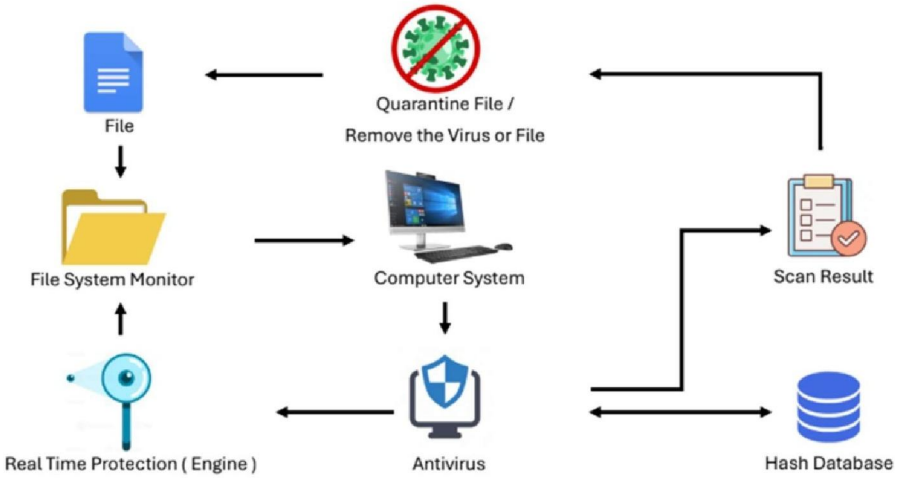
III. EXISTING SYSTEM

This diagram represents the architecture of an existing system, CrowdMAV. It starts with user inputs, where files and applications are submitted for evaluation. The system uses a virus scanning agent for initial detection, classifying objects as unclassified, benign, or problematic. Experts further classify unclassified objects and suggest rules. Machine learning algorithms refine the process by updating the antivirus knowledge base with known virus samples, benign files, and behavior detection rules, creating a feedback loop for improving detection accuracy.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025



Proposed System



This diagram illustrates the proposed antivirus system. It begins with monitoring files through a file system monitor and providing real-time protection via a scanning engine. Files are scanned and checked against a hash database, with results displayed for the user. If a threat is detected, the infected file is either quarantined or removed, ensuring system safety and maintaining optimal performance.

Problem Statement

Nowadays, there are many risks in the digital world, like viruses and malware, that can harm our computers and steal our data. These problems can cause big issues like losing important files or slowing down our systems. To help solve this, our antivirus software (MidBrain) will protect your computer from these threats.

IV. RESEARCH METHODOLOGY

The research methodology for the MidBrain Antivirus project focuses on building a basic antivirus system with key features including real-time protection, file scanning, full system scanning, junk file removal, RAM boosting, and virus removal. The system uses signature-based detection to identify known viruses and malware. Real-time protection continuously monitors files and system activity for potential threats. Users can manually initiate file scans and full system scans to detect viruses. The junk file remover clears unnecessary files, while the RAM booster optimizes system performance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.67
Volume 5, Issue 4, March 2025

V. RESULT

Our midbrain antivirus provides essential features like real-time protection, ensuring continuous safety against threats, and thorough file and system scanning to detect and eliminate viruses. It includes a junk file remover to optimize storage, a RAM booster for enhanced device performance, and a reliable virus removal tool. These core features make it a practical and effective solution for maintaining system health and security.

VI. FUTURE SCOPE

The future scope of our midbrain antivirus includes regular updates to tackle evolving threats, enhanced with an intuitive and visually appealing GUI. We plan to integrate advanced AI for real- time learning and self-improvement from past mistakes, ensuring smarter threat mitigation. The antivirus will expand to work seamlessly on multiple platforms, including mobile devices, car systems, and IoT setups. With cross-device compatibility and cutting-edge technology, it will adapt to users' dynamic needs while offering maximum security and convenience.

REFERENCES

[1] M. Al-Asli and T. A. Ghaleb, “Review of Signature-based Techniques in Antivirus Products,” in *Proceedings of the 201S International Conference on Computer and Information Sciences (ICCIS)*, 2019, pp. 1–6. doi: 10.1109/ICCISci.2019.8716381.
[2] S. Banik, S. S. M. Dandyala, and S. V. Nadimpalli, “Heuristic-based Detection Techniques,” *International Journal of Advanced Engineering Technologies and Innovations*, vol. 1, no. 2, pp. 352, 2022.
[3] X. Wang, Y.-C. Jhi, S. Zhu, and P. Liu, “Behavior Based Software Theft Detection,” in *Proceedings of the 1Cth ACM Conference on Computer and Communications Security (CCS ’0S)*, 2009. doi: 10.1145/1653662.1653696.
[4] Ö. Aslan, M. Ozkan-Okay, and D. Gupta, “A Review of Cloud-Based Malware Detection System: Opportunities, Advances and Challenges,” EJERS, European Journal of Engineering and Technology Research, vol. 6, no. 3, pp. 1–8, Mar. 2021.
[5] A. Halimaa and K. Sundarakantham, “Machine Learning Based Intrusion Detection System,” in *Proceedings of the 201S 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, Tirunelveli, India, 2019, pp. 916-920, doi: 10.1109/ICOEI.2019.8862784.
[6] C. Sadowski and G. Levin, “SimHash: Hash-based Similarity Detection,” University of California, Santa Cruz, Dec. 13, 2007. [Online]. Available: https://www.webrankinfo.com/dossiers/wp-content/uploads/simhash.pdf.
[7] L. Radvilavicius, L. Marozas, and A. Cenys, “Overview of Real-Time Antivirus Scanning Engines,” *Journal of Engineering Science and Technology Review*, vol. 5, no. 1, pp. 63-71, Mar. 2012.
[8] H. Asamoah, “Antivirus Software Versus Malware,” Bachelor’s thesis, Vasyl’ Stus Donetsk National University, Information Technologies Department, Vinnytsia, Ukraine, 2021.
[9] M. A. H. Saeed, “Malware in Computer Systems: Problems and Solutions,” IJID (International Journal on Informatics for Development), vol. 9, no. 1, pp. 1-8, Jun. 2020, doi: 10.14421/ijid.2020.09101.
[10] O. K. Akinde, A. O. Ilori, A. O. Afolayan, and O. B. Adewuyi, “Review of Computer Malware: Detection and Preventive Strategies,” International Journal of Computer Science and Information Security (IJCSIS), vol. 19, no. 11, pp. –, Nov. 2021. [Online]. Available: https://doi.org/10.5281/zenodo.5847957.