Cyber Gaurdian

Soham Murkar[1], Ayana Xavier[2], Aarohi Taleler[3], Akanksha Sing[4], Nilambari Narkar[5]
[1,2,3,4,5] *Xavier Institute of Engineering, Mahim*

Abstract—**In today's digital world, the rapid growth of online communication and data exchange has increased the chances of cyber threats through file sharing. Existing systems often lack efficient real-time detection and rely heavily on manual checks, making users vulnerable to malware, ransomware, and other harmful content. These threats can compromise data integrity, privacy, and overall system security, highlighting the urgent need for automated and reliable protection mechanisms. To address these challenges, we have proposed Cyber Guardian which introduces a secure platform that automatically scans uploaded files to detect and report potential risks. The system integrates file validation, malware detection algorithms, and an instant notification feature to alert users about harmful files. It uses a combination of pattern matching and threat analysis techniques to ensure accurate and fast detection of malicious content before it reaches the user's device. The implementation of Cyber Guardian, aim to enhance user safety and promote secure file handling practices. The project demonstrates how automation and intelligent detection can act as a proactive defense against cyber threats. By simplifying the process of identifying harmful files, and contributes to a safer digital environment. It serves as an efficient first line of defense in modern cybersecurity.**

Index Terms— **Python Core language for threat detection scripts and system monitoring. Tkinter /Electron/Flutter, Watchdog, Os library, Virus Total API, Real-time Notification Library**

I.INTRODUCTION

In the age of rapid digital transformation, the integration of technology into every aspect of personal and professional life has significantly increased the exposure to cybersecurity risks. With internet connectivity becoming a necessity and data being stored, shared, and accessed across multiple platforms, cybercrime is no longer limited to large organizations or government institutions. Ordinary users, small businesses, and students are equally vulnerable to attacks such as malware infections, unauthorized intrusions, ransomware encryption, phishing attempts, and data manipulation. Every device connected to the internet whether a laptop, smartphone, or IoT gadget acts as a potential entry point for malicious actors.

The frequency, sophistication, and automation of cyber threats have increased exponentially over the past decade. According to several global cybersecurity surveys and research reports, thousands of new malware variants are generated daily, and cyberattacks have evolved from simple viruses to highly intelligent and concealed intrusion techniques. Traditional antivirus solutions, although useful, function largely as reactive defense systems detecting and removing threats after the system has already been compromised. By the time the antivirus identifies malicious activity, the damage may have already been done: data theft, corruption, or unauthorized access.

Thus, the modern cybersecurity landscape demands a proactive security mechanism one that constantly analyzes system activity, predicts the possibility of malicious behavior, and takes preventive action before a threat escalates. Users need security tools that are not only intelligent but also interactive and easy to understand, enabling even non-technical individuals to manage threats efficiently. To address this need, our mini project introduces Cyber Guardian, a Smart Intrusion Detection and Response Application. Cyber Guardian is designed as a proactive real time defense system that continuously monitors the device's processes, file activities, and user interactions. Unlike conventional antivirus software that only scans periodically or after a threat occurs, Cyber Guardian actively observes system behavior, identifies suspicious activity, evaluates risk levels, and immediately informs the user if anything unusual is detected. The system highlights the exact file, folder, application, or process responsible for triggering the alert, making threat identification simpler and more transparent.

A distinguishing feature of Cyber Guardian is its interactive guidance system. Instead of only showing a warning message, the application provides step-by-

step instructions to help users take 9 corrective actions, such as isolating the file, deleting it, stopping malicious processes, or blocking unauthorized access. This makes the system suitable for users with minimal technical knowledge, ensuring that cybersecurity awareness becomes accessible to all.

The project incorporates essential principles of cybersecurity, data monitoring, automation, pattern recognition, and user-focused interface design. By constantly analyzing system behavior rather than relying solely on predefined virus signatures, Cyber Guardian increases the chances of identifying unknown or emerging threats that traditional tools may fail to detect. In doing so, the application enhances digital safety, promotes preventive awareness, and reduces dependency on external technical support.

II.LITERATURE SURVEY

A Machine Learning Approach for Malware Detection by S. Singh and R. Gupta, published in IEEE Access (2021). This paper proposed a machine learning-based model for detecting malware using feature extraction and classification algorithms. The authors collected large datasets of benign and malicious files and trained models such as Random Forest and Support Vector Machine (SVM) to identify harmful patterns. The system achieved high accuracy in detecting known malware but required frequent retraining to handle newly emerging threats. Although the model was effective in improving detection rates, it was computationally heavy and not suitable for lightweight or real-time applications.

A key paper by Zhuoran Li & Dan Zhao (2022), titled "ThingNet: A Lightweight Real-time Mirai Variants Hunter through CPU Power Fingerprinting," establishes a novel method for hardware based behavioral detection. Instead of only inspecting software code, their system identifies malware (specifically Mirai variants) on low-power IoT devices by monitoring their CPU power consumption. They discovered that malicious processes create a unique, measurable "fingerprint" in power draw, distinct from normal operations. A compact Convolutional Neural Network (CNN) is then used to recognize this malicious fingerprint in real-time. This study is highly relevant as it proves that proactive behavioral monitoring can be both non-intrusive and extremely efficient, supporting Cyber Guardian's core goal of observing system behavior to catch new, unknown threats.

Addressing the need for efficient static file analysis (checking a file before it runs), the "MALITE" system by Sidharth Anand et al. (2023) provides a practical solution for constrained devices. Their technique cleverly converts malware binaries into images, allowing machine learning models to identify them based on their visual textures and patterns, which differ between malware families (e.g., ransomware vs. spyware). These images are then fed into lightweight classifiers, like a Random Forest (MALITE-HRF) or a very small neural network (MALITE-MN). This research provides a direct, low-cost methodology for Cyber Guardian's file upload detection feature, enabling rapid analysis that is far more powerful than simple extension-checking.

Most recently, the work on "Lightweight Behavior-Based Malware Detection" by M. Anisetti et al. (2024) provides a framework for real-time dynamic analysis (monitoring a program as it runs). To maintain high performance, their system only tracks "cheap-to-compute" behavioral features. These include monitoring process sequences

III.PROPOSED SYSTEM

The proposed system, Cyber Guardian, is an intelligent intrusion detection and response application designed to proactively safeguard a user's system from cyber threats. Unlike traditional antivirus software which primarily depends on predefined virus signatures Cyber Guardian focuses on behavior-based analysis. It continuously monitors system activities, file behavior, user interactions, and running processes to identify abnormal or suspicious patterns that may indicate malware execution, unauthorized file manipulation, or intrusion attempts.

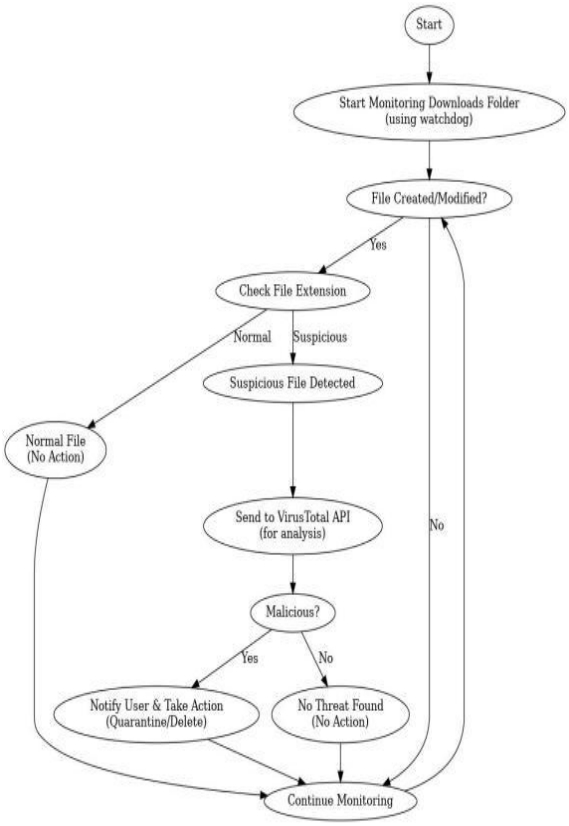
The system performs real-time scanning and monitoring, enabling it to detect threats the moment they begin to exhibit harmful behavior, rather than after the system is already compromised. For every event or activity detected, Cyber Guardian evaluates parameters such as file origin, execution behavior, access patterns, and system resource usage. This enables the system to identify sophisticated malware, zero-day threats, and ransomware that may be hidden inside legitimate files or disguised as normal processes.

Once a suspicious activity is detected, Cyber Guardian immediately notifies the user through an alert popup or dashboard notification. The alert includes essential information such as the threat type, severity level, affected file path, and associated process

Once a suspicious activity is detected, Cyber Guardian immediately notifies the user through an alert popup or dashboard notification. The alert includes essential information such as the threat type, severity level, affected file path, and associated process. What differentiates Cyber Guardian from existing security tools is its ability not only to detect threats but also to guide users in resolving them. Instead of technical logs or ambiguous warnings, the system provides step-by-step actionable guidance, enabling user even those without cybersecurity knowledge to remove or neutralize the threat safely and efficiently.

Cyber Guardian further enhances user experience with a clean and intuitive interface, providing a centralized dashboard where users can view alerts, analyze activities, and perform threat.

The system emphasizes ease of use without compromising on technical accuracy, everyday users.

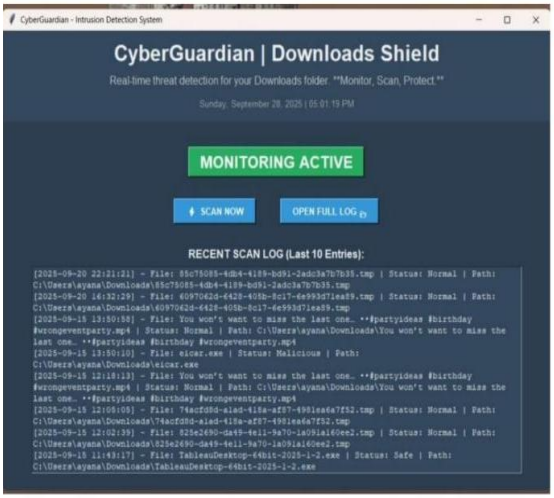


IV.DETAILS OF HARDWARE&SOFTWARE

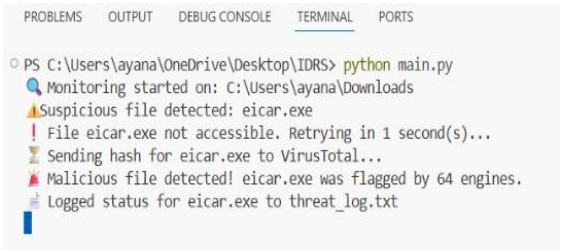
Processor**:** Intel i5 or higher
RAM**:** 8 GB (Minimum), 16 GB (Recommended)
Storage**:** 500 GB HDD or 256 GB SSD
Graphics**:** Integrated graphics (or dedicated if using visualization tools)
Peripherals**:** Keyboard, Mouse, Monitor
Software Requirements
Python Core language for threat detection scripts and system monitoring.
Tkinter/Electron/Flutter Will be Used to create the app's graphical user interface (GUI).
Watchdog Monitoring downloads folder.
Os library Stores threat logs and user activity securely for review.
Virus Total API Checks the files and detects intrusions.
Real-time Notification Library Sends instant alerts to the user when threats are detected.

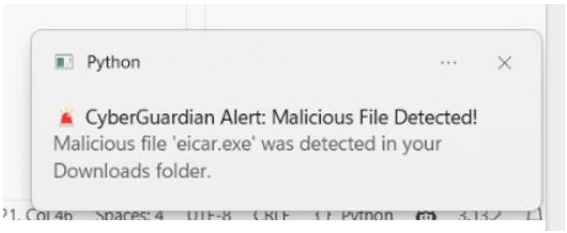
V.EXPERIMENT & RESULTS

Interface of the project



Real-time Malicious File Notification





VI.CONCLUSION

The Cyber Guardian project successfully demonstrates the design and implementation of an effective, real-time threat detection and response system. By focusing on proactive monitoring of file system entry points, this project directly addresses the critical security gap left by traditional, reactive antivirus software. The system's ability to continuously monitor system activity, intercept new files, and leverage a powerful cloud-based API (Virus Total) for analysis ensures that threats are identified before they can be executed.

The project's success is validated by its two primary Effective Detection: The integration of the Virus Total API, which aggregates over 70 scan provides a highly accurate, consensus-based verdict on potential threats, as proven by the successful, instantaneous detection of the EICAR test User-Centric Response: The automated, real-time alert system provides clear, non-technical notifications, transforming security from a passive background process into an interactive, user empowering experience. The GUI and scan logs further enhance this by providing transparency and a persistent record of all system activity.

In its current form, Cyber Guardian provides an effective and user-friendly solution that enhances cybersecurity for end-users. It highlights the importance of proactive security measures and showcases how modern, API-driven security principles can be integrated into accessible software for both novice and experienced users.

VII.FUTURE WORKS

While the current system provides a robust framework for file-based threat detection, its architecture is designed for significant expansion. The following directions are proposed for future enhancements: Machine Learning Integration: The next logical step is to implement local, on-device AI/ML algorithms. This would allow the system to perform predictive threat analysis based on file characteristics, moving beyond simple signature matching to detect "zero-day" threats that have not yet been seen by any antivirus engine.26 Automated Response Mechanisms: To increase protection speed, an "auto-pilot" mode would be introduced. This would allow the system to automatically quarantine or neutralize high-confidence threats without user intervention. This would be a user-configurable setting, allowing novices to opt for full automation while advanced users retain manual control.

Cross-Platform Support**:** The current prototype is built for a single operating system. Future work would involve re-engineering the application to be cross-platform, extending its protection to macOS and Linux environments, and eventually creating lightweight companion apps for mobile platforms (iOS and Android).

Cloud-Based Threat Intelligence: Beyond the Virus Total API, the system could be integrated with additional cloud-based threat intelligence feeds (CTI). This would allow it to receive real-time updates on new malicious IP addresses, domain names, and attack patterns, enabling it to proactively block threats at the network level.

Advanced Reporting & Visualization: The current log file would be expanded into a full, interactive dashboard. This would provide detailed, visual reports and heat maps, helping users understand their system's vulnerabilities, see historical threat trends, and identify the most common types of attacks they are facing

ACKNOWLEDGMENT

We, group 2, consisting of Ayana Xavier (57), Aarohi Talele (51), Akanksha Singh (50) and Soham Murkar (61) would like to express our heartfelt gratitude to the Principal, Dr. Lata Ragha, the Head of Department, Prof. Dr. Sushama Khanvilkar, Ms. Nilambari Narkar and the Xavier Institute of Engineering, Mahim for giving us the best guidance possible and make learning a fun experience.

REFERENCES

[1] S. Singh and R. Gupta, "A machine learning approach for malware detection," IEEE Access, vol. 9, pp. 45898-45912, 2021.
[2] Z. Li and D. Zhao, "ThingNet: A lightweight real-time Mirai IoT variants hunter through CPU power fingerprinting," in Proc. IEEE International Conference on Communications (ICC), 2022.
[3] S. Anand et al., "MALITE: Lightweight malware detection and classification for constrained devices," IEEE Transactions on Emerging Topics in Computing, vol. 13, no. 3, pp. 1099–1112, 2023.
[4] M. Anisetti et al., "Lightweight behavior-based malware detection," in Management of Digital
EcoSystems 15th International Conference, MEDES 2023, Revised Selected Papers, Springer, 2024, pp. 237–250.
[5] Python Software Foundation, Python Language Reference, version 3.x. [Online]. Available: https://www.python.org
[6] G. Jovanovic, Watchdog: Python API and shell utilities to monitor file system events, 2023. [Online]. Available: https://github.com/gorjan-jovanovic /watchdog
[7] VirusTotal, VirusTotal Public API v3.0 Documentation, 2024. [Online]. Available: https://developers.virustotal.com/reference/overview
[8] Python Software Foundation, "Tkinter —Python interface to Tcl/Tk," Python 3.x Documentation. [Online]. Available: https://docs.python.org/3/library/ tkinter.html
[9] European Institute for Computer Antivirus Research (EICAR), EICAR Anti-Malware Test File, 2024. [Online]. Available: https://www.eicar.org /download-anti-malware-testfile/