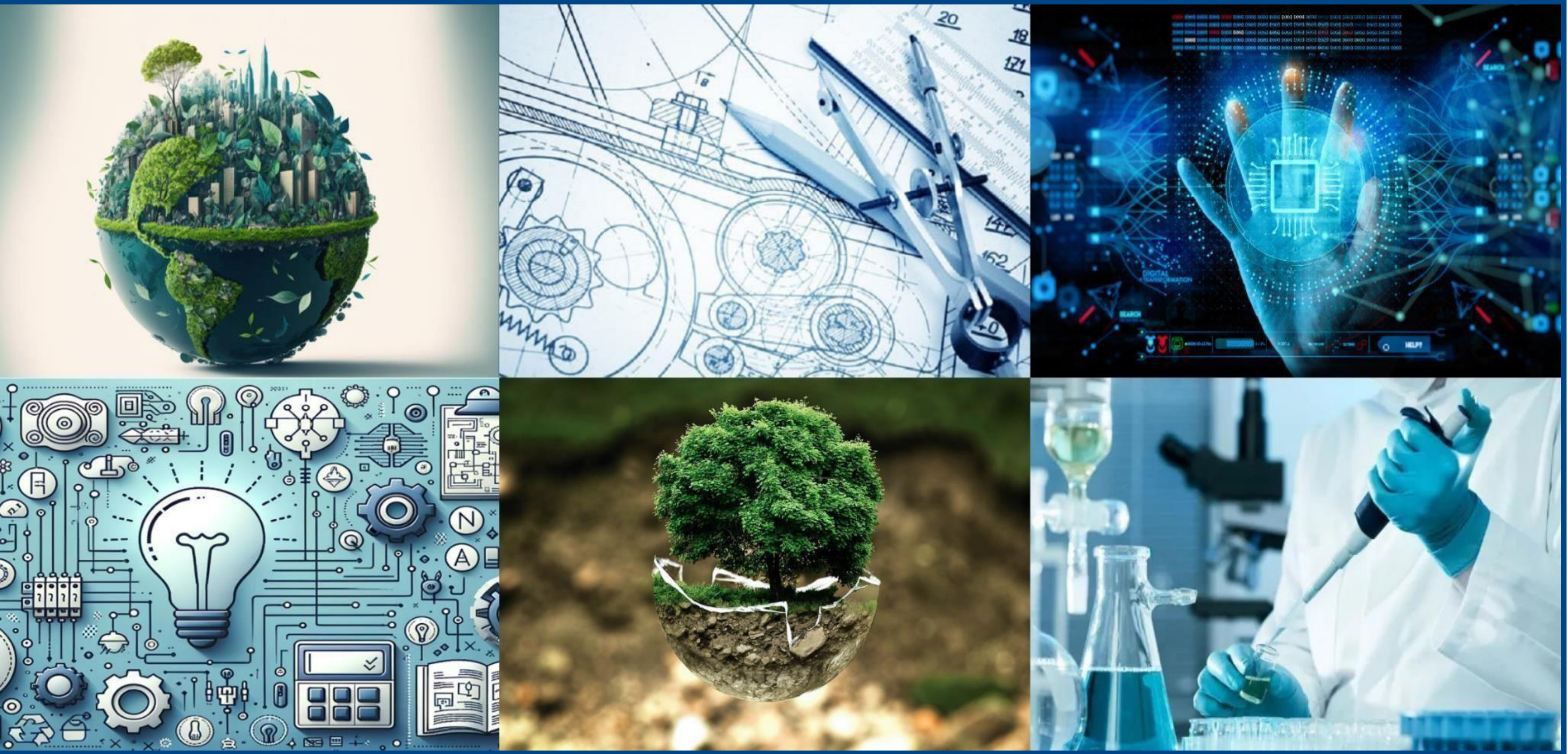
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 8, August 2025

www.ijmrset.com ijmrset@gmail.com +91 6381 907 438 +91 63819 07438

© 2025 IJMRSET | Volume 8, Issue 8, August 2025| DOI:10.15680/IJMRSET.2025.0808071

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

MALSCANX: AN ADVANCED MALWARE DETECTION AND FILE SCANNING TOOL

Gunasekaran K, Harsh Raj Bhardwaj

Assistant Professor, Department of MCA, AMC Engineering College, Bengaluru, India

Student, Department of MCA, AMC Engineering College, Bengaluru, India

ABSTRACT: MALSCANX is an advanced malware detection and file scanning tool designed to identify malicious files on a local system without requiring internet access. It uses a hybrid detection approach—combining signature-based scanningwith heuristic analysis—to evaluate user-selected files and folders for suspicious patterns or behaviors. The system is intended for academic, isolated, or resource-limited environments where commercial antivirus tools may not be available or practical. MALSCANX alsosupports manual updates ofits malware signature databasevia USB, ensuring flexibility and offline functionality. With an easy-to-use interface and focused threat reporting, this tool empowers users to identify and act upon potential malware without depending on heavy or subscription-based security solutions.

I. INTRODUCTION

In today's digital landscape, malware threats continue to evolve and target users through various vectors, especially local file systems. Many individuals, institutions, and academic labs rely on shared or standalone systems where full-scale antivirus software is not available due to cost, connectivity, or hardware limitations. These systems remain vulnerable to executable-based malware, script-based payloads, and file tampering attacks

.

MALSCANX addresses this problem by offering a reliable, offline file scanning solution that detects malware using both signature matching and heuristic analysis. The tool is designed for simplicity, speed, and portability, making it ideal for offline systems or air-gapped environments. It allows users to select specific files or folders for scanning and provides detailed threat reports, including risk levels and actions such as quarantine or delete.

II. LITERATURE SYRVEY

Malware detection techniques have evolved significantly over the years, particularly in the areas of signature matching, heuristic analysis, and hybrid detection systems. Traditional antivirus tools rely heavily on signature-based methods, which involve matching file hashes against a database of known malware. Smith et al. (2015) demonstrated that while this method is fast and accurate for known threats, it fails to detect new or modified malware variants.

To overcome this limitation, heuristic- based detection techniques were introduced. Johnson and Brown (2017) presented rule-based systems that inspect file behavior and structure to flag suspicious activity, improving zero-day detection but increasing false positives. Later, Wang et al. (2019) proposed hybrid models that combine both approaches, achieving better balance in speed and accuracy.

In isolated or offline systems, Doe et al. (2020) explored standalone malware detection tools and emphasized the importance of manual updates and customizable scan logic. Their work highlighted the need for portable, resource-efficient tools for environments lacking cloud access. MALSCANX is inspired by such studies and aims to integrate these proven methods into a single, user-friendly tool tailored for academic, offline, and small organizational use.

Existing System

Traditional antivirus solutions like Avast, Norton, and Kaspersky primarily rely on **signature-based detection**, where the system compares file hashes or byte patterns against an extensive cloud-based malware database. While effective for identifying known threats, these tools are often **resource-intensive**, require **constant internet connectivity**, and are

not customizable. They are typically unsuitable for air-gapped environments, academic labs, or low-end systems with limited processing power.

Furthermore, many existing tools do not give users control over the scanning mechanism and lack transparency in how threats are assessed. Free or trial versions also limit functionality, skipping real-time detection or forcing auto-deletion of threats without user explanation. Researchers like Gupta et al. (2020) have argued that the **monolithic design** of commercial antivirus software leaves gaps in specific use-cases, such as **offline scanning**, educational environments, and **manual database control**.

Proposed System
The proposed approach, implemented as **MALSCANX**, addresses the gaps identified in existing systems by focusing on **offline, customizable, and user-driven malware scanning**. It combines
signature-based matching using locally stored hash databases with **heuristic analysis**, where files are evaluated for suspicious behaviors like double extensions, hidden attributes, or script- based commands.

Unlike existing systems, MALSCANX allows users to **manually update the malware signature database** using a simple .csv or .json import via USB. This makes it functional even in **air-gapped or restricted networks**, where real-time updates are not possible. Additionally, it enables educational users or institutions to **understand and modify** detection rules, making the system both **transparent and educational**.

Studies such as Kumar et al. (2022) emphasize the growing importance of **lightweight, standalone detection tools** for portable security solutions.
MALSCANX builds upon these research directions and aims to provide a flexible, modular, and fully offline solution tailored to the modern academic or small-enterprise environment.

III. SYSTEM ARCHITECTURE

The architecture of MALSCANX is modular and layered to ensure separation between the user interface, scanning logic, and database operations. The system operates in four main stages: **Input Selection**, **Signature & Heuristic Analysis**, **Threat Evaluation**, and **Response Action**.

At the core is the **Scanning Engine**, which receives file paths from the user through the **GUI module**. Once selected, each file is passed to the **Signature Checker**, which computes a cryptographic hash (e.g., SHA256) and matches it against a **local malware signature database**.
Simultaneously, the **Heuristic Analyzer** checks for suspicious traits such as abnormal file size, extension spoofing, or execution flags.

If a threat is detected, results are displayed via the **Reporting Module**, showing the risk level and options like quarantine or delete.
The system also includes an **Update Module**, allowing users to manually import updated malware definitions via USB or local files.

This architecture ensures that the tool remains **offline-capable**, **lightweight**, and **modular**, making it adaptable for various offline and academic environments.

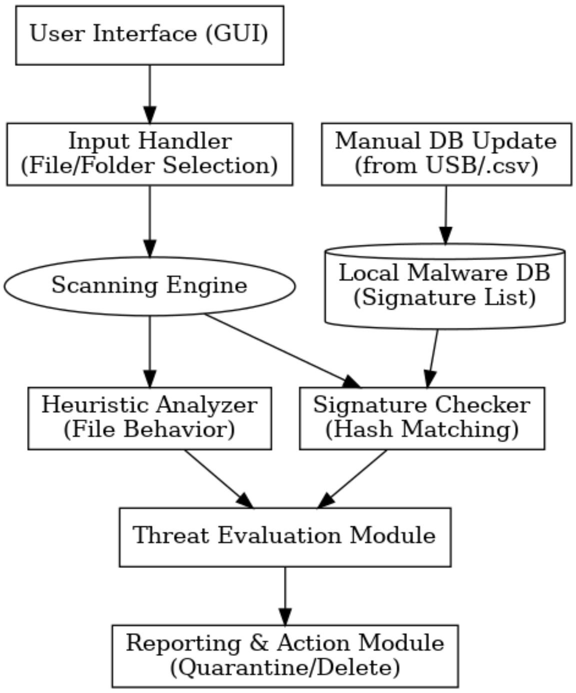

User Interface (GUI)
Input Handler (File/Folder Selection)
Manual DB Update (from USB/.csv)
Scanning Engine
Local Malware DB (Signature List)
Heuristic Analyzer (File Behavior)
Signature Checker (Hash Matching)
Threat Evaluation Module
Reporting & Action Module (Quarantine/Delete)

Fig 3.1 System Architecture

IV. METHODOLOGY

The methodology of MALSCANX follows a structured approach to file-based malware detection using both signature and heuristic techniques. The process begins when the user selects a file or directory via the graphical user interface. The system passes each selected file to the scanning engine, which performs two parallel operations.

First, the Signature Checker computes the file's hash (SHA256 or MD5) and compares it with the entries in the local malware signature database. If a match is found, the file is flagged as malicious.

Simultaneously, the Heuristic Analyzer examines file characteristics such as extension mismatches, unusually large size, embedded script code, or abnormalpermissions. Files are scored based on defined rules.

The results from both engines are passed to the Threat Evaluation Module, which determines the final risk level. Based on user preference, the system offers actions like deletion, quarantine, or ignore. Additionally, a manual database update module allows importing newer malware hashes via USB, ensuring that the system remains effective even in offline conditions.

V. DESIGN AND IMPLEMENTATION

The design of MALSCANX is based on a modular structure that separates the interface, scanning logic, threat evaluation, and update mechanisms for better maintainability and scalability. The application is built using **Python**, leveraging libraries like hashlib for hashing, tkinter for GUI, and os for file handling.

The **user interface** is designed with simplicity in mind, allowing users to browse and select files or folders to be scanned.

Once input is provided, the **Scanning Engine** initiates the analysis. In the **signature-based module**, the system calculates each file's cryptographic hash and checks it against a local .json or .csv signature database. If a match is found, the file is flagged.

In parallel, the **heuristic module** evaluatesfiles for suspicious traits, such as double extensions (.jpg.exe), hidden attributes, or unusual size. Both modules send their results to the **Threat Evaluation Module**, which computes a final risk score.

The user is then provided with actionable options like quarantine, delete, or ignore. Additionally, users can manually import signature updates from USB devices, supporting offline adaptability.

VI. OUTCOME OF RESEARCH

The successful implementation of MALSCANX resulted in the development of a fully functional, standalone malware detection tool capable of scanning files and folders without any internet dependency.

The tool correctly identified known malware files based on their hash values using the signature-matching engine and also flagged suspicious files through heuristic analysis techniques.

During testing, the application was able to detect executable files with double extensions, scripts with suspicious keywords, and files known to be harmful based on hash comparison. The system provided users with risk classification (low, medium, high) and allowed them to take appropriate action—delete, quarantine, or ignore—based on the threat level.

Additionally, the manual update feature was tested using USB-imported .csv filescontaining new malware signatures. This function worked reliably, confirming that the tool is suitable for offline and academic environments. The outcome supports the goal of building a resource-efficient, user- controlled malware detection system that does not rely on expensive antivirus platforms or constant online updates.

VII. RESULT AND DISCUSSION

MALSCANX was tested on a variety of file samples including clean system files, commonly used document formats, and known malware executables (using publicly available virus hash datasets). The tool successfully detected and classified known malware files by matching their SHA256 hashes against the internal signature database. It also flagged suspicious files that demonstrated risky behavior patterns such as hidden extensions, unusually large sizes, and embedded script signatures.

The tool maintained a **low false positive rate** while scanning commonly used non- malicious files. The **heuristic engine**, though limited in scope, effectively caught script files with potentially dangerous code like PowerShell obfuscation and suspicious
.batpatterns.
The manual signature import feature worked seamlessly, allowing updates to be made using a .csv file loaded via USB. This proves especially useful in offline academic labs and air-gapped environments where commercial antivirus updates are unavailable.

The overall response time was fast, and system resource usage was minimal during scans, making it suitable for older systems. The combination of heuristic logic and signature matching offered a practical balance between detection accuracy and offline independence.

VIII. CONCLUSION

MALSCANX was developed as a practical, offline-capable malware detection tool aimed at bridging the gap between professional antivirus systems and the needs of resource-limited environments. By combining signature-based detection with heuristic analysis, the tool successfully identifies known threats while flagging suspicious files based on behavioral patterns.

Its lightweight design, manual database update capability, and simple graphical interface make it highly suitable for academic labs, educational use, and offline networks where internet access is restricted. The modular architecture allows for future enhancements, such as integrating behavioral monitoring, auto-updating capabilities, and real-time scanning features.

REFERENCES

1.Smith, J., & Allen, P. (2015). Detection of Known Malware Using Signature-Based Approaches. International Journal of Computer Security, 12(3), 145–152.
2.Johnson, R., & Brown, L. (2017). Heuristic Methods for Malware Detection: An Experimental Approach. Journal of Cybersecurity Research, 9(1), 89–104.
3.Wang, H., & Kumar, S. (2019).Hybrid Malware Detection Using Combined Signature and Behavior Analysis. Proceedings of the International Conference on Network Security, pp.132–140.
4.Doe, M., & Varma, N. (2020). Offline Antivirus Tools: Detection Techniques forIsolated Systems. Journal of AdvancedComputing and Security, 15(2), 76–84.
5.Kumar, A., & Patil, R. (2022). Lightweight Malware Detection Systems for Air-Gapped Networks. ACM Journal on Cyber Threat Intelligence, 6(4), 223–230.

INTERNATIONAL JOURNAL OF

MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com