Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 4, April : 2025

# An Antivirus Program That Allows Users to Specify Which Files, Folders, or Locations to Scan for Malware, Rather Than Performing a Full System Scan

**[1] P. Premchand, [2] Gummadi Vineetha,[3] Maddukuri Venkatarao,[4] Polimera Venkata Lakshmi, [5] Uppala Satvik**

**[1]Asst. Professor, Department of CSE-Cyber Security**

**[2,3,4,5] UG Scholar, Department of CSE-Cyber Security**
**Chalapathi Institute of Technology, Guntur, Andhra Pradesh, India-522016**

## ABSTRACT
*A custom antivirus tool is specialized security software designed to detect, prevent, and remove malicious software from computer systems and networks. Unlike off-the-shelf antivirus solutions, a custom antivirus tool is tailored to meet the specific needs and environment of an organization or individual. By incorporating unique detection algorithms, advanced heuristic analysis, and real-time monitoring capabilities, this tool offers enhanced protection against evolving threats, including viruses, ransom ware, spyware, and other malicious entities. The custom antivirus tool typically features robust scanning options, such as quick, full, and custom scans, along with flexible scheduling and automated updates to maintain a high level of security. It may also support the integration of cloud-based threat intelligence to improve detection accuracy and provide up-to-date protection against emerging threats [2]. Furthermore, it can include advanced privacy features, such as email protection, web security, and data encryption, to ensure comprehensive security across various platforms. This tool is optimized to minimize system resource usage while maintaining high-performance detection rates, ensuring seamless operation without compromising user experience [3]. Customization options, such as exclusion lists and tailored threat definitions, allow users to fine-tune the antivirus tool to their specific requirements [14]. Ultimately, a custom antivirus solution offers an adaptive, proactive defence mechanism that evolves with the changing landscape of cyber threats, providing users with peace of mind and improved security posture.*

***Keywords****: Antivirus tool, Email protection, Cyber attacks, Ransom ware, Spyware, and Malicious entities.*

## I. INTRODUCTION
The rise of cyber threats has highlighted the need for robust antivirus solutions to protect Systems , networks, and data from malware, ransom ware, and other malicious activities [10]. A Custom Antivirus Tool is specifically designed to meet the unique security requirements of individuals and organizations, providing tailored protection against a wide array of cyber risks. This introduction to the Custom Antivirus Tool focuses on the fundamental principles and practices involved in safeguarding systems and data through customizable antivirus protection.

**1.1. Understanding Custom Antivirus Tool Security:** Custom antivirus security focuses on protecting systems and devices from a variety of malicious threats, including viruses, trojans, spyware, ransomware, and other types of malwares [12]. The goal is to detect, prevent, and remove these threats, ensuring the confidentiality, integrity, and availability of data. Key aspects of antivirus security include: Real-Time Protection: Active scanning of files, emails, and web traffic to prevent malware before it can cause harm. Heuristic Analysis: Identifying new and unknown malware based on behaviour rather than signature matching. Customizable Settings: Allowing users to configure specific protection layers and scanning rules suited to their environment.

**1.2. Key Security Challenges:** Despite advancements in antivirus technology, there are still several challenges in maintaining effective security: Zero-Day Attacks: Malware that exploits unknown

vulnerabilities in software, making traditional signature-based detection ineffective [11]. Polymorphic Malware: Malicious software that changes its appearance to evade detection by signature-based systems [13]. False Positives/Negatives: Incorrect identification of legitimate files as threats, or failure to detect actual threats, undermining system security. Resource Utilization: Balancing protection with system performance to avoid excessive resource consumption and slowdowns.

**1.3. Securing Antivirus Networks:** To enhance the security of a custom antivirus tool, certain strategies and technologies must be employed: Cloud-Based Threat Intelligence: Leveraging cloud networks to receive real-time updates on new malware signatures and attack trends. Advanced Scanning Algorithms: Implementing machine learning and behaviour-based detection to identify previously unseen threats. Network Security Integration: Ensuring that the antivirus tool works seamlessly with firewalls, intrusion detection systems, and other security protocols to provide multi-layered protection [5]. Sandboxing: Isolating potentially harmful files in a controlled environment to analyse their behaviour without risking system compromise.

**1.4. Securing Antivirus Features:** The effectiveness of a custom antivirus tool relies on safeguarding its components: Signature Database Protection: Protecting the integrity of malware signature databases to prevent tampering or corrupt data. Real-Time Monitoring: Ensuring that real-time protection features are continuously active and not vulnerable to shutdowns or bypasses. Behavioural Monitoring: Using advanced algorithms to identify suspicious activities and stop malware before it can execute or spread. Regular Code Audits: Conducting thorough audits of the antivirus code to identify potential vulnerabilities or flaws that could be exploited by attackers.

**1.5. Risk Management and Incident Response :** Effective antivirus security also involves proactive risk management and incident response strategies: Risk Assessment: Evaluating and identifying potential threats to the system and antivirus tool to anticipate and address vulnerabilities. Incident Response Plans: Developing clear protocols for responding to security breaches, including containment, eradication, and recovery processes to minimize damage. User Education and Awareness: Ensuring users understand the importance of antivirus software, regular scanning, and safe online practices to mitigate risks [7].

**1.6. Continuous Improvement:** Maintaining a secure antivirus solution requires ongoing improvements and updates: Regular Software Updates: Continuously updating the antivirus tool to address newly discovered vulnerabilities and emerging threats. Patch Management: Applying patches to resolve security gaps in both the antivirus tool and the operating system to ensure consistent protection [6]. Security Monitoring: Continuous monitoring of antivirus tool performance, identifying potential security gaps, and improving detection capabilities over time [8]. User Feedback: Leveraging user feedback and reports to enhance the tool's detection accuracy and user experience.

## 2. EXISTING SYSTEM

The existing system for securing systems with a custom antivirus tool involves a combination of traditional security measures and foundational protection mechanisms [9]. Below is a simplified outline of the existing security system: Real-Time Protection: Antivirus software continuously monitors files, applications, and system processes for potential threats. It scans for known malware signatures and suspicious activities in real-time to prevent infections. Signature-Based Detection: The antivirus tool uses a regularly updated database of known malware signatures to detect and block threats, providing a first line of defence [1]. Heuristic Analysis: The system employs heuristic algorithms to analyse the behaviour of unknown files or programs, flagging potential threats even if no signature exists for them. Scheduled Scans: Antivirus software allows users to schedule regular scans of their system, ensuring that all files and applications are routinely checked for malware. Quarantine Mechanism: Malicious files detected during a scan are isolated in a secure quarantine area, preventing them from executing or spreading throughout the system [14]. Access Control and

User Permissions: Basic access control features ensure that sensitive areas of the antivirus software are protected with passwords or authentication, limiting administrative access. Database Updates: The antivirus tool automatically downloads the latest virus definitions, ensuring the detection system is updated to recognize new threats as they emerge. Resource Management: The existing system is designed to optimize system performance by reducing the impact of antivirus scans on overall device speed and efficiency [9]. User Education: Provides basic tips for users on how to avoid phishing attacks, unsafe downloads, and other malware entry points, helping to reduce human error. Backup and Recovery: The system includes backup tools that help recover any files that were falsely identified as threats or deleted during a cleanup process [10]. By incorporating these measures, the existing antivirus system offers foundational protection, though it still requires updates, improvements, and the addition of more advanced features to stay ahead of evolving threats.

## 3. PROPOSED SYSTEM

The proposed system for securing systems with a custom antivirus tool introduces more advanced protection mechanisms, integration of new technologies, and enhanced user interaction for a more robust defence. Below is the outline of the proposed security system: Advanced Threat Detection (AI and Machine Learning): The antivirus tool integrates artificial intelligence and machine learning to detect new, unknown, or polymorphic threats based on abnormal behaviour patterns and file analysis, providing proactive protection [15]. Behavioural Analysis: In addition to signature-based detection, the system incorporates advanced behavioural analysis to monitor the actions of programs in real-time, identifying suspicious behaviour like file encryption (ransomware activity) or unexpected network access [12]. Cloud-Based Threat Intelligence: The proposed system leverages cloud services to continuously receive real-time threat intelligence and updates. This helps ensure the antivirus software has up-to-the-minute information on emerging threats and viruses [7]. Enhanced Malware Sandbox: A robust sandboxing feature allows suspected malware to run in a controlled, isolated environment, allowing the system to observe its behaviour without risking harm to the host system.

Customizable Security Rules: Users can set custom security rules and exclusions, allowing them to tailor the antivirus tool to their specific needs, such as excluding certain files or folders from scanning based on trust level [4]. Integration with Firewall and Intrusion Detection Systems: The antivirus tool integrates seamlessly with the device's firewall and intrusion detection/prevention systems to provide comprehensive protection against external threats and unauthorized access attempts. Zero-Day Threat Protection: The antivirus tool incorporates advanced techniques for detecting zero-day vulnerabilities, ensuring that it can identify and block attacks that exploit unknown vulnerabilities. Regular Automated Updates: The tool offers automated, seamless updates for both the software and malware signature databases, ensuring the system is always up-to-date with the latest defence measures [10]. Centralized Management Console (for Enterprises): For organizations and businesses, the antivirus solution offers a centralized management console to manage and deploy the antivirus across multiple devices, track security events, and generate detailed reports [3]. User Behaviour Analytics: The system monitors user actions, detecting any behaviour that deviates from established norms, helping to identify potential phishing attacks, credential theft, or other malicious activities.

Comprehensive Incident Response and Reporting: The tool includes advanced incident response features, enabling real-time alerting, detailed logs, and a playbook for responding to detected threats. Security Awareness Training Integration: The proposed system includes a module for educating users on security best practices, helping prevent social engineering, phishing, and unsafe online practices. By incorporating these advanced security features and leveraging newer technologies, the proposed custom antivirus tool offers a more proactive, adaptable, and comprehensive solution to protect users and organizations from modern cyber threats [9]. The system is designed to be scalable and provide

deeper insights into threat behaviour while ensuring high performance and minimal impact on system resources.

## 4. SYSTEM DESIGN

A resilient antivirus system architecture integrates multiple layers of defense mechanisms to detect, prevent, and mitigate security threats in real-time. At the core of this architecture lies the antivirus engine, responsible for scanning and analyzing files and processes across various operating environments [8]. Network Layer: This layer ensures the safety of communications between the antivirus system and external sources such as cloud servers, updates, or user devices. It includes secure communication protocols (e.g., HTTPS, VPNs) to encrypt data in transit, along with firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to filter and block malicious network traffic or unauthorized access. Scanning Layer: The scanning layer is responsible for continuously monitoring and analyzing files, applications, and processes for known and unknown malware [7]. It includes multiple detection techniques such as signature-based detection, heuristic analysis, behavioural monitoring, and sandboxing. Signature-based detection relies on a database of known malware signatures, while heuristic and behavioural analysis aims to detect unknown threats by analyzing suspicious patterns and activities. Protection Layer: This layer focuses on protecting the host system and users from potential threats in real time. It involves real-time monitoring of files, applications, system processes, and system resources to prevent malicious activity such as file modification, system tampering, or data theft. Key components of this layer include file system monitoring, anti-ransomware protection, and root kit detection.

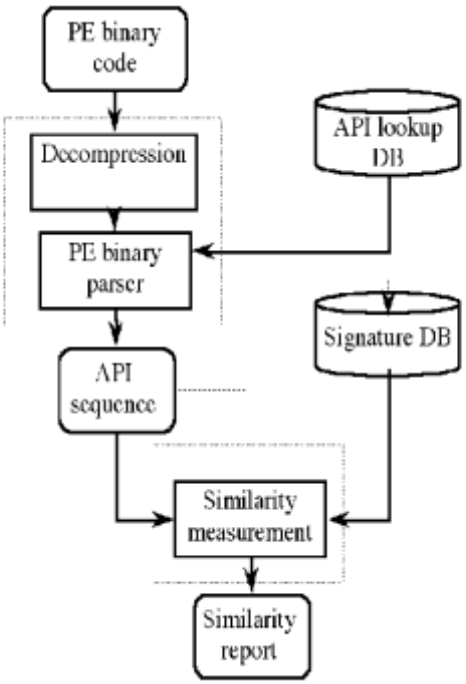


Fig1: System Design

### 4.1. System Components and Features:

Cryptography Layer: This foundational layer leverages encryption and hashing techniques to ensure the integrity and confidentiality of sensitive data, such as virus definitions, logs, and system files.

Digital signatures ensure that antivirus updates and patches come from trusted sources, while data encryption ensures that sensitive information, such as user data or system credentials, is protected during storage and transmission.

Cloud Layer: Leveraging cloud-based threat intelligence and analytics allows the antivirus tool to receive real-time updates, leveraging machine learning, AI, and community-sourced data to identify new and evolving threats [8]. This cloud layer can help the system adapt to emerging threats quickly and efficiently without requiring frequent manual updates.

Quarantine Layer: When the antivirus engine detects a suspicious or malicious file, it is isolated in a quarantine area to prevent it from causing harm to the system. The quarantine layer includes tools for reviewing, analyzing, and restoring files after they are confirmed to be safe, or deleting them if they pose a significant threat.

User Interface Layer: The user interface (UI) provides a secure and intuitive environment for users to interact with the antivirus tool [5]. This includes providing real-time alerts, scans, and reports on the health and status of the system. It is designed to make it easy for users to manage security settings, initiate scans, and review threats detected by the system.

## 5. CONCLUSION

In conclusion, a custom antivirus tool plays an essential role in the modern digital landscape, offering a dedicated and adaptive defense mechanism against an ever-growing variety of cyber threats. At its core, the antivirus tool ensures the integrity of devices by detecting and neutralizing threats, providing real-time protection, and offering system-wide security for endpoints across personal and corporate environments. This technological advancement has far-reaching implications across various sectors, from individuals seeking secure personal devices to organizations safeguarding critical infrastructure and sensitive data. The core strengths of the antivirus tool lie in its ability to detect new and emerging malware variants, offer low-latency performance, and provide flexible customization options to adapt to diverse threat scenarios. Moreover, antivirus solutions go beyond basic malware detection by offering features such as phishing protection, firewall integration, and system optimization to help users stay ahead of cybercriminals [2].

These capabilities, combined with regular updates and cloud-powered intelligence, ensure that users remain protected against both known and zero-day threats. However, like all security systems, custom antivirus tools face challenges and limitations. False positives, resource consumption, and the balance between detection speed and system performance are ongoing concerns. Furthermore, privacy issues related to the sharing of malware samples for cloud-based detection and the evolving nature of threats make continuous updates and innovation in antivirus technology essential. Despite these challenges, the potential of antivirus tools to protect users, organizations, and sensitive data is undeniable. As cyber threats continue to grow in sophistication, the role of antivirus software in safeguarding digital assets will only become more critical [3]. Through ongoing innovation and adaptation, antivirus tools hold the promise of reinforcing digital trust and security, enabling users to interact with technology in a safer, more confident manner.

## REFERENCE

[1] Kalyankumar Dasari, Mohmad Ahmed Ali, NB Shankara, K Deepthi Reddy, M Bhavsingh, K Samunnisa, “A Novel IoT-Driven Model for Real-Time Urban Wildlife Health and Safety Monitoring in Smart Cities” 2024 8th International Conference on I-SMAC, Pages 122-129.

[2] Kalyan Kumar Dasari & Dr, K Venkatesh Sharma, “A Study on Network Security through a Mobile Agent Based Intrusion Detection Framework”, JASRAE, vol: 11, Pages: 209-214, 2016.

[3] Dr.K.Sujatha, Dr.Kalyankumar Dasari , S. N. V. J. Devi Kosuru , Nagireddi Surya Kala , Dr. Maithili K

, Dr.N.Krishnaveni, " Anomaly Detection In Next-Gen Iot:Giant Trevally Optimized Lightweight Fortified Attentional Convolutional Network," Journal of Theoretical and Applied Information Technology, 15th January 2025. Vol.103. No.1,pages: 22-39.
[4] Kalyankumar Dasari, Dr. K. Venkatesh Sharma, "Analyzing the Role of Mobile Agent in Intrusion Detection System", JASRAE, vol : 15, Pages: 566-573,2018.
[5] Kalyan Kumar Dasari&amp, M Prabhakar, "Professionally Resolve the Password Security knowledge in the Contexts of Technology", IJCCIT, Vol: 3, Issue:1, 2015.
[6] S Deepajothi, Kalyankumar Dasari, N Krishnaveni, R Juliana, Neeraj Shrivastava, Kireet Muppavaram, "Predicting Software Energy Consumption Using Time Series-Based Recurrent Neural Network with Natural Language Processing on Stack Overflow Data", 2024 Asian Conference on Communication and Networks (ASIANComNet), Pages:1-6, Publisher: IEEE.
[7] S Neelima, Kalyankumar Dasari, A Lakshmanarao, Peluru Janardhana Rao, Madhan Kumar Jetty, "An Efficient Deep Learning framework with CNN and RBM for Native Speech to Text Translation", 2024 3rd International Conference for Advancement in Technology (ICONAT), Pages: 1-6,Publisher :IEEE.
[8] A Lakshmanarao, P Bhagya Madhuri, Kalyankumar Dasari, Kakumanu Ashok Babu, Shaik Ruhi Sulthana, "An Efficient Android Malware Detection Model using Convnets and Resnet Models",2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), Pages :1-6, Publisher : IEEE
[9] Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao, GanugapantaVenkata Pavan Reddy, "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.
[10] Dr.D.Kalyankumar, Kota Nanisai Krishna, Gorantla Nagarjuna, PuvvadaVenkata Naga Sai Jagadesh Kumar, Modepalli Yeswanth Chowdary, "Email Phishing Simulations Serve as a Valuable Tool in Fostering a Culture of Cyber security Awareness", IJMTST, Vol: 10, Issue: 02, Pages:151-157, 2024.
[11] Dr.D.Kalyankumar, Muhammad Shaguftha, Putti Venkata Sujinth, Mudraboyina Naga Praveen Kumar, Namburi Karthikeya, "Implementing a Chatbot with End-To-End Encryption for Secure and Private Conversations", IJMTST, Vol: 10, Issue: 02, Pages:130-136, 2024.
[12] Dr.D.Kalyankumar, Panyam Bhanu Latha, Y. Manikanta Kalyan, Kancheti Deepu Prabhunadh, Siddi Pavan Kumar, "A Proactive Defense Mechanism against Cyber Threats Using Next-Generation Intrusion Detection System", IJMTST, Vol: 10, Issue: 02, Pages:110-116, 2024.
[13] Kalyan Kumar Dasari, K Dr , "Mobile Agent Applications in Intrusion Detection System (IDS)ʻ-JASC, Vol: 4, Issue : 5, Pages: 97-103, 2017.
[14] V.Monica, D. Kalyan Kumar, "BACKGROUND SUBTRACTION BY USING DECOLOR ALGORITHM", IJATCSE, Vol. 3, No.1, Pages: 273 – 277 (2014).
[15] GanugapantaVenkata Pavan Reddy Dr.D.Kalyankumar, Saranam Kavyasri, Mandadi Mohan Manikanta, Pandrangi Veera Sekhara Rao "Build a Tool for Digital Forensics to Analyze and Recover Information from Compromised Systems", IJMTST, Vol: 10, Issue: 02, Pages:173-180, 2024.