[1]Xiao-Bin Wang, Guang-Yuan Yang, Yi-Chao Liand Dan Liu, “Review on the application of artificial intelligence in antivirus detection system<sup>i</sup>”, 2008. doi: 10.1109/iccis.2008.4670733.

The significance of antivirus systems is emphasized by the authors in light of the growing occurrence of malware and computer viruses. The primary technologies utilized in antivirus systems, namely virus prevention, detection, elimination, and immunity, are outlined. Virus detection involves ascertaining whether a file harbors a virus, and this can be accomplished through the utilization of monitor technology or file-self detection technology.

1. Start the program.
2. Initialize the intelligent agent and necessary data structures.
3. Scan the specified directory or directories to gather file information.
4. Iterate through each file in the directory.
5. Retrieve file attributes such as name, size, type, and date created/modified.
6. Apply predefined rules or machine learning algorithms to categorize the file based on its attributes.
7. Determine the appropriate category or categories for the file.
8. Store the file in the respective category or create a new category if needed.
9. Repeat steps 4-8 for all files in the directory.
10. Optionally, provide feedback or suggestions to improve categorization accuracy.
11. Display the categorized files or generate a report.
12. Allow the user to perform actions on the categorized files, such as moving, copying, deleting, or tagging.
13. Provide an option to save the categorized file information for future reference.
14. End the program.

## Pros of the file type intelligent agent approach to identify viruses based on file type:

Efficiency: By analyzing the file type, the intelligent agent can quickly determine whether a file is potentially malicious or not. This helps to streamline the virus identification process and save time.

[1]H.-D. Huang, C.-S. Lee, H.-Y. Kao, Y.-L. Tsaiand J.-G. Chang, “Malware behavioral analysis system: TWMAN”, 2011. doi: 10.1109/ia.2011.5953604.

Accuracy: Certain file types, such as executable files or scripts, are more commonly associated with malware. The intelligent agent can leverage this knowledge to prioritize the analysis of files with high-risk file types, increasing the accuracy of virus detection.

MADE:SecurityAnalyticsforEnterpriseThreatDetection <https://doi.org/10.1145/3274694.3274710>

Early Detection: File type analysis can provide an initial indication of potential threats even before performing a detailed scan or analysis of the file's content. This allows for early detection of potential viruses, helping to mitigate the risk of infection.

**UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware : Amin Kharaz, Sajjad Arshad, Collin Mulliner, William Robertson, and Engin Kirda, Northeastern University**

Reduction of False Positives: By focusing on specific file types associated with malware, the intelligent agent can reduce false positives. This means that legitimate files are less likely to be mistakenly flagged as viruses, reducing the impact on system performance and user experience.

**Nazca:DetectingMalwareDistribution inLarge-ScaleNetworks**

## Cons of the file type intelligent agent approach:

Limited Scope: Relying solely on file type analysis may not be sufficient to detect all types of viruses. Sophisticated malware can disguise itself by using innocent-looking file types or by manipulating file headers. Therefore, additional analysis methods are required to ensure comprehensive virus detection.

<https://www.usenix.org/legacy/event/sec06/tech/full_papers/kirda/kirda_html/>

Vulnerability to File Type Spoofing: Malicious actors can intentionally manipulate the file type information to mislead the intelligent agent. They may change the file extension or modify file headers to make the file appear as a benign file type. This can bypass the file type analysis and evade detection.

The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation

File Type Ambiguity: Some file types can be associated with both legitimate and malicious files. For example, certain script files can be used for legitimate purposes as well as for executing malware. In such cases, relying solely on file type analysis may result in false negatives or the misclassification of files.

[1]Sudhakar and S. Kumar, “An emerging threat Fileless malware: a survey and research challenges”, *Cybersecurity*, vol. 3, no. 1, 2020, doi: 10.1186/s42400-019-0043-x.

Lack of Behavioral Analysis: File type analysis focuses primarily on static attributes of files and does not consider the behavioral aspects of potential viruses. Advanced malware can exhibit polymorphic behavior or use obfuscation techniques, making it challenging to identify based solely on file type analysis.

# **Malware behavioural detection and vaccine development by using a support vector model classifier** <https://www.sciencedirect.com/science/article/pii/S0022000014001780>