Scanning Antivirus (Your shield against digital threats)

Name : Yogeshwar Saini

Roll No. E23MCAG0025

Class / Sec : MCA – B1

Email : e23mcag0025@bennett.edu.in

PROJECT OVERVIEW:

Malware code which is affected from different types of viruses is become an biggest problem in the world of internet on the global level . while on demand scans can be used once . there are many techniques and technology which are used to protect the user and their valuable data . most of the time we are trying to implement the real time scanning mechanism but this technology is using too much system resources such as memory and CPU and provide too much less protection .

In this research paper we suggest you to different open source plateform an dthe method of real time scanning antivirus and describing about their performanence , and the method on which the antivirus is work on them and provide their advantage and disadvantage on real time scanning . such kind of researches and its method helps in successfully implementation of real time scanning mechanism and provide the direction in which we can move our next step in creating an real time scanning antivirus .

The main aim of this work is to build the Scanning antivirus that consume the minimal storage of the virus database it contains the three major component i.e 1) scan engine 2) virus database 3). Updater . . database contain all the hashes of the viruses . creating a database is not a difficult task while the virus scanner in running mode for this process much amount of memory is needed . to overcome this type of difficulity we introduce such type of virus scanner that uses minimum amount of main memory space . in this processs of scanning some pattern are loaded into a memory at a time and the engine scanning the file according to a particular pattern . once the scan is complete then the another set of pattern will be loaded and the scan is repeated again . hence antivirus scan engine should be customize to be adaptable with the modified database.

Keywords – Malwares ; Pattern Matching ; Signatures.

INTRODUCTION

An scanning antivirus is one of the most commonly security solution used in the electronics devices like desktop, tablets etc . some factors that affects the performanence of an scanning antivirus are speed, memory consumption and upto date virus database (VDB). Scan speed and memory utilization depends upon the size of the database . that means that smaller the database scanning process will be faster and the larger database will require much amount of memory . we can not reduce the database size as we know the viruses hashes are much play an important role in scanning the file and detecting the copy of viruses . an another reason is also for not deleting the the database is that it conatin the hashes of known viruses.

Whenever a new virus is discovered in the markst it is impossible for an virus scanner which is existed into the system is detect the same . therefore a new hashes is generated for each newly discovered virus and the same hashes should be updated in the database by the vendor once it is tested successfully.

LITRATURE REVIEW

The paper provides an overview of tools used for malware analysis. It discusses both static and dynamic analysis tools, including their functions and how they are used. The paper emphasizes the importance of choosing the right tools based on the specific needs of the analysis. It also highlights that some tools are available for free, while others require purchase. The paper serves as a guide for analysts to select the appropriate tools for malware analysis.

The paper "Methods of virus detection and their limitations" by Umakant Mishra discusses the challenges in detecting and scanning viruses due to the increasing number of viruses and their signatures, which in turn increases the size of the signature database and scanning time. The paper explores techniques to improve scanning speed and resource efficiency, such as scanning only those viruses according to the type of files, scanning only specific areas of a file depending on the file type, and selecting only one or a few detection algorithms to run each time the scanner is loaded, either randomly or by other selection criteria, without running all detection algorithms at once. These techniques help reduce the total number of search operations and scanning time, and avoid searching through the entire file looking for infection.

The paper "Introduction to Virus Scanners" discusses the methods of scanning for viruses, emphasizing on-demand and on-the-fly scanning. It explains that both methods involve the same scanning process but differ in the order and priority of scanning. The paper also covers the methods of virus removal and file repairing, highlighting that anti-virus programs may attempt to repair infected files, quarantine them, or delete them if necessary. It also discusses the recovery of original program code in case of infections. The paper provides a comprehensive overview of virus scanning and removal techniques, shedding light on the advantages and drawbacks of each method

The paper "Signature-based Malware Detection for Unstructured Big Data Using Hadoop Map-Reduce" proposes a signature-based malware detection system using Hadoop Map-Reduce. It discusses the challenges of malware detection in unstructured big data and the need for a scalable solution. The paper suggests that larger shifts in malware signatures could be achieved by utilizing more characters of existing signatures. It explains the Hadoop Map-Reduce approach, which involves the use of mappers and reducers to process large data sets in parallel on a cluster of computers. The paper also outlines the implementation of the algorithm, highlighting the potential improvements in performance by working the I/O of nodes concurrently, providing more throughput .

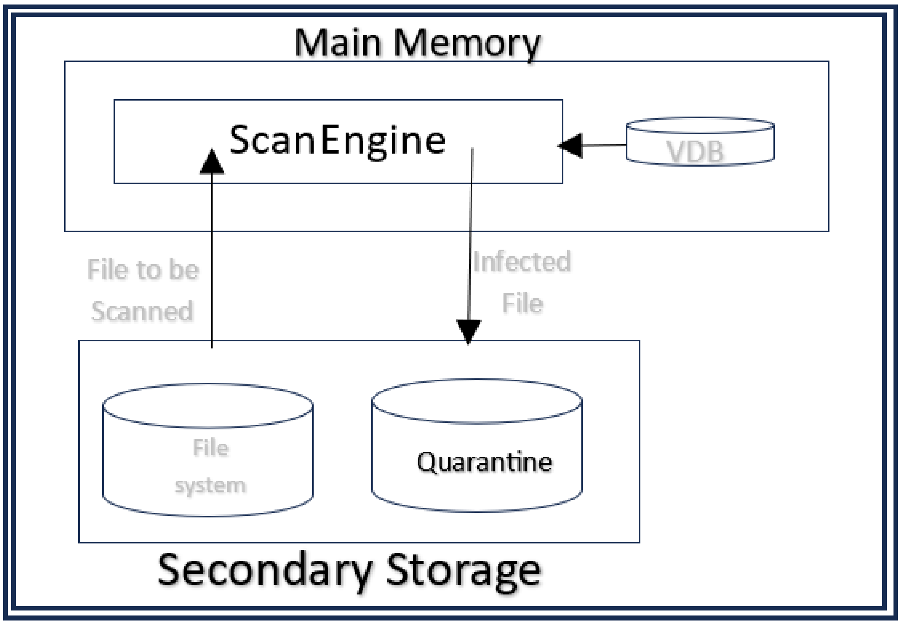
The paper "Improving speed of virus scanning" discusses a method for accelerating virus scanning by reducing the time spent on reading data from a disk. The patent (7036147) describes a technique that involves using two threads in parallel, with one thread reading the data from the disk while the other thread scans the pre-read data. This approach aims to eliminate the delay associated with reading the data, which can account for up to 40% of the scanning time. By employing this segmentation method, the invention seeks to improve the efficiency of virus scanning operations, particularly in the context of a large number of virus signatures
The paper "Scantime Antivirus Evasion And Malware Deployment Using Silent-SFX" explores the use of Self-Extracting Archive (SFX) for malicious purposes, particularly the concept of Silent SFX, which can silently deploy malware into a target machine, bypassing runtime-based antivirus scans.

The study analyzes the working of SFX, the functioning of Silent SFX, and provides a comparison between Traditional SFX and Silent SFX. The paper also presents the results of testing Silent SFX, showing its effectiveness against scan-time antivirus scans. However, it notes that this technique does not provide security during runtime and real-time antivirus scans, only working against user-initiated or automated scan-time antivirus scans

The paper provides an overview of real-time antivirus scanning engines, discussing various techniques and approaches to detect and prevent malware infections. It covers topics such as Bloom Filters, Deep Packet Inspection, Cache-Resident Filters, Summary Cache, SHOCK, Dazuko, efficient signature-based malware detection on mobi le devices, energy-greedy anomalies, and behavioral detection of malware on mobile handsets .The paper also explores the use of smart batteries for mobile device profiling and intrusion detection .

Working Of Antivirus Software :

In this phase we describe the working process of the antivirus software that how it work what is its performance during the process . here first module is the scanning phase in which engine starts its work which has the ability to scan the files and after completed its scanning process it declared the result of the absence and presence of virus in the system. With the help of virus hashes . here antivirus engine matches the hash of every file with its virus file if hashes were matched it declared that file if infected and make that file in the quarantine mode . here we have to know that both the engine and database are loaded in the same memory and they should stay there until the scan engine stay. Heare quarantine file is restricted to meet with the another file .



UNDERSTANDING MALWARE HASHES :

Virus detection software are considerd as the fast scanning software which are used to protect detect and removes threats from the computer such as system virus , malicious files , spyware , hijackers and many more viruses , these types of software are helpful to protect us from social engineering attacks . here we describe that scanner used database for scanning the virus these hashes are generally carried out from the database in the sequential order.

1. **MD5 hashes Techniques :** In this techniques the virus infected files matched by Md5 hashes which will present already in the database and checksum of a target file or of a specific location .
2. **Sha256 hashes Techniques:** In this process When a user opens, executes, or downloads a file, the antivirus software calculates the SHA-256 hash of the file and checks it against its database which is present into the memory. If there is a match, the file is flagged as malicious.

SCANNING AND METHOD OF DETECTION :

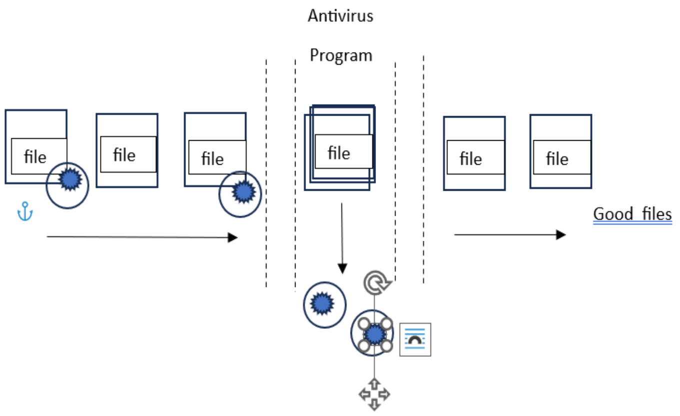


Diagram depict the scanning process (1)

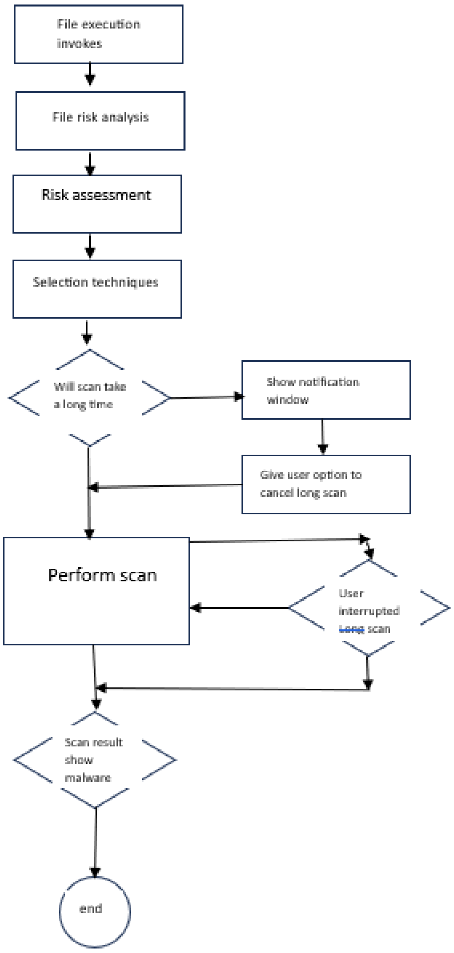
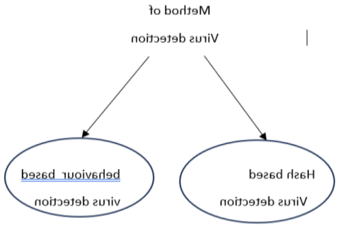


Diagram depict the scanning process (ii)

Method of Malware detection :

There are various process of virus detection . i.e signature based malware detection and the behaviour based malware detection .


Method of Virus detection
behaviour based virus detection
Hash based Virus detection

- Here in the hashes based malware detection (generally which is renowed as signature scanning method) . this type of method used to compare the content of a file to the hashes which are present into the memory . if the hash value is matched then it declare the presence of virus in the system , if not match then it declare that file is free from virus .

- On the other hand the technology which is known as behaviour based detection . this method identify the unwanted activity of such code which is present in the form of virus will be detected by its unknown behaviour . some drawback of this method is that some time it cannot detect exact malware and return false result.

Experimental Analysis :

Our analysis on the scanning antivirus provides the different time comparision over the different files when applying some algorithm . because most of the scanning antivirus presently existing are not able to scan the whole content of the files and the folders , while they just scan either the header or footer of the file or may be generally depend on the type of the file which is present for it as the type of input .

METHODOLOGY USED :

Some methodology are used in the scanning antivirus software are given below :-

1. **File Hashing :** in this each file using a method called SHA-@%^ hashing . this is a long string that represent the content of the file .
2. **Malware Detection by Hash :**
   It checks if the hashes matches any known malware hashes it identify the malware .
3. **Virus scanner :** similar to the folder scanner , the function searches for virus in different folder . if the virus or malicious file is to be found it start monitoring its activities and track its name and the path of the infected file .
4. **Ram Booster :** in this process engine close some specific application that are known to consume a amount of memory . this can help to maintain complete system performance.
5. **Real Time Protection :** this engine regularly monitors a specific folder for checking any change which is created or not , if there is any disturbance occur in the file or folder then it start checking for the malware in the real time .

in this research we have used some tools in static or dynamic mode for analysing the malware :

Basic Static Tools

Tools	Description
CFF explorer	Used to analyse malicious file without disturbing the inner structure .
Virus total.com	Is a type of website used for finding viruses

Some Dynamic analysis Tools

Tools	Description
• VMWare Work station • Process • Monitor • Process explorer	• Is used as a virtual machine to run the malware sample. • Used to monitor all activity. • Within the system in real time. • Is used for navigate the task that are currently running in a system path.

CONCLUSION :

In this paper we have to be focused on that roadmap of creating best and efficient scanning antivirus which is used to detect malware , which is staying inside the distributed file system .. as we know that the demand of antivirus increases day by day and corresponding storage is also needed . it require fast and best way to identify the malware against the stored data . we have to implement different pattern matching algorithm to identify the hashes of the files. The aim of our experiment is to perform the scanning of data on the real world data set . as we know that the size of our dataset increase , our scanning speedup also will be increase . in this way we can optimize our result of scanning and get better performanence in terms of execution time .

REFERENCES :

[1] O. Erdogan and P. Cao, Hash-AV: fast virus signature scanning by cache-resident filters, Proc. Of the International Conference on Systems and Networks Communications (ICSNC), 2007. [5] M. Fisk and G. Varghese, An analysis of fast string matching applied to content-based forwarding and intrusion detection, Technical Report CS2001-0670, University of California – San Diego, 2002. [6] H. Yin, et al., "Panorama: capturing system-wide information flow for malware detection and analysis," in Proceedings of the 14th ACM conference on Computer and communications security, 2007, pp.

[2] Chieh-Jen Cheng, 2012. “A Scalable high-performance virus detection processor against a Large Pattern Set for Embedded Network Security”, 20-5.

[3] http://www.tomshardware.com/reviews/anti-virus-virus-sc anner-performance.2777.html

[4] Umakant Mishra, “An Introduction to Computer Viruses”, trizsite journal, Feb 2007, http://www.trizsite.com/articles.

[5] Y. Miretskiy, A. Das, C. P. Wright, E. Zadok “Avfs: An OnAccess Anti-Virus File System”, In proceedings of the 13th USENIX Security Symposium, 6-6, 2004.

[6]. J. Ogness “Dazuko: an open solution to facilitate on-access scanning”, Virus Bulletin, 2003.