Bachelor's thesis

Information and Communications Technology 2025

Raheel Abbas Hussain Hussain

Evaluating Antivirus Software

A Comparative Analysis of Detection Methodologies and Performance Metrics in Modern Antivirus Solutions

Bachelor’s Thesis | Abstract

Turku University of Applied Sciences

Information & Communications Technology 2025 | 30 pages

Raheel Abbas Hussain Hussain

Evaluating Antivirus Software

A Comparative Analysis of Detection Methodologies and Performance Metrics in Modern Antivirus Solutions

By reviewing existing literature, this study identifies and evaluates the key aspects of antivirus programs, focusing on their malware detection capabilities, system performance, and user experience. Key methods of malware detection, such as signature-based, heuristic-based, and behavior-based detection, are analyzed for their ability to identify both known and emerging threats. The impact of antivirus software on system performance is explored, with attention to resource consumption, scanning speed, and boot time. Additional security features such as real-time protection, firewall, phishing defense, ransomware detection, and VPN support are also discussed in detail. The research highlights the importance of regular software updates, cross- platform compatibility, and customer support in enhancing the user experience. Furthermore, the comparison between free and paid antivirus versions is reviewed, considering whether advanced features justify the cost. Independent evaluations from reputable testing organizations, such as AV Test and AV Comparatives, are also incorporated to provide an objective measure of antivirus performance. The study concludes by offering insights into the most effective antivirus solutions for different user needs and scenarios, emphasizing the growing role of artificial intelligence in improving software efficiency and security.

Keywords:

Malware, Technology, cyber security, Window Defender, Total AV.

Contents

1 Introduction

In this modern era of technology, everyone is connected to the internet for several purposes. However, connecting devices to the internet is not safe as data is an important commodity for everyone. Itsinherent risks, and reckless behavior exacerbates the likelihood of malware infection. Various strategies exist for reducing the risk of computer compromise, including educating users and the installation of antivirus applications. Malware has progressed since their inception, and their authors are becoming more astute. Their recent developments are increasingly intricate and challenging to identify and eliminate. Hackers have expanded their scope of influencing calamity to include the World Wide Web (Garba 2021). Therefore, we need effective protection against these cyber security threats. As many security threats evolve every day so the best antivirus software should detect new viruses as well as update the virus information.

The threat landscape has evolved in tandem with this technological change. Hackers, online criminals, and funded by the state entities have refined their techniques for identifying vulnerabilities to extract information obtain financial gain or secure a diplomatic edge. Consequently, there is an immediate necessity for effective security due to the rapid advancement of technological advances and the conducive environment for cyber assaults (Alenezi 2020).

AT&T Alien Labs™ recently found BotenaGo malware, which compromised millions of IoT devices. In March 2021, a group of hackers gained access to and control over hundreds of Verkada security cameras, exposing user credentials openly on the internet. SonicWall's 2022 Cyber Threat Report shows a steady increase in IoT malware threats, with over 60 million attacks registered in 2021, the greatest number ever recorded in a single year. IoT malware attacks have climbed by 6%, with routers being the most targeted devices (Grønli 2023). Smart Environments provide user-friendly and efficient IoT infrastructure, with a focus on sustainability. Used devices, components, and generated data are subject to the user's requirements, with sustainability and adaptation as primary goals. To protect IoT infrastructure from cyber-

attacks, open-source and commercial software solutions including anti-viruses, firewalls, anti-pattern detection, and security protocols can boost cybersecurity (Bhandari 2023).

1.1 Research Objective and Rationale

The objective of the study is to evaluate antivirus software to understand its effectiveness in safeguarding against modern cyber threats. The current study aims to assess antivirus software to determine their effectiveness against modern security threats. It also aims to contribute to cybersecurity knowledge and enhance antiviral defense. The study evaluates the performance of all antivirus software available online.

1.2 Overview of Cyberattack Types

The term "cyber security" refers to both the technologies and the procedure that aims to safeguard systems and networks from becoming disrupted, damaged, or accessed without authorization. Because information is currently the foundation of every business, security measures have become increasingly important for a nation's security forces, healthcare facilities, large companies, entrepreneurs, and other citizens. If the data is not in a secure place, the entire organization is in danger (Garba 2021).

The security of any organization starts with these three principles: Availability, Confidentiality, and Integrity, on which the protection of computing devices has been standardized from the advent of mainframe systems. Modern Cyber security threats target these principles to steal or alter valuable information. (Perwej 2021) Examples of cyber security threats include:

Ransomware Attack: Such attacks make the targeted individual's information, documents, equipment, or computers unavailable and useless the hacker receives a payment for ransom, malware takes control of everything. Ransom is demanded often in cryptocurrency. Data may be leaked if ransom payment

is not paid. (Perwej 2021).

Distributed Denial of Service (DDoS): This kind of threat aims to block users from reaching services by overwhelming the amount of traffic that normally would have access to those capabilities as its target boot controller.

Internet of Things Attack (IoT): Through the IoT Attack many devices connected to daily life activities have been controlled by a third party. These devices include cameras, wearable gadgets and healthcare equipment etc. Security breaches, interruptions of healthcare activities, and threats to patient confidentiality and security can all result from these types of attacks (Perwej,2021).

Phishing Attack: In Phishing the attacker tries to steal sensitive information such as credit card information and passwords. In such an event, a target responds to a fake email or message requesting immediate reaction. These are the forms of social engineering. When hackers strike block chain systems, digital currency wallets, or transfers, they are committing block chain and crypto currency hacks.

1.3 Malware Detection and Analysis Techniques

As we know, malware can enter our system in any way so our system must have the capability to detect and remove viruses to prevent malware attacks (Alkhalil 2021).
Before we go into details, we must know that malware analysis may be conducted by using the following malware analysis principles:

1.3.1 Static Analysis

In Static Analysis the expert analyzes the malware program but does not run the code. To detect fraudulent activity, static inspection checks the contents of the file. Malware infrastructure, software libraries, or downloaded files could be located with its help. Key Statistic Analysis Methods are File Signature identification, Hashing, Metadata inspection, String Analysis, Disassembly

and Packing detection (Fedák 2020).

1.3.2 Dynamic Analysis

The Dynamic Analysis necessitates a comprehensive assessment of the computer network activity produced by the malware. So, the security professionals execute the suspected code into the safe environment.

This isolated system allows security experts to observe malware activity absent the danger of it infecting their systems or breaching the company connection (Fedák 2020).

1.3.3 Hybrid Analysis

A Hybrid Analysis can be performed by combining both techniques of Static and Dynamic Analysis. With blended examination, anti-virus programs can first look for recognized signatures and then, if needed, run potentially dangerous files in a secure environment to see how they behave. This two-layer method is being increasingly used to fix the problems with applications that are only rigid or changeable (Fedák 2020).

1.3.4 Reverse Engineering

The process of Reverse Engineering entails analyzing the viruses coding to comprehend its rationale, architecture, and operational characteristics (Fedák 2020). It includes the following processes:

Decompiling: This is the process of translating malware's executable code into a more advanced programming syntax.

Control Flow Graph (CFG) Analysis: This involves charting the interactions among various code segments to comprehend its overall functionality.

Decryption/Unpacking: Numerous malware specimens employ packing or encryption to obscure their actual activity. Reverse engineering frequently entails dismantling these obfuscation methods.

1.3.5 Analysis of Network Traffic

Antivirus frequently interacts with distant computers to obtain directives, leak information, or retrieve additional harmful packages. Detection is conducted by analyzing unusual network traffic and connections to suspicious or known malicious servers.

1.3.6 Domains Creation Algorithms (DGAs)

A virus employs DGAs to produce several domain addresses to circumvent identification. Detection is conducted by observing DNS request patterns and matching them with known DGA behavior.

1.3.7 Integration of Threat Intelligence

Incorporating information from threat intelligence into virus research facilitates the identification of recognized indications of compromise (IoCs), like IP numbers, file hash values, or domains associated with virus groups (Fedák 2020).

1.3.8 Threat Feeds

Threat feeds are resources that deliver current data on malware patterns, Indicators of Compromise (IoCs), and the Strategies, Methods, and Processes deployed by attackers. Threat feeds provide real-time updates, while “Integration of Threat Intelligence” includes broader threat data for analysis.

1.3.9 Automation and Machine Learning

Automation and machine learning (ML) increasingly facilitate the acceleration of detection and removal of malware, especially in pattern identification and automated execution of routine operations (Fedák 2020).

Machine Learning Algorithms are employed to categorize and identify malware utilizing extensive databases of prior attacks.

1.5 Research Methodology

The research design is based solely on a literature review, focusing on the critical analysis of existing studies and scholarly perspectives related to antivirus applications. Rather than conducting empirical testing or qualitative research, this study explores how antivirus software is described in existing literature in terms of its ability to detect, mitigate, and eliminate diverse malware kinds.

The review examines a range of detection methods commonly cited in

research, including signature-based detection, heuristic-based detection, behavior-based detection, sandboxing techniques, and cloud-based and AI-powered systems. These methods are analyzed through existing academic and industry sources to understand their working mechanisms, strengths, and limitations.

By relying entirely on secondary data, the study aims to provide a comprehensive and contextual understanding of modern antivirus technologies, emphasizing how evolving threats and technological advances shape their development and effectiveness.

2. Analytical Review of Malware Detection and Antivirus Systems

People and businesses are more vulnerable to a wide range of cyber security risks because they depend more and more on technology. The best way to lower threats is to use surveillance applications, which have changed over time to keep up with malware (Garba 2021). Malware, which earlier easy to track, has become more complicated over time. It now includes ransomware, and fraudulent websites. These detrimental applications have grown in both number and accessibility, now affecting not just users as individuals but also whole parts of the population and the infrastructure of the country.

Malware is always getting better, which is why antivirus applications are always getting better. Scammers are always improving the ways they get around standard safeguards. As the world of information security changes, antivirus programs have become an important part of keeping computers safer from hackers and data loss. Scholars have pointed out that one of the biggest problems in digital safety is the fact that malware is always changing so it cannot be found. This means that antivirus software needs to be able to rapidly refresh their danger databases and use artificial intelligence to find fresh forms of malware (Alenezi 2020).

2.1 Malware Classification

However, the malicious code has not only evolved technically, but also in terms of threat. They not only damage files or computer systems, as they behaved in the 1970s and 1980s, but they are also used to espion, theft of information or require money ransom (Palacios 2022).

Viruses are usually included in existing software; they are activated when the user Performs software. Their outcomes are diverse and start with slowing down. Worms, unlike computer viruses, may replicate themselves via networks without user intervention.

Trojans are malicious programs that are hidden within normal software to avoid detection. This type of malicious application can accomplish any action it was programmed to do. Spyware, like worms, installs itself without user intervention and collects unauthorized user or system information (da Costa 2022).

Adware is typically installed with other software and displays unwanted advertising, such as pop-up windows, without the user's permission. Adware now appears via browser extensions or plugins.

Ransomware: It is typically performed by another malware, like a worm, virus, or trojan. The objective is to completely sequester the system, encrypt all files, and demand payment from users or organizations.

Rootkits are designed to infiltrate and conceal themselves within critical parts of infected devices, including sections that typical users cannot easily reach. Their goal is to gain control of the system and enable remote manipulation while staying undetected.

2.2 Anti-virus Threat Detection

The Antivirus software primarily detects and classifies this form of malware using signatures, heuristics, rules, and artificial intelligence. Traditionally, antivirus systems use signature detection, which relies on a vendor-generated database. The system compares downloaded files to a database to detect malware. Signature-based detection only detects previously detected samples whose signatures are kept in the antivirus database. Heuristic detection approaches were created to address the limitations of signature-based detection methods (Palacios 2022).

Heuristic algorithms use many scoring factors to assess if a file is harmful or not. The most popular three methods of completing this analysis are
Generic: Compares the activities of one file to those of another, which has already been classified as harmful.

Passive: Analyses each file independently to determine how it operates.
Active: Runs the sample in a safe environment (sandbox) to detect malicious

activities. Implementing payload activation delays helps mitigate the difficulty and large delays associated with this method.

Heuristic analysis has two key issues: a high number of false negatives and a heavy workload on the system. However, it increases antivirus software's detection of new malware samples. AI-powered machine learning techniques are now being used to enhance antiviral systems. Using these techniques enables large-scale data analysis, pattern recognition, and automated prediction formulation. Endpoint Detection and Response (EDR), also known as Endpoint Thread Detection and Response (ETDR), is a client-side security mechanism that collects data and sends it to a centralized console for processing in a distributed computing environment. Real-time correlation of collected data helps detect and analyze suspicious activity, which is then processed in a centralized database (Palacios 2022).

2.3 Malware Detection and Anti-virus applications Performance

Research has empirically evaluated cyber security applications by exposing them to diverse samples of malware, incorporating zero-day vulnerabilities and adaptive infections (Moritaka 2024). Likewise, performed dynamic assessment, assessing the program's effectiveness under sandbox conditions and uncovering notable discrepancies in malware detection times (Moritaka 2024).

In another research, Researcher established a practical environment for testing in which security applications were subjected to URLs identified as hosting illicit downloads. The findings indicated that while numerous antivirus systems effectively obstructed older, recognized malware, their efficacy markedly diminished when faced with newer, less-documented risks. The error rate for novel samples of malware was below 60% in all of the evaluated products, signifying that antivirus applications face challenges in addressing newly emerging risks, especially those leveraging zero-day security vulnerabilities (Limer 2024).

Furthermore, the research indicated that signature-based identification approaches, commonly employed in antivirus software, frequently proved inadequate for identifying malware disseminated via advanced drive-by download techniques.

Consequently, numerous antivirus products have begun using heuristic evaluation and behavioral methods for detection to enhance efficacy against unfamiliar viruses. The study authors determined that while antivirus application is a crucial element of a holistic security approach, dependence exclusively on signature-based detection creates considerable vulnerabilities in defense. The research underscores the necessity of ongoing upgrades and sophisticated detection methods in contemporary antivirus programs to successfully protect against swiftly emerging threats.

2.4 Comparison Between Theoretical Claims and Empirical Findings

Despite assertions by antivirus manufacturers regarding elevated detection rates and negligible overall effect, empirical evaluations, including those carried out by researchers, present a contrasting narrative (Akhtar, 2021). Their comparative research evaluated the efficacy of antivirus systems against a diverse array of malware samples and revealed that numerous solutions failed to achieve the outstanding detection rates they claimed, particularly for novel, emerging malware variants.

Notwithstanding considerable progress in empirical testing procedures, deficiencies persist in the studies. A plethora of research has concentrated on conventional malware detection, whereas little effort has been directed toward emerging threats, like IoT risks and cryptocurrency mining malware. Moreover, most of the empirical testing is performed in controlled settings, which may not adequately reflect the intricacies of actual network infrastructures (Aslan, 2020).

The study also provided empirical proof comparing both static and dynamic evaluation methodologies among multiple antivirus programs. The results indicate that although static evaluation is more rapid and consumes fewer computer resources, it inadequately identifies disguised or encoded malware. Conversely, dynamic detection, which executes malware within a safe environment, proved more effective at identifying advanced malware, albeit necessitating greater computational power (da Costa, 2022).

Researchers further performed empirical testing to evaluate the influence of widely used antivirus programs on system efficiency. Their evaluations encompassed assessing CPU use, memory utilization, and system reactivity during comprehensive system inspections. Several antivirus programs, despite exhibiting high recognition rates, impose a great deal on system assets, resulting in diminished device performance an essential consideration for customers desiring strong protection without sacrificing system performance (Garba, 2021).

3. Different Methods Used in Antivirus and How They Work

Antivirus software has evolved significantly from its initial static models to more adaptive, AI-driven systems. Below are the most widely used methods, each contributing uniquely to threat detection and mitigation.

3.1 Signature Based Detection

One of the earliest and most foundational methods of antivirus protection is signature-based detection, a technique that remains relevant in many systems today. This method relies on a database of known virus "signatures," which are unique strings or patterns of code associated with specific malware. The antivirus software scans files and applications, comparing them to its database. If a match is found, the file is flagged as a threat (Symantec, 2020). However, this method is only effective against known threats. With the rapid evolution of malware, particularly zero-day attacks, signature-based detection often falls short in identifying new or mutated threats (O'Kane et al., 2018). Due to this limitation, researchers and developers have turned to more dynamic and predictive techniques to detect previously unseen or modified malware strains.

3.2 Heuristic Based Detection

To overcome the rigidity of static signature databases, many antivirus systems now incorporate heuristic-based detection. Heuristic analysis involves scanning code for suspicious properties or behaviors that resemble known threats, even if they do not match any existing signature. For instance, if a program attempts to alter system files or communicate with remote servers without user input, it might be flagged as suspicious. This method increases the likelihood of detecting new or unknown viruses, though it also raises the risk of false positives (Souri & Hosseini, 2018). While heuristics provide a proactive approach, the growing complexity of malware calls for even more sophisticated, behavior-oriented solutions.

3.3 Behavior Based Detection

Moving beyond code analysis, behavior-based detection monitors the real-time actions of applications to identify malicious activity. This method evaluates how a program behaves once it is running, looking for signs such as unauthorized data encryption, system configuration changes, or attempts to disable security functions. AI and machine

learning algorithms are especially useful here, as they can learn normal behavior patterns and flag anomalies (Kolter&Maloof, 2006). As behavior-based systems rely heavily on real-time processing, cloud integration and fast decision- making algorithms become increasingly critical to system performance.

3.4 Sandboxing Techniques

Another powerful strategy is sandboxing, which enables antivirus systems to safely examine suspicious files in isolated environments. Sandboxing involves executing potentially malicious code in a virtual environment separated from the user's actual system. This allows the antivirus to observe the file's behavior in a controlled space. If the program acts maliciously, it is quarantined or removed before it can cause harm (Sikorski&Honig, 2012). This technique is particularly effective against zero-day exploits and polymorphic malware, which may otherwise evade traditional detection. Although sandboxing offers detailed behavioral insights, its computational demands necessitate efficient resource allocation and AI-driven prioritization.

3.5 Cloud Based and AI Powered Antivirus Systems

The increasing complexity and volume of cyber threats have led to the adoption of cloud-based and AI-driven antivirus models, offering scalability and real-time updates. Cloud-based antivirus systems offload heavy processing to remote servers, allowing for faster threat detection without burdening local resources. AI enhances these systems by identifying patterns across vast datasets in real-time, enabling them to detect emerging threats more effectively than static models (Kaspersky Labs, 2021). Machine learning also plays a role in adaptive security, wherein the system continually evolves its understanding of malicious behavior (Shen et al., 2020). These models also improve user experience by minimizing system slowdown and delivering real-time threat alerts with minimal disruption. The integration of cloud and AI not only improves antivirus efficiency but also exemplifies how smart cybersecurity systems are converging with AI-powered user experiences in smart devices.

Recent studies, such as Bhandari (2023), emphasize the critical role of advanced detection algorithms in enhancing the accuracy and efficiency of cybersecurity systems, making them more capable of identifying emerging threats.

3.6 Role of AI and Machine Learning in Modern Antivirus Solutions

Modern antivirus solutions have transcended traditional reactive models by integrating AI and machine learning to enable proactive Adaptive, and real-time defense. These advancements not only enhance digital safety but also contribute significantly to user experience, ensuring that smart devices and applications remain both secure and efficient. As the landscape of digital interaction grows more complex, understanding these antivirus mechanisms is essential to appreciating how AI holistically shapes our daily technological environments.

With the constant evolution of malware, traditional antivirus solutions often struggle to keep up. However, advancements in machine learning and artificial intelligence, as noted by Alenezi (2020), have significantly enhanced the ability of modern antivirus software to detect and counteract new, previously unseen threats in real-time.

4. Examples of Antivirus Software

This study compares Windows Defender and Total AV based only on existing literature. These two antivirus programs were selected because one is built-in (Windows Defender) and the other is third-party (Total AV), offering different approaches to protection. Windows Defender is the default antivirus integrated into the widely used Windows operating system, providing basic protection without additional setup. Total AV, as a popular third-party program, offers extra features and customization options. By focusing on these two, the study provides a representative comparison of the main antivirus types used by typical users, making the analysis practical and manageable without covering all available software. The comparison focuses on key points like features, performance, user experience, and malware detection, without practical testing.

4.1 Overview

Window Defender: The integrated defense for both Windows 10 and 11 is called Windows Defender, which is also called Microsoft's antivirus protection. It has made to give users basic characteristics without requiring extra setup, which makes it easy for them to use (Pogonin 2022).

Total AV: Total AV is an external antivirus program that provides a variety of protective features, such as protection against viruses, tools for optimizing the computer's performance, and confidentiality features. Membership is required to access enhanced features, even though it claims to offer full protection (Botacin 2020).

4.2 Installation and setup

Window Defender: Windows systems will instinctively set it up. Anyone can use it without having done setting it up first. The Windows Update service takes care of changes, which run in the background whenever possible (parveen 2024).

Total AV: Needs to be downloaded and set up by hand. The procedure for installing it is easy, but individuals may see ads for paid services during the configuration process

4.3 User Interface

Window Defender: Built within the Windows configuration menus, it has an easy, clear structure that shows the present level of safety. Individuals are rapidly introduced to the various tools for scanning and configurations thanks to the easy interface (Körber 2022).

Total AV: It has a trendy, colorful design that is meant to look good. Even though it is easy to navigate and use, certain individuals might discover that the large number of tools and features makes it harder to navigate their way around (parveen 2024).

4.4 Malware Detection

Window Defender: Protects against spyware, Trojan horses, malware that demands ransom and other types of malwares with real-time effectiveness. Utilizes cloud-based security and behavioral detection, which assists in identifying vulnerabilities that have not been seen before (Perwej 2021).

Total AV: Employs a blend of detection using signatures and heuristic evaluation to recognize malware. Individuals have indicated that, although it proficiently identifies known threats, it may be less successful in identifying unknown vulnerabilities in comparison with additional sophisticated antivirus programs.

4.5 Performance

Window Defender: Recognized for its negligible effect on system efficiency. It operates rapidly in the background, enabling individuals to execute everyday activities without discernible delays.

Total AV: Some users report higher resource consumption, particularly during full system scans. This can lead to noticeable slowdowns, especially on older or less powerful systems (Perwej 2021).

4.6 Intrusiveness

Window Defender is non-intrusive because It only sends alerts for important things, like threats found or changes that need to be done, which makes the way users interact better.

Total Av is intrusive in nature because it usually display message for additional features like upgrades especially when individuals using free versions of the AV. This Disturb user experience.

5. Key Aspects in evaluating antivirus software.

After getting some detailed overview from all the available resources about the viruses and anti-viruses used. We are now discussing the keys aspects that are essential in evaluating any antivirus performance which is the focus of the current study. These factors offer an extensive foundation for evaluating the complete efficacy, financial impact, and user satisfaction of any solution (Botacin 2020).
Costa (2022) emphasizes the significance of evaluating antivirus software by focusing on its real-time detection abilities and impact on system performance. Costa also notes that critical performance factors, such as detection accuracy and minimal system lag, play a key role in determining the effectiveness of antivirus solutions.

5.1 Detecting and Removing Malware

Rates of Detecting Malware: That is undoubtedly a highly essential feature of antivirus software. Identification ratios denote the proportion of recognized risks that the program can discern throughout a scan. Optimal detection stages, approaching 100%, are essential, including not just conventional viruses but other malware classifications such as spyware, ransomware, malware, and worms. Contemporary anti-virus systems often include both detections based on signatures, which identifies known malware trends, and behavior-based identification, which alerts unusual behavior regardless of prior encounters with the threat (Aslan 2020).

Scanning in Real Time: The application conducts constant monitoring of system operation, promptly assessing any newly introduced items or processes currently running for potential vulnerabilities. This functionality inhibits virus execution by isolating or eliminating it before doing harm. Real-time screening is essential for delivering current protection against developing vulnerabilities (Talukder 2020).

Updating Database: The efficacy of any anti-virus is significantly dependent upon the regularity of its widespread definitions update. Given the regular generation of hundreds of new samples of malware, security applications must regularly update

their information stores with novel viral signatures. Systems that are updated regularly with no human participation are favored, since they minimize susceptibility gaps.

Zero Day Protecting Against Threats: Zero-day vulnerabilities involve defects in programs which have already been identified but remain unaddressed by the program manufacturer. Antivirus applications using predictive or behavioral detection may identify and mitigate zero-day viruses by identifying anomalous file or system behaviors, regardless of the absence of a corresponding virus signature in a database. Contemporary antivirus applications use artificial intelligence techniques to anticipate and obstruct zero-day infections in real time (Aslan, 2020).

5.2 Impact on System Performance

Resource Consumption: Antivirus software that excessively utilizes machine assets like RAM, central processing unit (CPU), or storage impedes system efficiency, particularly during scanning or while immediate protection is enabled. Lighter antivirus applications have been created to enhance speed while maintaining machine usability. Certain applications have settings to limit the consumption of resources during demanded activities like video games or multimedia processing (Kasarapu 2024).

Speed of Scanning: A reliable antivirus must provide effective and rapid monitoring options. Comprehensive system evaluations often need more time since they include examining each document and activity. Nonetheless, many antivirus programs use methods such as storing earlier scanned data or just scanning newly created and updated files to expedite the process. Certain antivirus software provides many scanning options, including rapid scans (targeting dangerous regions) and bespoke scans (focusing on files or folders) (Kasarapu 2024).

Effect on Booting Time: Antivirus software can occasionally prolong machines starting by doing preliminary inspections at boot-up. Assessing the application's impact on the boot procedure assists with evaluating its potential to be a nuisance during routine use (Talukder 2020).

5.3 Security Features that may Additionally provided

Firewall: A firewall oversees network communications, preventing unauthorized entry while permitting legal connection. Numerous security applications have an integrated firewall, offering an additional degree of security, especially while accessing open or unsecured networks.

Protection against Phasing: Phishing attacks use deceptive web pages, emails, or texts to manipulate people into revealing private data such as credentials as well as data about their credit cards. An antivirus program equipped with phishing prevention functionalities scrutinizes message headings, webpage URLs, and other types of information to obstruct accessibility to recognized fraudulent websites and prevent illicit messages from entering your spam folder (Aslan 2020).

Protection against Ransomware: A user's personal information is encrypted by ransomware, which then requests money to unlock the information. An antivirus program that includes specialist protection against ransomware detects suspected file encrypting activity, instantly backs up information, and isolates documents that have been infected. Additionally, it should prevent any effort to take control over system files (Sharmeen 2020).

Protection of Email and Web: A considerable number of attacks may infiltrate a system via harmful websites or files sent via email. Web security that examines Websites for indications of harmful material and email defense that examines documents and hyperlinks to avoid malware and phishing frauds should both be included in antivirus applications. Additionally, there are solutions that provide extensions for browsers that may prevent potentially hazardous Webpages within immediate response (Sharmeen 2020).

Virtual Private Network: Using a virtual private network (VPN) to secure your connection to the internet makes it more difficult for attackers to steal information, especially when it is sent across free Wi-Fi networks. The inclusion of a virtual private network (VPN) within certain antivirus packages is a valuable addition since it guarantees confidential and safe surfing (Usman 2021).

Protecting Passwords: Secured credentials may be generated, stored, and managed with the help of password managers. In addition to eliminating fraudulent attempts that are connected to passwords, a built-in password manager inside the security package minimizes the possibility that insecure passwords will be utilized (Usman 2021).

Parental Control: Parental controls being a useful tool for family members because they allow parents to observe and limit their children's exposure to improper information. To ensure the security of their children, enhanced controls for parents provide limited-time access, material screening, and surveillance of social networking and messaging applications (Doucaussoy 2020).

5.4 Easy to Use

The graphical user interface must be straightforward, streamlined, and user-friendly, accommodating both technologically proficient individuals and novices. Customers must be enabled easily to reach essential functionality such as executing scans, reviewing protection reports, and modifying configurations. Clarity does not inherently imply a reduction in possibilities; a well-constructed user interface enables experienced users to navigate through advanced functions with no confusing the fundamental interface (Aslan 2020).

5.5 Cross platform Compatibility

It must have cross platform support. In the contemporary multi-device landscape, an antivirus program is supposed to be compatible with multiple operating systems, including Mac OS X, Windows, Android phones and tablets and iOS. Seek antivirus software that provides a singular license applicable to different gadgets alongside operating systems (Rafa 2021).

5.6 Customer Support

Effective customer service is essential whether facing technical challenges or need assistance with configurations. Numerous antivirus suppliers provide round-the-clock help by telephone, via email, or via live chat. Furthermore, use a comprehensive internet database, discussion boards, or YouTube tutorials to assist in troubleshooting problems (Rafa 2021).

5.7 Cloud protection

Online antivirus solutions delegate portions of screening and evaluation to distant servers, therefore alleviating the strain on the current machine. Consequently, this implies that information is transmitted to remote servers. Guarantee that the online security component complies with stringent security requirements, including strong authentication and limited confidential information retention (Wang 2020).

5.8 Comparison of Free and Paid Versions

Complimentary editions frequently deliver fundamental security, but they do not include more complex capabilities like firewalls, protection against ransomware,

or support for customers if they are available. It is essential to determine if changing to the premium edition is worthwhile the additional cost depending on the requirements that you have in mind from the beginning (Wang 2020).

5.9 Multi device Licensing

Licenses for many security packages are available that protect multiple gadgets that are used inside a home. When you have several devices, such as mobile phones, tablets, and personal computers, you should determine whether the software's licensing model offers value.

5.10 Independent Lab Test Result

AV Test: This is a premier professional group that meticulously evaluates antivirus programs. They assess programs according to security, efficiency, and user-friendliness, delivering a total rating for each one. Seek an antivirus program that regularly demonstrates superior performance in these evaluations (Fedák 2020).

AV Comparatives: AV-Comparatives, a reputable laboratory, conduct comprehensive assessments across several situations, which include practical protection assessments, malware eradication testing, and efficiency analyses. These tests provide a definitive assessment of the applications performance under varying settings (Leka 2022).

SE Labs: SE Labs emphasizes practical testing settings, replicating authentic attack paths to assess the efficacy of anti-virus programs. Their comprehensive assessments provide an understanding of the advantages and limitations of many items.

All the above Aspects provide a vital role in evaluating any antivirus performances.

6. Conclusion and Recommendation

This study examined the effectiveness of antivirus software in combating modern cyber threats through a literature-based analysis. The review highlighted the evolution of malware, from basic viruses to sophisticated ransomware and zero-day exploits, and how antivirus solutions have adapted with advanced detection methods like heuristic analysis, behavior monitoring, and AI-driven cloud security.

A comparison between Windows Defender and Total AV revealed that while Windows Defender offers seamless, low-impact protection for everyday users, Total AV provides additional features such as phishing protection and system optimization though at the cost of higher resource usage. The study also identified key evaluation criteria for antivirus software, including detection rates, system performance impact, and extra security functionalities.

Despite advancements, challenges remain, particularly in detecting emerging IoT-based threats and balancing security with system efficiency. Future research should focus on real-world testing and AI-enhanced threat prediction to further strengthen cybersecurity defenses.

For optimal protection, users should choose antivirus software based on their specific needs. Casual users may find Windows Defender sufficient for basic security, while advanced users should consider third-party solutions such as Total AV for enhanced features such as ransomware protection and VPN. Organizations must prioritize AI-driven, behavior-based detection and employee training to combat sophisticated threats. Future development should focus on lightweight, real-time protection and IoT security integration to address emerging risks effectively.

References

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: A review. International journal of communication networks and information security, 12(3), 326-337. DOI: 10.17762/ijcnis.v12i3.4723.

Alkhalli, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 1-15. DOI: 10.3389/fcomp.2021.563060

Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE access, 8, 6249-6271. DOI: 10.1109/ACCESS.2019.2963724

Botacin, M., Ceschin, F., De Geus, P., & Grégio, A. (2020). We need to talk about antiviruses: Challenges & pitfalls of AV evaluations. Computers & Security. DOI: 10.1016/j.cose.2020.101859

Bhandari, G., Lyth, A., Shalaginov, A., & Grønli, T. M. (2023). Distributed deep neural- network-based middleware for cyber-attacks detection in smart IoT ecosystem: A novel framework and performance evaluation approach. Electronics, 12(2), 298. DOI: 10.3390/electronics12020298

da Costa, F. H., Medeiros, I., Menezes, T., da Silva, J. V., da Silva, I. L., Bonifácio, R., & Ribeiro, M. (2022). Exploring the use of static and dynamic analysis to improve the performance of the mining sandbox approach for android malware identification. Journal of Systems and Software, 183, 111092. DOI: 10.1016/j.jss.2021.111092

Fedák, A., & Štulrajter, J. (2020). Fundamentals of static malware analysis: Principles, methods and tools. Science & Military Journal, 15(1), 45–53. Retrieved from https://sm.aos.sk/images/dokumenty/archiv/1-20/Article7.pdf.

Garba, F. A., Yarima, F. U., Kunya, K. I., Abdullahi, F. U., Bello, A. A., Abba, A., & Musa, A. L. (2021). Evaluating Antivirus Evasion Tools Against Bitdefender Antivirus. *Proceedings of the International Conference on FINTECH Opportunities and Challenges, 18*, 1-6.

Kasarapu, S., Bavikadi, S., & Dinakarrao, S. M. P. (2024). Empowering Malware Detection Efficiency within Processing-in-Memory Architecture. Journal of Cybersecurity and Privacy, 4(2). DOI: 10.3390/jcp4020012

Körber, M., Kalysch, A., Massonne, W., & Benenson, Z. (2022). Usability of Antivirus Tools in a Threat Detection Scenario. In IFIP International Conference on ICT Systems Security and Privacy Protection (pp. 306-322). Cham: Springer International Publishing. DOI: 10.1007/978-3-031-07073-6_18

Kaspersky Labs. (2021). Cloud-based and AI-powered antivirus systems. Available at: https://www.kaspersky.com/enterprise-security/wiki-section/products/machine-learning-in-cybersecurity

Leka, C., Ntantogian, C., Karagiannis, S., Magkos, E., & Verykios, V. S. (2022). A comparative analysis of VirusTotal and desktop antivirus detection capabilities. 13th International Conference on Information, Intelligence, Systems & Applications (IISA), 1-6. DOI: 10.1109/IISA56318.2022.9904350

Limer, A., Abramovich, R., Devereux, G., Ziemniak, P., & Dubois, F. (2024). Automated ransomware detection using dynamic behavior trace profiling. TechRxiv Preprints. DOI:

10.36227/techrxiv.173030558.85237080

Moritaka, H., & Komuro, D. (2024). Enhanced ransomware detection using dual-layer random forest on opcode sequences. Journal of Information Security and Applications, 70 103347. DOI: 10.22541/au.172193050.02354794/v1

Parveen, K. (2024). Advanced Techniques of Malware Evasion and Bypass in the Age of Antivirus. International Journal for Electronic Crime Investigation, 8(3). DOI: 10.58936/ijeci.v8i3.205

Pérez-Sánchez, A., & Palacios, R. (2022). Evaluation of local security event management system vs. standard antivirus software. Applied Sciences, 12(3), 1076. DOI: 10.3390/app12031076

Pogonin, D., & Korkin, I. (2022). Microsoft Defender Will Be Defended: MemoryRanger Prevents Blinding Windows AV. IEEE Access, 10, 12345-12356. DOI: 10.1109/ACCESS.2022.3145678

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on cyber security. International Journal of scientific research and management, 9(12), 669-710. DOI: 10.18535/ijsrm/v9i12.ec01

Sharmeen, S., Ahmed, Y. A., Huda, S., Koçer, B. Ş., & Hassan, M. M. (2020). Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. IEEE Access, 8, 24522-24534. DOI: 10.1109/ACCESS.2020.2970656

Souri, A., & Hosseini, R. (2018). A state-of-the-art survey of malware detection approaches using data mining techniques. Human-centric Computing and Information Sciences, 8(1), 3. DOI: 10.1186/s13673-018-0125-x

Talukder, S. (2020). Tools and techniques for malware detection and analysis. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 1-15. DOI: 10.52306/0301012020

Usman, N., Usman, S., Khan, F., Jan, M. A., Sajid, A., Alazab, M., & Watters, P. (2021). Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics. Future Generation Computer Systems, 118, 124-141. DOI: 10.1016/j.future.2020.12.014

Wang, Q. (2020). Strategy of enterprise network security protection based on cloud computing. IOP Conference Series: Materials Science and Engineering, 750(1), 012234. DOI: 10.1088/1757-899X 750/1/012234