International Journal of Innovative Research in Computer Science and Technology (IJIRCST)
ISSN(Online): 2347-5552, Volume-13, Issue-2, March 2025
https:/doi.org/10.55524/ijircst.2025.13.2.3
Article ID IRP-1585, Pages 14-18
www.ijircst.org

Comparative Analysis of AI based Antivirus Software Programs Ensuring Cyber Security

Zahra Jabeen[1], Khusboo Mishra[2], and Binay Kumar Mishra[3]

[1] Department of Computer Science, Veer Kunwar Singh University, Ara, Bihar, India
[2, 3] University Department of Physics, Veer Kunwar Singh University, Ara, Bihar, India

Correspondence should be addressed to Zahra Jabeen; jabeen.zahra5@gmail.com

Received: 27 January 2025 Revised: 11 February 2025 Accepted: 25 February 2025

ABSTRACT- In today's digital arena security of the computer systems is one of the most important factors for users and businesses, as an attack on a system via the internet (cyber-attack) may cause heavy data loss and considerable harm to businesses. The increasing range of cyber-attacks has made traditional anti-virus scanners inefficient and are not fulfilling the desired need for protection. Hence, an advanced level of skill is required for the development of anti-attacking tools embedded with Artificial Intelligence to combat cyber threats. Modern warfare and international cybercrime have also increasingly involved cyber-attacks including targeted distribution attacks or highly networked spying, resulting in extremely dangerous malware attacks that were explicitly designed and released by nations to cause large-scale damage to organizations or infrastructure. Because of such evolving threats, more advanced tools for malware detection, prevention, and recovery are increasing in demand which would aim at defending computing networks from attack. This paper introduces a comparison between some of the best-rated artificial intelligence-embedded antivirus software programs so that a well-suited one could be used by users or enterprises accordingly. This report draws a basic understanding of the technological features provided by each of the software programs and also shows some evident drawbacks, if present. Meanwhile, it also points out some facts related to the use of AI in antiviruses and the scope of Artificial Intelligence in Cyber security.

KEYWORDS- Antivirus, Artificial Intelligence, Machine Learning, Deep Learning, Cyber security.

I. INTRODUCTION

Artificial Intelligence is the technology where computer systems have been trained to think, learn, and behave like humans to perform tasks like decision-making, problem-solving, or understanding natural language. Whether voice assistants or self-driving cars, AI has been transforming industries around the globe. This technology is among the ground breaking innovations that is determined to provide intelligent machines for the evolution of industries. Sparking endless possibilities, AI-driven security analytics has emerged as a transformative solution to analyze huge datasets to identify potential security threats. These security threats may include infection through worms, viruses, or malware and hacking through harmful software. Some of the possible problems that may occur after a virus/ worm infects a computer system are as follows [1]:

- Deletion or corruption of the files causes data loss.
- Making the entire system unusable by crashing it.
- Stealing personal identification data such as credit cards and numbers.
- Automatically sending spam emails from the computer
- Launching DDoS attacks against websites and other internet services.

Hacking via harmful software, including:

- Utility-like tools that produce malicious software by amalgamation of viruses, worms, and Trojans popularly known as constructors.
- Developers are using program libraries specifically designed for producing Malware.
- Encryption utilities are used to hide malicious software from antivirus software.
- Pranks interact with a computer to disturb the regular process.
- Misleading Programs fake their features about what they do to the system.
- Malware directly or indirectly harms local or networked computers.

Specific differences between AI-powered antivirus software and traditional antivirus software are shown below in table 1.

Table 1: Difference between AI-powered antivirus software and traditional antivirus software

FEATURE	AI-BASED	TRADITIONAL
DETECTION METHODOLOGY	Employs advanced machine learning algorithms to identify patterns and behaviors associated with malware, enabling it to detect previously unknown threats.	Typically relies on signature-based detection, which involves comparing files to a database of known malware signatures.
BEHAVIORAL ANALYSIS	Analyzes the behavior of software in real-time to identify potentially malicious activities, activates AI-based systems to detect zero-day threats and polymorphic malware.	Traditional mapping of historic data is performed.
ADAPTABILITY	Adapts and learns from new threats continuously, can update its algorithms and models based on evolving malware trends.	New patterns are added manually
FALSE POSITIVE REDUCTION	Distinguishes between legitimate software and malware, reducing false positives.	No such intelligence is found
AUTOMATION	Incorporates automation capabilities, allowing for faster response times to threats, automatically processes threat remediation and quarantine.	Need for manual intervention by security analysts
SCALABILIT	Handles large volumes of data and network traffic efficiently	Fails to ensure effective threat detection and response due to lack of predictive capabilities
PREDICTIVE CAPABILITIES	Predictive analytics to anticipate potential threats based on historical data and current trends.	No prediction could be performed

II. LITERATURE REVIEW

A. Few techniques to scan files for detecting Malware

- Behavioral Analysis- looks out for suspicious behavior that indicates new threats.
- Heuristic Analysis- identifies the potential malware while tracking code and behavior.
- Removal and quarantine techniques- first disable detected malware and then isolate it.
- Regular Updates ensure that the software can detect new threats effectively.
- Real-Time Protection prevents the spread of executed malware. See the below figure 1 here we are showing the key areas where AI can plays a vital role.

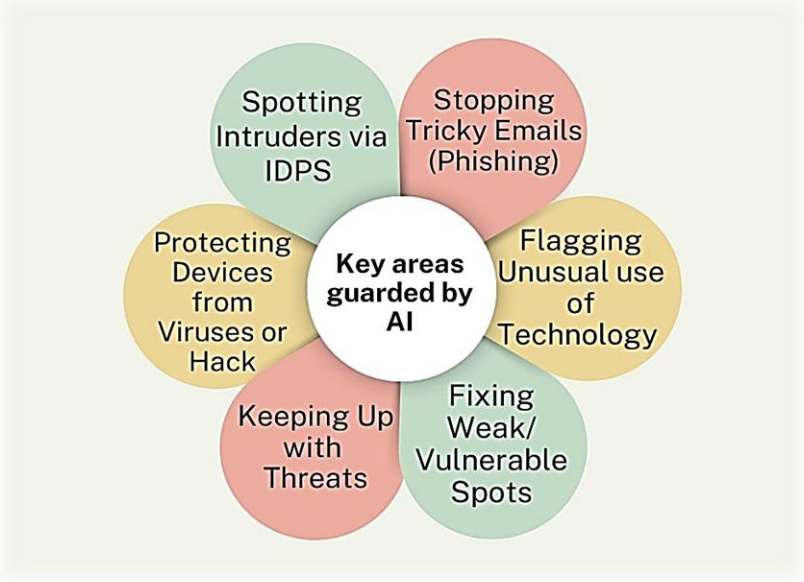

Figure 1: Key areas where AI plays a vital role in keeping us guarded online

B. Some reasons why we would not benefit from investing in an antivirus

- Ending up on suspicious websites- Websites that are not reliable enough are the primary source of numerous cyber threats that infect our devices. Premium antivirus software programs provide intrusive ads that block malicious sites and avoid any malware encounter.
- Having personalized business rules- As per the UK Cyber Security Breaches survey, in 2023, 32% of businesses and 24% of charities faced phishing attempts, breaches, or attacks. These numbers grow even higher for medium businesses (59%), large businesses (69%), and high-income charities earning £500,000 or more annually (56%) therefore it is important to have antivirus software to avoid any such losses [2].
- Frequent online shopping- A 2023 data from Statista reports that the United States had more than 270 million people buying stuff online which makes up over 81% of the whole US population. For putting out credit card details nearly every day, it is suggested to use an AI-encrypted and secure browser that ensures safe transactions.
- Sharing devices with kids- Parental control features, such as webcam blocking protects children even while parents are not at home. There are conditions where more than a few devices are connected to home Wi-Fi which must be protected by antivirus all of them at once, saving the hassle of catering to each separately.

Coding an Antivirus is very technical and hard, but here's just a simple draft of how your AV could work [3].

- The AV will start by first hashing the file and comparing the hash with a hash list in a database using MD5 (or SHA1, if you prefer).
- The AV scans through all the present files, including .dlls. Whenever a malware is found, it gets deleted.
- The scanner scans the startup folder and registry entry in all possible startup places and if found, deletes the registry and file.
- Search the local hard drive and delete malware if found.

III. METHODOLOGY

Antivirus software scans the device to detect known or unknown malicious threats and removes them. They must regularly update themselves so that they are capable of detecting newly emerged threats. One of the techniques like a Heuristic scan, detects unfamiliar malware software by analyzing the behaviour of the programs.

We conducted thorough hands-on tests on 25 antivirus tools to sort out the top 10 antivirus programs in 2024 to help the users select the one that fits their needs best(See table 2). Apart from our experiences, we have also used recommendations from various other organizations that provide security software efficiency [4] [5].

Table 2: Comparative analysis done on different Antivirus Software

S. No.	Antivirus	Operating System	Maximum devices covered	Advantages	Disadvantages
1.	Bitdefender Total Security	Windows, Mac, Android, iOS	10	• Strong defense against malware. • Configurable interface. • Safepay banking protection, multi-layered anti-ransomware, gaming and streaming modes, VPN. • Excels in real-time protection and deep system scanning.	• Scans can be slow. • VPN usage caps. • Not recommended for current infections.
2.	Norton 360 Select with LifeLock	Windows, Mac, Android, iOS options	5-10	• Identity theft protection. • Access to unlimited VPN. • Subscription tiers include features like Intelligent firewall, PC maintenance, bundled backup tool with online storage. • Smart Firewall, PC cloud backup, parental controls, and system optimization features. • VPN provides adequate security with AES-256 encryption and the OpenVPN or IKEv2 tunnelling protocols.	• Plans are expensive after the introductory period • Unreliable VPN kill switch. • Lacks file encryption and shredder.
3.	Avast One	Windows, Mac, Android, iOS options	Up to 30	• Excellent malware protection. • Amazing gamer mode. • Extra security tools including VPN, firewall, malicious URL blocker, and password manager.	• Sneaks in unnecessary extras. • Free VPN is limited. • Not a huge upgrade from the free version.

4.	McAfee+ Premium	Windows, Mac, iOS, Android	10	• Bundled VPN with unlimited usage. • Includes identity anti-theft tools VPN, spam filter, intelligent firewall, ID theft protection, ID Protection through McAfee Protection Centre website, enhanced system performance. • Offers an App Boost feature i.e., File Shredder.	• The Antivirus engine needs to work on macOS. • Entry-level product only covers one device. • Family plans are pretty expensive.
5.	F-Secure Total	Windows, Mac, Android, iOS	10	• Network protection. • Excellent malware blocking. • Remote and live support is available. • Network protections, remote support, VPN.	• Not the best for new users • Doesn't work on Chromebook
6.	Trend Micro Antivirus+ Security	Windows, Mac, Android, iOS	10	• Very clean interface. • Safe banking tools. • Capable URL blocking Ransomware monitoring, Pay Guard banking protection, high-quality URL blocking. • PC Health Checkup feature that works fast and finds unnecessary files and passwords for quick cleaning. • Trend Micro Password Manager can store passwords from information and even has a secure notes folder.	• Missing key features include rival offerings. • Some impact on system speed. • Limited configurability
7.	Avira Internet Security	Windows, Mac, Android, iOS, Chromebook	25	• Impressive anti-phishing and web protection. • Plenty of options to customize. • A stand-out free plan. • Proactive anti-ransomware, software updater, web protection. • Game Booster effectively stops Office from using any CPU percentage, optimizing unused apps to use 0% CPU. • VPN, a firewall, and a password manager. • Avira's Identity Assistant regularly scans the internet using an ongoing algorithm to check if your personal data has been exposed on the dark web.	• Slows down app launches and file downloads. • Lots of setup required. • Not the best option for mobile.
8.	ESET Internet Security	Windows, Mac, Android options, Chromebook options	5	• Easy to install. • Some good security add-ons include Multi-layered protection, user-friendly parental control, web access protection that detects and blocks scams and phishing sites, email client protection that scans incoming and outgoing emails, and antispam protection that detects and removes spam emails. • Anti-Theft feature monitors its usage and tracks its location using IP address localization.	• New threat detection reserved for premium users. • No iOS protection.
9.	Malwarebytes Premium	Windows, Mac, Android, iOS, Chromebook	5	• Stellar malware removal. • Real-time security status. • Malware removal tools like uninstall protection include exploit protection with online activities that will be confidential, and you'll gain protection from man-in-the-middle attacks while surfing the web on public hotspots.	• Some tools only available on Windows • VPN costs extra.
10.	Intego Mac Premium Bundle X9	Mac	5	• Specifically designed for Mac. • Good system cleaner. • Parental controls. • Network protection, system cleaner, backup scan caches, downloads, logs, and trash for unused files that take up unnecessary space.	• Separate downloads for each tool. • Not the best for mobile.

According to independent lab results of the Antivirus test and comparisons, most of the tested providers perform similarly. Norton and TotalAV excelled in our in-house tests, while ESET and McAfee scored perfectly in the field of protection, performance, and usability.

However, we must keep in mind certain factors while looking for an antivirus:

A. Performance

Reviews of performance tests should be used to compare how the antivirus software affects our system's speed and performance. It could be checked if it slows down the computer during scans or regular use with free software trials.

B. Features

Search for additional features in the antivirus software, such as firewall protection, email scanning, parental controls, and secure web browsing protection, and then choose the software that holds features aligning with our specific needs and preferences.

C. Reliability

Visit the official product website and check whether antivirus software provides regular updates for its virus definitions and database or not. It's also evident to check the reputation of antivirus software online which will ensure security against the latest threats and avoid concerns about data breaches maintaining user privacy.

D. Compatibility

Compatibility of antivirus software with operating systems (Windows, macOS, or Linux) or any other devices such as smartphones or tablets should be checked before purchasing.

E. Ease of use

A user-friendly interface provides for hassle-free protection and thus we must check on the trial version to see how easy the antivirus is to install, navigate, and use.

F. Security

Additional security features like a VPN, a password manager, etc could be added as they will provide an extra layer of security for your devices.

IV. LIMITATIONS AND CHALLENGES

Achieving success in the field of accuracy and reliability for malware detection is still one of the largest challenges faced in this new breed of malware detection algorithms [6] [7]. Even the most advanced AI-integrated antivirus models may still struggle to match the accuracy of traditional models. There is continuous research happening in machine learning system to achieve a high enough accuracy level making them trustworthy, reliably useful, and consistent in their detections.

V. CONCLUSION

As digitalization continues to proliferate and new technologies are introduced every day, cyber risk will inevitably grow. While we cannot fully prepare for various potential scenarios on how technology is and will influence and change our lives or become a potential venue to be exploited, the challenges pointed to herein are something we need to at least think about. In conclusion, AI-driven security analytics represent a paradigm shift in cyber security, offering organizations the ability to extract actionable insights from big data, proactively identify threats, and strengthen their defence posture in the face of evolving cyber risks. Therefore, it’s safe for us to say that by leveraging AI algorithms and machine learning techniques, antivirus software can swiftly identify and combat both known and previously unseen threats, enhancing overall cyber security.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] New Era Technology, "10 Common Causes of Data Loss, Prevention, and Data Recovery Tips and Tricks," 30 Aug 2023. Available from: https://www.neweratech.com/uk/blog/10-common-causes-of-data-loss/

[2] niBusinessInfo, "Impact of Cyber Attack on Your Business," Available from: https://www.nibusinessinfo.co.uk/content/impact-cyber-attack-your-business

[3] Lawrence Liu, "How can I code a simple antivirus software from scratch that uses AI to detect viruses?", 23 Dec 2017.

[4] Benedict Collins, "The Best Antivirus Software in 2024 for PC," TechRadar, 23 July 2024.

[5] Šarūnas Karbauskas, "Best Antivirus Software in 2024," Cybernews, 21 June 2024.

[6] Quickheal, "Antivirus Security and the Role of Artificial Intelligence (AI)," 29 May 2023.

[7] https://www.linknovate.com/affiliation/accenture-24095/all/?query=security%20and%20stability