IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁐ Peer-reviewed / Refereed journal ⁐ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12208

A Study on Artificial Intelligence Integrated Antivirus model to support Cyber Security

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

Research Scholar, Department of Computer Science, Veer Kunwar Singh University, Ara, Bihar, India[1]

Research Scholar, P.G Department of Physics, Veer Kunwar Singh University, Ara, Bihar, India[2]

Professor, P.G Department of Physics, Veer Kunwar Singh University, Ara, Bihar, India[3]

Abstract: The process of protecting networks, computers, mobile devices, servers, electronic systems and data from malicious attacks is called Cyber Security. It's also referred as Information Security (INFOSEC) or Information Assurance (IA) or System Security. In cyber world threats are constantly new, malevolent hackers are not going to give up anytime soon. As long as there are hackers, the cyber security will remain a trending technology. And to provide the strong need of cyber security professionals, the number of cyber security jobs is growing three times faster than other technical jobs. AI has enabled us to develop useful tools such as speech recognition (Siri), search engines (Google), and facial recognition software (Facebook) etc. With strong public-private partnerships and cross-pollination among industry, academia, and international partners, we can build an unshakeable cyber security foundation based on sensor-embedded systems, data, and AI-driven predictive analytics. According to Gartner, by 2025, 60% of organization will use cyber security risk as a primary determinant in conducting a third party transaction. This article shows the implementation of artificial intelligence on antivirus as both beneficial and detrimental.

Index Terms: Cyber Attacks, Cyber Security, Artificial Intelligence, Antivirus, Machine Learning

I. INTRODUCTION

This article guides a stepwise walkthrough of the use of artificial intelligence techniques and knowledge-intensive tools which would be vital in new offensive methods like dynamic installation of protected perimeters and integral crisis management and fully automated reactions to attacks in networks. According to Tech Republic, mid-sized companies receive over 200,000 alerts for cyber events each day, and a team of human experts cannot possibly address all of them. As a result, certain threats are likely to go unnoticed, leading to significant damage to network. Businesses wanting to grow in the digital world must look on Artificial Intelligence and other advanced technologies to bolster their cyber security defenses. Some principal artificial intelligence techniques applied in antivirus detection are proposed as heuristic technique, data mining, agent technique, artificial immune, and artificial neural network.

It is to be believed that it must promote the production of new artificial intelligence algorithm and improve the performance of existing antivirus detection system.

II.APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBER SECURITY

It is nearly the time where every product we use has artificial intelligence integrated with it. With newer technologies evolving every day the future of antivirus protection is exciting. There are advanced forms of malware like spyware, rootkits, worms, trojans, ransomware, etc. The need to harness AI and ML in cyber security is highlighted by all with its major benefits as mentioned below:

Automated attack vector processing: Artificial Intelligence can work on millions of vectors per second and also thwart nascent attacks by rapidly identifying novel patterns.

Zero-Trust Model Support: Diverse data sets without AI are simply not actionable or relevant because human behaviors are predictable. Artificial Intelligence helps in developing the complete threat analysis required to preserve a functional zero-trust model.

Threat Operations Management: Artificial intelligence can support cyber security teams by prioritizing warnings and incidents, automating the interpretation of attack signals and customising defenses in response to the pace and size of the attacker.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12208

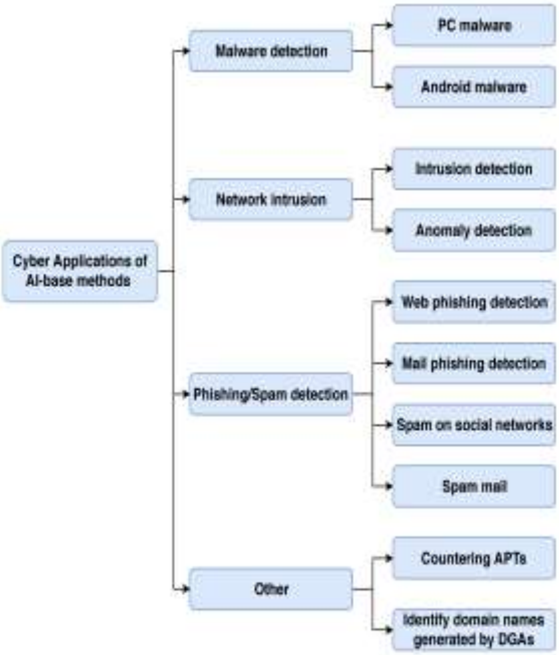

Figure 1: Main branches of cyber security applications adopting AI techniques

Use-cases of AI in cyber security

a) Many companies claim that their AI-based cyber security tool helps banks and their other financial organizations in identifying threats to security and adversaries while analyzing transactions to find weak security risks.

b) Another software has a smart antivirus program that utilizes Artificial Intelligence to find, stop, and foresee threats. This tool does not require virus signature updates, in contrast to typical antivirus software, but it will eventually learn to recognize harmful applications from beginning to end.

c) ML-AI backed software scrutinizes network traffic statistics in order to find out the baseline behavior of each device and user in the company. The software learns to identify a critical departure from the general user behavior and immediately instructs the organization of cyber hazards after getting input and other training datasets from subject matter experts.

Several antivirus software that are using artificial intelligence technology are as listed below:

1. Avast Antivirus – Cyber Capture is a core feature of the Avast security suite, specially targeting unknown malware and zero-days. When an unidentified suspicious file arrives into a system, CyberCapture activates and instantly isolates the host system. The suspicious file automatically gets uploaded to an Avast cloud server for data analysis. Later, the user gets a positive or negative notification in reference to the status of the file. At the same time, your data is getting fed back into the algorithms to define further and enhance our system security. Accompanied with the Behavior Shield tool, Avast Free Antivirus also keeps an eye on your installed applications and report for any new suspicious behavior. It’s also worth mentioning that we have VPN support with the SecureLine VPN, that anonymizes all our data online.

Main features of Avast include:

a. Blocks viruses and advanced malware
b. Detect malicious and fake website
c. Blocks remote access attacks
d. 30 days money-back guarantee
e. Compatible with Windows, Mac, and mobile systems

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 2, February 2025

DOI: 10.17148/IARJSET.2025.12208

2. **Bitdefender** – Bitdefender has almost perfect scores from AV-TEST and its top virus detection rate. This security solution shows an advanced anti-ransomware shield with Multi-layered ransomware protection. This antivirus unites effectiveness, functionality and simplicity. That's why, we get strong antivirus protection, along with file security and firewall, packed in a simple and user friendly package.

Key features include:

a. Web filtering technology
b. Advanced Threat Defense
c. Bitdefender Photon to save resources and improve the speed
d. Global Protective Network
e. Vulnerability assessment

3. **ESET Smart Security** - ESET uses multi-layered technologies to prevent infiltration by viruses, worms, spyware, adware, rootkits, Trojan horses and other threats. This antivirus has its own in-built machine learning engine that uses the combined power of a group of six classification algorithms and neural networks as such deep learning. This allows it to generate a consolidated output and help correctly label the incoming sample as malicious, clean or potentially unwanted

4. **BullGuard** - This one comes with features such as Identity Protection, Parental Control and Game Booster. The amount of characteristics offered even on the standard package is exceptional with Anti Phishing, Behavioral Engine and Vulnerability Scanner on top of all.

5. **Avira** - For malware analysis, it uses the coarse-to-fine strategy, through the complex techniques of supervised learning and exploring the data from clusters, and determines if data is malware or not. This complete antivirus tool comes with a shield for email and social network scams and clever ad-tracking functionality or cleaning features to erase your digital traces. You also benefit from free VPN protection that can secure sensitive information online and hide your online behaviors.

Its key feature includes:

a. Advanced AI and machine learning
b. Cross-platform compatibility
c. Real-time protection and updates
d. Light on the system's resources
e. Fast scanning

6. **Windows Defender** - This new AI-powered security system feature will start with its enterprise customers, but eventually filter down to Windows 10 systems for regular consumers. Windows Defender is regularly updating itself and is now one of the top enterprise and consumer security solutions. It is very useful as a part of the safekeeping platform as it can analyze threats to network. It can manage a big amount of information and based on that data, it can create threat models and prevent possibility to any damage. It can also identify a threat before-hand.

7. **Deep Instinct D-Client** - Deep Instinct uses a machine learning technique known as deep learning, to detect "any file before it is accessed or executed" on your system. The Deep Instinct D-Client makes use of static file analysis in association with a threat prediction model that allows it to eliminate malware and many other system threats autonomously.

8. **Cylance Protect** - Cylance is presented as the first full-fledged artificial intelligence-backed antivirus. Cylance is majorly marketed for business users, as its client-oriented protection. The administrative console is entirely cloud-based, but the decisions are made at the endpoint. Cylance Smart Antivirus depends entirely on Machine Learning and Artificial Intelligence to distinguish malware from legitimate data which results in an antivirus that doesn't bog the system down by continuously scanning and analyzing files. Cylance Smart Antivirus waits until the moment of execution and instantly kills the threat without human intervention.

DOI: 10.17148/IARJSET.2025.12208

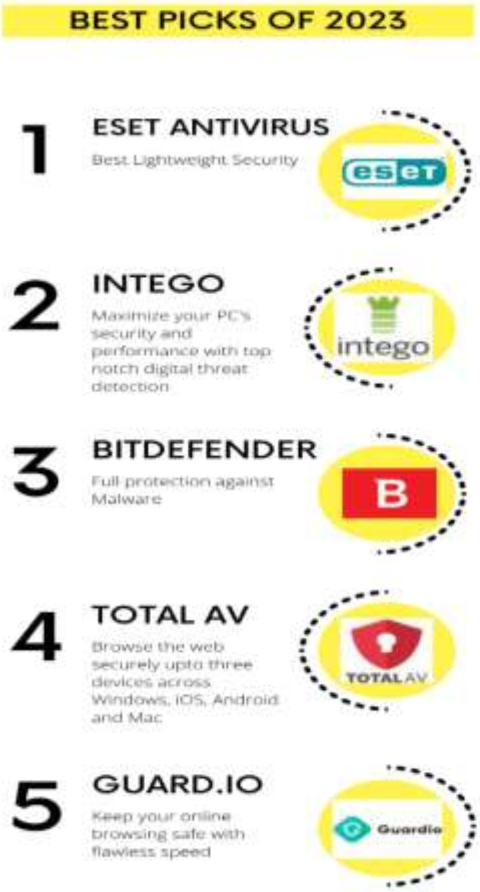
BEST PICKS OF 2023
1
ESET ANTIVIRUS
Best Lightweight Security
eset
2
INTEGO
Maximize your PC's security and performance with top notch digital threat detection
intego
3
BITDEFENDER
Full protection against Malware
B
4
TOTAL AV
Browse the web securely upto three devices across Windows, iOS, Android and Mac
TOTAL AV
5
GUARD.IO
Keep your online browsing safe with flawless speed
Guardio

Figure 2: Best rated Artificial Intelligence Integrated Anti-Virus

III. METHODS

To understand what the baseline of security is for a given system, Artificial Intelligence integrated antivirus leverage sophisticated mathematical algorithms associated with the data from other deployments. Apart from this, they also learn how to react to files that step outside that window of normal functionality. AI aims in producing a new type of intelligent automation that responds like human intelligence. To meet this goal, machines need to learn via currently three major types of learning algorithms as listed below-

1) Supervised learning: This learning technique requires a training process with a large set of data that has been previously labeled. These learning algorithms are often used as a classification mechanism or a regression mechanism.

2) Unsupervised learning: In contrast to supervised learning, unsupervised learning algorithms use unlabeled training datasets. This approach is used to reduce dimensionality, cluster data or estimate density.

3) Reinforcement learning: Reinforcement learning is a type of learning algorithm that learns the best actions based on rewards or punishment. This type of learning is useful for situations where data is not given or limited.

Bio-inspired computation is a branch of AI which is a collection of intelligent algorithms and methods that adopt characteristics and bio-inspired behaviors and to solve a wide range of complex academic and real domain problems. Among many biological-inspired methods, the following techniques are most commonly used in the cyber security domain:

DOI: 10.17148/IARJSET.2025.12208

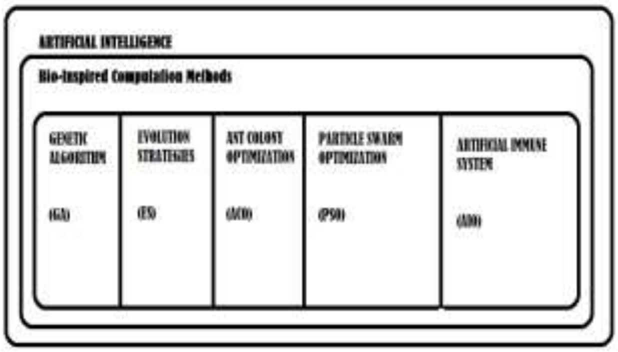
ARTIFICIAL INTELLIGENCE
Bio-inspired Computation Methods
GENETIC ALGORITHM (GA)
EVOLUTION STRATEGIES (ES)
ANT COLONY OPTIMIZATION (ACO)
PARTICLE SWARM OPTIMIZATION (PSO)
ARTIFICIAL IMMUNE SYSTEM (AIS)

Figure 3: Bio-inspired computation methods used in AI

IV. RESEARCH FINDING

According to experts, the sphere that requires AI's help desperately is Internet security. In that sense, the big players in the antivirus industry are steadily turning to this new technology.

The AI-based antivirus can improve its functionality based on its experience. Since artificial intelligence itself is a young technology, its implementation in modern antivirus solutions is still in the early stage. Using open-source antivirus will benefit the requirement of transparent security. These antivirus software tools can be used for business requirements from organizations or personal security needs. Many big antivirus companies offer free versions of their main product with basic but highly valuable features. According to Deloitte insights

a. The global market for Cyber AI technology and tools is expected to grow by US$19 billion between 2021 and 2025
b. One estimate says Cybercriminals will be able to choose from a growing number of network-connected physical assets i.e. 29.3 billion by 2023 while seeking a soft attack vector
c. At The Commonwealth Cyber Initiatives at Virginia Tech and Deloitte, researchers are collaborating to understand 5G network security design and implementation, and working to identify low-level signal jamming by implementing an AI-based interference scheme and machine learning models before it brings down the network.

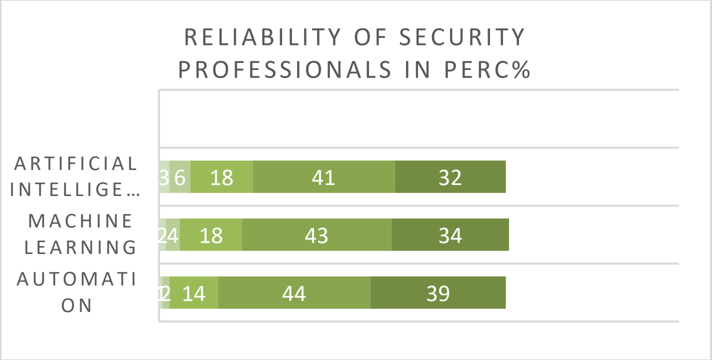

Figure 4: Organizations rely heavily on automation, machine learning, and Artificial Intelligence (Cisco 2018 Security Capabilities Benchmark Study)

V. CONCLUSION

It could be difficult to know where to begin when it comes to protecting your institution from cybercrime. There is so much information out there that it can become overwhelming, especially when the information is conflicting. AI-based antivirus software makes decisions based on its experiences. It is an effective part of the safekeeping platform as it can use reason to analyze threats to network. It can manage a huge amount of information and based on its data, it can create threat models, prevent possible damage and also identify a threat long before it happens.

Despite potential downsides, AI will drive cyber security forward and improve organizations' security posture.

Therefore, being cyber Smart is the need of the hour. So while we must protect ourselves, it’s going to take all of us to really protect the system we all rely on.

DECLARATION

Decalarion	Suggestions
Funding/ Grants/ Financial Support	No, I did not receive it.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	All authors have equal participation in this article.

BIOGRAPHY

Zahra Jabeen is a Research Scholar in the University Department of Computer Science from Veer Kunwar Singh University, Ara, Bihar, India. Her work, published in renowned Scopus and UGC journals, has generated critical discourse and earned prestigious accolades. She has completed her Bachelor of Technology (B.Tech) and Master in Technology (M.Tech) in Computer Science & Engineering. Jabeen.zahra5@gmail.com

Khushboo Mishra is a Research Scholar in the P.G Department of Physics from Veer Kunwar Singh University, Ara, Bihar, India. She is determined to bring some positive advancements in the society with research findings in her work.
kmishra.j94@gmail.com

Binay Kumar Mishra is working as a Professor in P.G Department of Physics, Veer Kunwar Singh University, Ara, Bihar, India. He has qualified in MS. c., Ph.D , Physics with specialisation in Plasma Physics, Nano Flow and IoT. He has an educational experience of more than 29 years.
drmishrabinay@gmail.com

REFERENCES

[1]. https://towardsdatascience.com/five-hypotheses-as-to-why-artificial-intelligence-and-machine-learning-projects-fail-7c6b2c456d41
[2]. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf
[3]. https://www.engati.com/blog/ai-for-cybersecurity#:~:text=AI%20eliminates%20time%2Dconsuming%20tasks,on%20more%20critical%20security%20tasks.
[4]. https://www.mdpi.com/2073-8994/12/3/410
[5]. https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security
[6]. https://www.google.com/search?q=scope+of+AI+in+cyber+security&oq=scope+of+AI+in+cyber+security&aqs=chrome..69i57j0i22i30j0i390i650l3.8326j0j7&sourceid=chrome&ie=UTF-8
[7]. https://www.engati.com/blog/ai-for-cybersecurity
[8]. https://windowsreport.com/artificial-intelligence-antivirus-windows-10/