DOI https://doi.org/10.36719/3104-4735/2/26-29

Huseyn Gasimov
Nakhchivan State University
PhD in Techniques
https://orcid.org/0000-0002-3714-875X
huseynqasimov@ndu.edu.az
Rugayyakhanim Garibzada
Nakhchivan State University
Master's student
https://orcid.org/0009-0001-4962-918X
ruqeyyexanim202027@icloud

Deep Learning versus Traditional Antivirus Software

Abstract

Cybersecurity has become increasingly complex, with traditional antivirus software struggling to keep up with modern threats such as zero-day exploits and advanced persistent threats (APTs). While traditional methods, including signature-based detection and heuristic analysis, remain effective against known malware, they fall short in detecting new or sophisticated attacks. The rapid evolution of cyberattacks, as well as the emergence of polymorphic and metamorphic malware, severely reduces the effectiveness of traditional defense methods. Because this type of malware changes its code structure with each execution, it easily manages to evade signature-based systems by confusing them. On the other hand, deep learning-based security systems leverage artificial intelligence to analyze patterns and behaviors, providing superior detection of previously unseen threats. These systems analyze large volumes of telemetry data, monitor behavioral changes in real time, and identify subtle patterns that traditional methods cannot detect. It is precisely these capabilities that make them an indispensable component in proactive defense strategies. However, deep learning systems require more computational resources and are vulnerable to adversarial attacks. A hybrid approach that combines traditional antivirus methods with AI-driven solutions offers a promising strategy to enhance cybersecurity defenses, providing comprehensive protection against a wider range of cyber threats.

Keywords: *cybersecurity, deep learning, antivirus software, machine learning, threat detection*

Introduction

Cybersecurity threats have evolved significantly over the years, with cybercriminals using sophisticated methods to bypass traditional defense mechanisms. Conventional antivirus software primarily relies on signature-based detection, where a file's attributes are compared to a predefined database of malware signatures. Malware developers often focus on information niches with a large number of users (Berrios, 2025, p. 8). Malware detection methods are divided into three types: static, dynamic and hybrid (Bensaoud, 2024, p. 4). In addition, heuristic analysis is used to detect suspicious behavior that is indicative of malware, even if the specific threat has not been previously identified. However, because both signatures and heuristic approaches are based on static characteristics, they cannot fully encompass the dynamic and changing nature of cyberattacks, and are consequently easily evaded by attackers. Despite these capabilities, traditional antivirus solutions struggle to combat modern threats such as zero-day exploits, polymorphic malware, and advanced persistent threats (APTs). Now malware uses clever tactics to avoid antivirus protection (Zakaria, 2025). These sophisticated forms of cyberattacks are constantly evolving, making it difficult for signature-based antivirus software to keep up. In addition, the increasing volume of new malware samples being created every day further exacerbates the limitations of traditional methods.

Because polymorphic and metamorphic malware can automatically change its code, traditional antivirus systems have difficulty distinguishing the different variants of the same malware, which significantly reduces the detection rate of threats. In contrast, deep learning-based security systems use artificial neural networks (ANNs) to dynamically analyze and classify malware. Unlike signature-based antivirus software, deep learning models do not rely solely on predefined patterns. Instead, they are trained on a large database of good and malicious code, allowing them to recognize complex patterns and behaviors associated with cyberthreats. This capability allows deep learning systems to identify and mitigate new and previously unknown attacks without requiring frequent updates to the malware signature database (Patel, 2022; Zhang, 2023).

Traditional antivirus software. Traditional antivirus software uses a combination of signature-based detection, heuristic analysis, and behavioral monitoring to identify and neutralize malware threats. Signature-based detection works by scanning files and processes against a database of known malware signatures. If a match is found, the antivirus software blocks or quarantines the threat. While this method is effective against known malware, it struggles to detect new and modified threats that have not yet been cataloged (Anderson, 2020). Many antivirus programs incorporate heuristic analysis to increase their detection capabilities. This approach examines file attributes, code structure, and runtime behavior to identify potentially malicious activities. While heuristic analysis provides a degree of protection against unknown threats, it is prone to false positives, where legitimate files may be flagged as malicious. Another common feature in traditional antivirus solutions is sandboxing, a technique that executes suspicious files in an isolated environment to observe their behavior before allowing them to run on the system. While effective, sandboxing can be resource-intensive and slow, limiting its practical use in real-time threat detection (Bishop, 2003).

Deep Learning-Based Security Systems. Deep learning improves cybersecurity by using artificial intelligence to analyze large amounts of data and identify malicious patterns. Unlike traditional antivirus solutions that rely on predefined signatures, deep learning models use neural networks to detect anomalies and suspicious behavior. These models are trained on a large database containing a variety of malicious and malware samples, allowing them to recognize previously unseen threats based on their properties and behaviors (Patel, 2022). Deep learning-based security systems use techniques such as behavioral analysis, anomaly detection, and real-time monitoring. Behavioral analysis involves studying the actions of files and programs to determine whether they exhibit malicious intent. Anomaly detection focuses on identifying deviations from normal system behavior that could indicate a cyberattack. These techniques allow deep learning models to adapt and improve over time, making them more effective at identifying complex threats than traditional antivirus software. These systems can also analyze large datasets in real time by automating behavioral model analysis, detecting the execution of suspicious activities in advance, and minimizing the spread of attacks. Because deep learning models analyze behavior rather than relying on known signatures, they can identify suspicious activity even without prior knowledge of a specific malware strain. Deep learning models also enable us to learn from examples of polymorphic and metamorphic malware to predict future attacks and create adaptive defense strategies. However, deep learning-based security systems are not without their challenges. Training and deploying deep learning models require significant computational resources, making them more demanding than traditional antivirus software. In addition, adversarial attacks, in which cybercriminals manipulate input data to trick AI models, are a growing concern in AI-based cybersecurity (Zhang, 2020).

Traditional Antivirus and Deep Learning Security. Traditional antivirus software and deep learning-based security systems each have their strengths and weaknesses. Traditional antivirus solutions are lightweight, reliable, and effective against known malware. They demonstrate high compatibility with common operating systems and applications and have a minimal impact on system resources, making them advantageous for small and medium-sized enterprises.

However, they require frequent updates and struggle to combat new and sophisticated threats. In particular, zero-day attacks, polymorphic malware, and advanced persistent threats (APTs) severely reduce the effectiveness of traditional antivirus software, as these attacks bypass known signature patterns from the outset to target the system (Chen, 2021, pp. 101-119).

On the other hand, deep learning-based security systems offer superior detection of zero-day threats, adaptability, and improved accuracy in identifying malicious activities. By analyzing large datasets, these systems model behavioral patterns, detect suspicious activities in advance, and can block previously unseen attacks. The adaptive learning capability of artificial intelligence enhances proactive defense against threats (Li, Zhao, 2020).

However, they require higher computing resources and expertise to implement effectively. The construction and training of deep learning models require powerful GPU and CPU resources, and expert knowledge in cybersecurity and the ethical use of data is also important for the models to function properly.

Emerging Threats and the Role of Hybrid Defense Models. As cyberthreats continue to evolve, attackers are increasingly using machine learning (ML) and artificial intelligence (AI) to circumvent traditional security mechanisms. For example, polymorphic malware can dynamically change its code and appearance, making it difficult to identify signature-based detection systems. Polymorphic malware generates a different code structure with each new execution, which delays detection by traditional antivirus signatures and also reduces the system's level of protection (Kazimov, 2020, pp. 45-47). In addition, AI-driven attacks can mimic human-like behavior, which can evade traditional heuristic and behavioral detection methods. AI-powered bots can mimic human behavior, including nuances such as keyboard rhythm and browser activity, which causes traditional detection systems to be fooled. These developments highlight the importance of adopting advanced security models such as deep learning to stay ahead of cybercriminals. Hybrid defense models that combine AI and traditional antivirus methods are becoming more relevant in this context. Deep learning models play a critical role in proactive security by identifying subtle patterns in large datasets, enabling the detection of previously unseen attacks (Hasanov, 2021, pp. 112-115). These models leverage the strengths of both approaches to create a more robust defense. AI can detect new and sophisticated attacks by analyzing large malware datasets, while traditional methods provide basic defense against known threats. In addition, such systems can leverage collaborative intelligence, where threat intelligence can be integrated from multiple sources to improve overall detection accuracy and response speed. Hybrid systems provide initial defense with signature-based filtering, while AI performs deeper behavioral analysis and minimizes defense gaps (Gasimova, 2020, pp. 59-63).

The Future of Cybersecurity: Integrating Traditional and AI-Based Approaches. The future of cybersecurity will likely involve a hybrid approach that combines traditional antivirus methods with AI-driven threat detection. Many cybersecurity firms are developing integrated solutions that use both signature-based detection for known threats and deep learning models to identify emerging threats.

This combination provides comprehensive protection while minimizing the limitations of each individual approach. As cyber threats continue to evolve, organizations and individuals must adopt multi-layered security strategies. By integrating deep learning alongside traditional antivirus solutions, cybersecurity defenses can be more robust, adaptive, and effective in mitigating cyber risks. (Aliyev, 2019, pp. 78-81).

Conclusion

In the modern era, cyber threats are becoming increasingly complex, and traditional antivirus software struggles to combat these threats on its own. Zero-day attacks, polymorphic and metamorphic malware, as well as advanced persistent threats (APTs), significantly reduce the effectiveness of traditional signature and heuristic-based systems.

On the other hand, deep learning and artificial intelligence-based security systems can detect unknown and complex attacks, offering proactive defense. They can analyze behavioral patterns in real time. However, these technologies require higher computational resources and expert knowledge, and they still have certain shortcomings against adversarial attacks. Therefore, hybrid defense models that combine traditional antivirus methods with AI-based approaches are considered a promising and effective strategy. A hybrid approach provides both rapid defense against known threats and the ability to detect new and advanced attacks through deep learning.

Consequently, the future of cybersecurity will be based on multi-layered and integrative approaches. Organizations and individual users will create more robust, adaptive, and agile defense strategies by combining both traditional antivirus solutions and AI-based models. This approach provides comprehensive defense against cyber threats and serves as an effective tool against future, increasing cyberattacks. It minimizes defense gaps and reduces vulnerabilities.

References

1. Aliyev, R. (2019). *Artificial intelligence and cyber threats*. Law Publishing.
2. Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.).* Wiley.
3. Bensaoud, A., Kalita, J., & Bensaoud, M. (2024). A survey of malware detection using deep learning. *Machine Learning with Applications, 16*, 100546. https://doi.org/ *and science*. Addison-Wesley.10.1016/j.mlwa.2024.100546
4. Berrios, S., Leiva, D., Olivares, B., Allende-Cid, H., & Hermosilla, P. (2025). Systematic Review: Malware Detection and Classification in Cybersecurity. *Applied Sciences, 15*(14), 7747. https://doi.org/10.3390/app15147747
5. Bishop, M. (2003). *Computer Security: Art and Science*. Addison-Wesley.
6. Chen, L., Wong, P., & Tan, H. (2021). Zero-day and advanced persistent threats: Challenges for conventional antivirus systems. *Journal of Information Security*, *10*(4), 101–119.
7. García, M., Pérez, J., & Sánchez, D. (2021). Resource requirements for AI-based security systems: A practical approach. *Computers & Security*, *100*, 102092.
8. Gasimova, S. (2020). *Hybrid Security Systems: Theoretical and Practical Approaches*. Science.
9. Hasanov, F. (2021). *Deep learning-based security models*. Science and Education.
10. Kazimov, Q. (2020). *Cyber security and modern attacks*. Science.
11. Li, X., & Zhao, Y. (2020). *Deep learning in cybersecurity: Enhancing threat detection and prediction*.
12. Mammadov, T. (2018). *Threat intelligence and cybersecurity management*. Low Publishing.
13. Patel, S., & Patel, D. (2022). Cybersecurity threats and their mitigation approaches using machine learning. *Journal of Cybersecurity and Privacy, 2*(3), Article 27. MDPI. https://www.mdpi.com/2624-800X/2/3/27
14. Zakaria, M., Hussein, S. (2025). Detection and Analysis of Obfuscated File-less Malware Using Advanced Machine Learning Techniques. *Proceedings of the 2025 IEEE International Conference on Machine Intelligence and Smart Innovation (ICMISI).* https://www.webofscience.com/wos/?app=wos&mode=Nextgen&path=%2Fwos%2Fwoscc%2Ffullrecord%2FWOS%3A001583425500065&IsProductCode=Yes&Init=Yes&DestApp=UA&Func=Frame&action=transfer&SrcApp=CR&locale=en&SID=EUW1ED0C283VDZDWwJtgNTQcjcrsq
15. Zhang, L., & Wang, H. (2023). *A new hybrid ensemble learning-based malware detection technique. In Advances in Intelligent Systems and Computing, Volume*. Springer. https://link.springer.com/chapter/10.1007/978-3-031-75957-4_20
16. Zhang, Y., Wang, X., & Zhang, Y. (2020). A hybrid deep learning model for malicious behavior detection. *Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Engineering (ICAICE).* https://ieeexplore.ieee.org/abstract/document/9123055

Received: 11.08.2025
Approved: 09.12.2025