<Conference abbreviation>
<Conference Series name> <Volume number and Year> <DOI Number>

Multi-Layer Malware Défense- A Survey: From Metaheuristic-Driven Detection to Adversarial Robust Operations

Doaa Sami Khafaga[1], Abdullah El-Baz[2], Amal H. Alharbi[3], Amel Ali Alhussan[4]

El-Sayed M. El-kenawy[5,6], Marwa M. Eid[7,8]

[1] Department of Computer Sciences College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University Riyadh, Saudi Arabia dskhafga@pnu.edu.sa

[2]Delta Higher Institute of Engineering and Technology Department for Civil Engineering, Mansoura 35511, Egypt ch2400169@dhiet.edu.eg

[3]Department of Computer Sciences College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University Riyadh, Saudi Arabia ahalharbi@pnu.edu.sa

[4]Department of Computer Sciences College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University Riyadh, Saudi Arabia aaalhussan@pnu.edu.sa

[5]Delta Higher Institute of Engineering and Technology Department for Communications and Electronics Mansoura 35511, Egypt

[6]Applied Science Research Center Applied Science Private University Amman, Jordan, skenawy@ieee.org

[7]Faculty of Artificial Intelligence Delta University for Science & Technology Mansoura 35111, Egypt

[8]Jadara University Research Center Jadara University, Jordan mmm@ieee.org

Abstract.

This study reviews methodologies spanning three major categories: detection, hybrid and quarantine, and resilience against ad- versarial threats. Detection-oriented systems demonstrate the capacity of classical and deep learning models to classify ma- licious activity across domains such as Android, Windows, and cloud infrastructures. Hybrid approaches extend these efforts by integrating static and dynamic analysis, anomaly and misuse detection, and diverse feature sets, ensuring both accuracy and operational safety through containment mechanisms. Resilience- focused research advances this paradigm further by addressing adversarial evasion and emphasizing adaptability, scalability, and continuity of protection. Collectively, these categories re- veal a trajectory from narrow classification accuracy toward holistic defense ecosystems capable of anticipating, mitigating, and recovering from threats. Despite advances, challenges re- main in interpretability, resource efficiency, and robustness to adversarial manipulation. Addressing these gaps will require lightweight architectures, explainable models, and collaborative defense frameworks.

Keywords. Malware detection, Hybrid analysis, Adversarial resilience, Machine learning, Cybersecurity.

1. INTRODUCTION

Traditional detection techniques based on static signatures or simple heuristics are insufficient, as modern malware variants rapidly adapt their signatures and behavioral patterns. These algorithms, in- spired by natural and evolutionary processes, provide strong capabilities in complex search spaces, excelling in feature selection, parameter tuning, and ensemble optimization [1]. In malware detection, feature selection plays a vital role by isolating discriminative attributes, reducing computational costs, and mitigating the curse of dimensionality [2]. The urgency of robust malware detection is intensified in IoT- enabled systems such as smart manufacturing, healthcare, and maritime transport. While IoT improves efficiency, it also increases vulnerability. Research demonstrates that quantum-inspired optimization, combined with neural networks, can achieve high accuracy and detect both known threats and zero- day exploits. Similarly, the Android ecosystem remains a significant target for malware due to its open architecture and vast user base. Hybrid metaheuristic approaches—combining Parti- cle Swarm Optimization (PSO), Genetic Algorithms (GA), and Ant Colony Optimization (ACO)—improve feature selection and, when integrated with ensemble models, enhance detection accuracy and scalability [3].

Metaheuristics have also proven effective in packet-level analysis for general-purpose malicious traffic detection, striking a balance between accuracy and real- time efficiency. Bio-inspired methods, such as Harris Hawks Optimization (HHO), mimic cooperative hunting strategies to escape local optima and enhance the robustness of classifiers. Similarly, Cuckoo Search efficiently selects optimal feature subsets, especially when combined with rough set theory [4] [5]. Systems that utilize ensembles are another development, leveraging a combination of classifiers optimized through metaheuristics to enhance diversity, accuracy, and adaptability to evolving malware strains.

2. LITERATURE REVIEW

The methodological landscape of malware detection research has undergone a profound transformation in the past two decades, evolving from early heuristic-based scanning procedures into a highly sophisticated domain that integrates machine learning, deep learning, metaheuristics, and hybrid computational strategies. In essence, it maps the intellectual and practical contours of the field by systematically cataloging how researchers have designed, implemented, and evaluated malware detection mechanisms across diverse computational environments and threat models [6]. The Harris Hawks Optimization, are employed to prioritize the most discriminative attributes, thereby improving both performance and computational efficiency [7]. In contrast, recurrent architectures, such as gated recurrent units and long short-term memory networks, have excelled at modeling sequential dependencies in program execution traces. These neural approaches achieved superior accuracy compared to traditional classifiers, especially when trained on large datasets. However, they also introduced challenges: their training required significant computational resources, their deployment consumed energy and memory, and their internal decision-making processes were opaque to human analysts [8].

Behavioral systems provide strong resilience against code obfuscation, as the underlying malicious intent typically manifests during execution regardless of superficial modifications. However, dynamic analysis is resource-intensive and susceptible to evasion techniques, such as malware delaying malicious activity until after analysis is complete.

Despite these challenges, behavioral detection remains a critical tool in identifying sophisticated threats. [9] The Android ecosystem became a focal point for many detection methodologies. As the most widely used mobile operating system, Android has attracted significant attention from malware developers and, consequently, from the research community. This dual emphasis on anomaly and misuse detection within distributed infrastruc- tures highlighted the adaptability of detection-oriented ap- proaches to diverse computing environments. [10] Specialized threats also inspired new directions of detection research. For example, cryptojacking malware, which steals computational resources to mine cryptocurrency, requires detection algo- rithms to be sensitive to resource usage patterns and fine- grained anomalies in system performance.. These examples reveal how detection-based methodologies can be customized to new attack vectors without compromising the principles on which they are based, namely observation and classification.

3. DISCUSSION

The evolution of malware detection highlights a trajectory from isolated classification systems to integrated and resilient defense ecosystems. Early detection-oriented approaches, cen- tered on classification accuracy, relied on feature engineering and deep learning to identify malware across various domains, including Android, Windows, and cloud infrastructures. While these systems established the feasibility of reliable detection, their focus on accuracy alone exposed limitations in adaptabil- ity, interpretability, and robustness against evasive strategies. Hybrid and quarantine-oriented frameworks emerged as a response, combining static and dynamic analysis, anomaly and misuse detection, and diverse feature sets. These frameworks not only improved accuracy and resilience but also introduced containment mechanisms that safeguarded systems even under uncertain conditions, thereby bridging the gap between the- oretical performance and real-world applicability. The most mature stage of this evolution is characterized by defense strategies emphasizing adversarial robustness and resilience. These approaches incorporate adversarial training, ensemble models, distributed architectures, and self-healing mechanisms to withstand and recover from sophisticated attacks. This shift reframes malware detection from a static endpoint to a continuous, adaptive defense cycle. Comparative reflection across detection, hybrid, and resilience paradigms highlights three themes: the growing need for integration, the progres- sion in scope from recognition to operational response and long-term resilience, and the critical role of adaptability in countering dynamic threats. Despite such developments, issues such as the absence of interpretability in deep models, resource limitations in IoT and mobile settings, operational risks of false positives, and adversarial machine learning threats remain. Solving these problems will take center stage in the the creation of sustainable, trustworthy, and future-proof malware defense mechanisms.

4. CONCLUSION

Malware defense has also undergone a shift in perspective, no longer relying solely on accurate detection but instead on a more holistic, combined approach to detection, containment, and resilience that is mutually reinforcing. Detection-based systems form the basis of this approach, as they offer identifi- cation capabilities for malicious patterns. Hybrid frameworks build upon this foundation with operational protection and real-world deployment plans. Resistance-based designs also incorporate flexibility and resiliency, allowing systems to resist adversarial manipulation and maintain continuity. Taken together, these techniques signify the evolution of malware study into a holistic approach to security,

one that focuses not only on threat identification but also prioritizes operational trust, stability, and recovery capabilities. This development underscores the importance of malware protection being multi- layered, dynamically adjustable, and scalable, as the tactics of attackers continually evolve with new methods. In the future, various challenges will persist, including the trade-off between efficiency and robustness, false positives, interpretability, and the unique constraints of the IoT and mobile environments. The non-interpretability of deep learning networks and the increasing prevalence of adversarial attacks are further indi- cators of the need for innovation.

REFERENCES

[1] Ahmed El-Sayed Saqr, Mohamed S Saraya, and El-Sayed M El- Kenawy. Enhancing co2 emissions prediction for electric vehicles using greylag goose optimization and machine learning. Scientific Reports, 15(1):16612, 2025.

[2] El-Sayed M El-Kenawy, Abdelhameed Ibrahim, Amel Ali Alhussan, Doaa Sami Khafaga, Ayman EM Ahmed, and Marwa M Eid. Smart city electricity load forecasting using greylag goose optimization-enhanced time series analysis. Arabian Journal for Science and Engineering, pages 1–19, 2025.

[3] R. Kumar, Vevekanandam, and R. Dey, "IoT-enabled bioimpedance and thermal imaging system for non-destructive fruit maturity assessment," International Journal of Vegetable Science, pp. 1–23, 2025, doi: 10.1080/19315260.2025.2574898.

[4] El-Sayed M Elkenawy, Amel Ali Alhussan, Marwa M Eid, and Ab- delhameed Ibrahim. Rainfall classification and forecasting based on a novel voting adaptive dynamic optimization algorithm. Frontiers in Environmental Science, 12:1417664, 2024.

[5] Amel Ali Alhussan, El-Sayed M. El-kenawy, Doaa Sami Khafaga, Amal H. Alharbi, and Marwa M. Eid. Groundwater resource prediction and management using comment feedback optimization algorithm for deep learning. IEEE Access, pages 1–1, 2025.

[6] Y. K. Shejwal, A. J. Hati, J. U. Kidav, A. K. Singh, and R. Kumar, "Neural network-based classification of beamforming matrices," International Journal of Satellite Communications and Networking, 2025, doi: 10.1002/sat.70002.

[7] Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, and Patrick McDaniel. Adversarial examples for malware detection. In Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS), pages 62–79. Springer, 2017.

[8] R. Kumar, R. K. Ratnesh, R. K. Chauhan, A. Kumar, M. K. Singla, and R. Gupta, "Non-invasive bio-impedance imaging and sensing for medical diagnostics and industrial applications," Journal of The Electrochemical Society, 2024.

[9] Tibra Alsmadi and Nour Alqudah. A survey on malware detection techniques. In 2021 international conference on information technology (ICIT), pages 371–376. IEEE, 2021.

[10] J. Ahyoev, P. K. Pandey, R. Kumar, M. Singla, S. Kokin, and M. Safaraliev, "Automated power factor correction through microcontroller in energy sector," Przegląd Elektrotechniczny, vol. 2024, no. 10, pp. 69–72, 2024, doi: 10.15199/48.2024.10.12.