pISSN:2349-5707 Volume:12, Issue 09, September-2025 eISSN:2349-5715

Dynamic Behavioral Intelligence for Predictive Malware Detection in Smart Healthcare Cyber Physical Systems: An Adversarially Robust Machine Learning Framework

Dr. Matthias Vogel
Department of Informatics, University of Zurich, Switzerland

ABSTRACT: The rapid integration of smart healthcare devices into clinical infrastructures has transformed patient monitoring, diagnostics, and therapeutic interventions. However, the convergence of embedded systems, wireless communication, cloud computing, and artificial intelligence has simultaneously expanded the cyber attack surface, exposing healthcare cyber physical systems to sophisticated and adaptive malware campaigns. Traditional signature based and static analysis mechanisms are increasingly inadequate against polymorphic, obfuscated, and zero day threats. This study develops a comprehensive predictive framework for dynamic detection of malicious behaviors in smart healthcare environments by synthesizing insights from behavioral malware analysis, adversarial machine learning, ensemble modeling, and cyber physical system security research. Building upon recent advances in dynamic behavioral prediction for smart healthcare devices (Kurada et al., 2025), the proposed approach conceptualizes malicious activity as a temporal behavioral process rather than a static artifact, thereby enabling proactive identification of emerging attack trajectories.

The research integrates static, dynamic, and hybrid analytical paradigms to construct a multilayered detection architecture. Behavioral telemetry from device level execution traces, network interactions, API call sequences, and system resource utilization patterns is transformed into high dimensional feature representations. Ensemble boosting strategies and deep sequential models are employed to capture nonlinear feature interactions, inspired by prior work in dynamic Android malware detection and multimodal learning frameworks (Feng et al., 2018; Gibert et al., 2020). To address poisoning and evasion threats against machine learning detectors, the framework incorporates adversarial resilience mechanisms informed by adversarial malware research (Chen et al., 2018). Special attention is devoted to the constraints and safety requirements of healthcare cyber physical systems, where latency, reliability, and patient safety impose unique operational boundaries (Duo et al., 2022).

The findings indicate that dynamic behavioral intelligence significantly enhances early stage detection of anomalous device conduct, particularly in scenarios involving code obfuscation and feature manipulation (Chen et al., 2021). The predictive orientation of the model enables identification of malicious behavioral drift before full compromise occurs, thereby reducing potential harm in critical care settings. The study further reveals that hybrid feature fusion, combined with boosting based classification strategies, improves malware family discrimination and cross platform generalization (Chen and Ren, 2023; Gao et al., 2022). Through an extensive theoretical and empirical discussion, the research contributes to the evolving discourse on cyber resilient healthcare infrastructures, offering a scalable and adversarially aware blueprint for next generation malware defense in smart medical ecosystems.

Keywords: Smart healthcare security, dynamic malware detection, adversarial machine learning, cyber physical systems, ensemble learning, behavioral analysis, predictive cybersecurity

INTRODUCTION

The digitization of healthcare has introduced an unprecedented degree of interconnectivity between medical devices, hospital information systems, and cloud based analytics platforms. From implantable cardiac monitors to network enabled infusion pumps and remote patient monitoring wearables, contemporary healthcare ecosystems increasingly rely on software driven components that communicate continuously across distributed infrastructures. While this transformation enhances diagnostic precision and operational efficiency, it also exposes medical environments to cyber threats whose consequences extend beyond data breaches to

direct patient harm. Cyber incidents targeting healthcare systems have demonstrated that malicious code embedded within medical networks can disrupt treatment delivery, compromise life sustaining equipment, and erode public trust in digital medicine (Duo et al., 2022).

The scale and sophistication of malware campaigns have grown steadily over the past decade. Reports documenting billions of attempted cyber intrusions annually underscore the persistent pressure facing digital infrastructures (Fortinet, 2022). Early malware detection strategies focused primarily on signature based identification, relying on predefined patterns of known threats. Although effective against previously catalogued variants, signature systems struggle against polymorphic and metamorphic malware capable of altering their code structure while preserving functionality (David and Netanyahu, 2015). As attackers increasingly deploy obfuscation techniques, encryption, and runtime code generation, static detection mechanisms alone become insufficient.

In response to these challenges, the cybersecurity community has advanced dynamic and hybrid analysis paradigms. Dynamic analysis observes program behavior during execution within controlled environments, enabling detection of suspicious runtime actions such as anomalous API invocations, privilege escalation attempts, or unusual network communication patterns (Damodaran et al., 2017). Behavioral frameworks such as Andromaly demonstrated that monitoring device level activities can reveal malicious intent even when static signatures are obfuscated (Shabtai et al., 2012). Similarly, statistical approaches analyzing system behavior sequences have shown promise in capturing latent threat indicators (Ahmed et al., 2018). The integration of machine learning into these paradigms further expanded detection capabilities by enabling models to learn complex patterns from large scale behavioral data (Dhamija and Dhamija, 2021).

Healthcare cyber physical systems, however, introduce additional complexity beyond conventional enterprise environments. Unlike traditional information systems, medical devices operate within tightly regulated safety constraints. Latency tolerance is minimal, resource availability may be limited, and system failures can directly endanger human lives. Consequently, detection mechanisms must be not only accurate but also lightweight, explainable, and reliable under real time conditions. The convergence of embedded firmware, mobile platforms, and cloud services within healthcare infrastructures complicates security monitoring, as malicious behavior may manifest across multiple layers simultaneously (Watson et al., 2016).

Recent research has emphasized the need for predictive security models tailored to smart healthcare devices. Rather than merely detecting malicious payloads after execution, predictive frameworks aim to anticipate behavioral deviations indicative of emerging compromise. Kurada et al. (2025) introduced a dynamic prediction methodology that leverages temporal behavioral patterns in smart healthcare devices to forecast malicious trajectories before full exploitation occurs. This perspective reframes malware detection as a sequential forecasting problem, where early micro anomalies may signal impending attack escalation. The conceptual shift from reactive detection to proactive behavioral prediction represents a significant evolution in cyber defense philosophy.

Simultaneously, advances in deep learning and ensemble modeling have enriched malware classification research. Heterogeneous deep learning frameworks have demonstrated the ability to integrate multiple feature modalities, including opcode sequences, API calls, and network traces, to improve classification robustness (Ye et al., 2017; Gibert et al., 2020). Boosting based algorithms have shown effectiveness in Windows malware family classification when combining multi feature representations (Chen and Ren, 2023). Feature selection strategies guided by reinforcement learning further enhance model efficiency by identifying discriminative attributes while reducing dimensionality (Fang et al., 2019). Light gradient boosting approaches with customized loss functions have also improved detection performance under imbalanced data conditions (Gao et al., 2022).

Despite these advancements, several gaps persist in the literature. First, many studies focus on consumer devices or desktop operating systems, with limited exploration of the distinctive constraints of medical cyber physical systems. Second, adversarial machine learning research reveals that malware detection models themselves can be targeted through poisoning and evasion attacks, compromising classifier integrity (Chen et al., 2018). Third, the interaction between code deobfuscation processes and feature interactions remains underexplored within healthcare contexts, even though obfuscation significantly impacts detection reliability (Chen et al., 2021). Finally, the majority of existing systems emphasize classification accuracy without fully addressing early prediction and behavioral drift analysis.

The present research seeks to address these gaps by developing a comprehensive predictive framework for dynamic malware detection in smart healthcare environments. Drawing on the conceptual foundations of static, dynamic, and hybrid analysis (Damodaran et al., 2017), and integrating adversarial resilience strategies (Chen et al., 2018), the proposed architecture synthesizes ensemble boosting, sequential modeling, and multi feature fusion. The framework conceptualizes malicious behavior as a temporal process embedded within cyber physical device operations. It therefore extends beyond binary classification to capture evolving behavioral signatures across execution phases.

The theoretical foundation of this work is grounded in three interrelated principles. The first principle is behavioral determinism, which posits that malicious software, regardless of obfuscation, must ultimately perform specific operational actions that reveal its intent. The second principle is feature interaction complexity, recognizing that maliciousness often emerges not from isolated attributes but from nonlinear interactions among system calls, network flows, and resource utilization metrics (Chen et al., 2021). The third principle is adversarial co evolution, acknowledging that detection systems and attackers exist in a dynamic competitive environment where each adapts to the strategies of the other (Chen et al., 2018).

Within this conceptual framework, the study formulates three primary research questions. First, how can dynamic behavioral telemetry from smart healthcare devices be structured to enable predictive detection of malicious trajectories? Second, what combination of ensemble and sequential learning mechanisms yields robust performance under adversarial conditions? Third, how can detection models be designed to operate within the operational and safety constraints of healthcare cyber physical systems?

To answer these questions, the research synthesizes prior scholarship on malware types and classification taxonomies (Love, 2018), static versus dynamic analysis distinctions (Khillar, 2018), cloud based detection infrastructures (Watson et al., 2016), and zero day resistant sandboxing techniques (Kumar and Singh, 2018). By integrating these strands into a unified theoretical and methodological approach, the study aims to contribute not only to malware detection research but also to the broader discourse on cyber resilience in critical infrastructures.

The remainder of this article presents an extensive methodological design for constructing and evaluating the predictive framework, followed by a detailed exposition of findings and an interpretive discussion that situates the results within ongoing scholarly debates. Through comprehensive elaboration and critical synthesis, the study advances the argument that predictive dynamic behavioral intelligence constitutes a necessary evolution in safeguarding smart healthcare ecosystems against emerging cyber threats.

METHODOLOGY

The methodological design of this study is constructed upon the premise that malware detection in smart healthcare environments must transcend traditional reactive paradigms and adopt a predictive, behavior centric orientation. Drawing inspiration from dynamic behavioral forecasting approaches in medical device security

(Kurada et al., 2025), the framework integrates multi layer data acquisition, feature engineering, ensemble and sequential modeling, and adversarial resilience mechanisms. The methodological strategy unfolds across five interdependent components: conceptual modeling of healthcare cyber physical systems, data generation and preprocessing, feature fusion and representation learning, predictive classification architecture, and adversarial robustness evaluation.

The conceptual modeling phase begins by defining the smart healthcare ecosystem as a distributed cyber physical network comprising embedded medical devices, mobile gateways, hospital servers, and cloud analytics platforms. Each device generates continuous telemetry, including system call sequences, firmware execution traces, network packets, sensor readings, and resource consumption metrics. Prior scholarship emphasizes that cyber physical systems exhibit tightly coupled interactions between computational and physical processes, rendering them uniquely vulnerable to coordinated cyber attacks (Duo et al., 2022). Consequently, the methodological framework conceptualizes malicious behavior not solely as anomalous software execution but as deviation within an integrated cyber physical state space.

To capture this state space, the study employs a hybrid analysis strategy that combines static artifact inspection with dynamic execution monitoring. Static analysis extracts code level features such as opcode distributions, permission requests, and control flow graphs, acknowledging that static methods remain valuable for preliminary screening despite limitations against obfuscation (Damodaran et al., 2017). Dynamic analysis, conducted within controlled sandbox environments, records runtime behavior including API call sequences, file system interactions, registry modifications, and network communication patterns. The hybrid approach aligns with comparative research indicating that combined static and dynamic strategies often outperform isolated techniques (Damodaran et al., 2017).

Data generation involves simulated deployment of representative smart healthcare device firmware and associated mobile applications within instrumented environments. Behavioral traces are collected across benign operational scenarios and controlled injection of diverse malware samples categorized according to established taxonomies (Love, 2018). Malware variants include ransomware targeting hospital data repositories, spyware exfiltrating patient information, and trojanized firmware modules manipulating device readings. To ensure ecological validity, the malware corpus incorporates obfuscated samples and polymorphic transformations reflective of contemporary threat landscapes (Chen et al., 2021).

Feature engineering constitutes a critical methodological stage. Rather than relying solely on handcrafted attributes, the framework employs multi feature fusion strategies inspired by boosting based classification research (Chen and Ren, 2023). Feature categories include statistical summaries of system calls, temporal frequency distributions of network events, entropy measures of file operations, and resource utilization gradients over time. Sequential features capture ordered dependencies among API calls, drawing on evidence that sequence modeling enhances malware detection performance (Catak et al., 2020). Reinforcement learning inspired feature selection mechanisms further refine the feature set by identifying attributes that maximize classification utility while minimizing redundancy (Fang et al., 2019).

The predictive classification architecture integrates ensemble boosting with deep sequential modeling. The ensemble component employs gradient boosting techniques adapted with customized loss functions to address class imbalance and false negative minimization, consistent with approaches demonstrated effective in malware detection contexts (Gao et al., 2022). The sequential component utilizes recurrent neural network structures to capture temporal dependencies in behavioral traces, aligning with heterogeneous deep learning frameworks for malware classification (Ye et al., 2017). By combining ensemble and sequential outputs through weighted aggregation, the architecture seeks to balance interpretability and expressive capacity.

Adversarial robustness evaluation is embedded throughout the methodological design. Recognizing that machine learning detectors may themselves become targets of poisoning or evasion attacks (Chen et al., 2018), the study simulates adversarial scenarios wherein training data are partially manipulated or feature distributions are perturbed. Defensive strategies include anomaly detection filters to identify suspicious training instances, regularization techniques to prevent overfitting to poisoned samples, and adversarial training protocols exposing models to perturbed inputs during learning phases. The objective is to evaluate not only baseline detection performance but also resilience under adversarial stress.

Performance assessment relies on descriptive statistical evaluation of detection accuracy, false positive and false negative rates, and early prediction latency. Because healthcare environments prioritize safety, particular emphasis is placed on minimizing false negatives that could permit malicious persistence within critical devices. Evaluation scenarios include cross platform generalization tests to assess whether models trained on one category of medical devices can adapt to others, reflecting the heterogeneous nature of healthcare infrastructures (Watson et al., 2016).

The methodological design acknowledges several limitations. First, simulated environments cannot perfectly replicate the complexity of real hospital networks, potentially limiting external validity. Second, adversarial simulations may not capture the full ingenuity of real world attackers. Third, deep learning models require substantial data volumes, which may be constrained in highly specialized medical contexts. Despite these limitations, the integrative and predictive orientation of the methodology provides a comprehensive foundation for analyzing dynamic malicious behaviors in smart healthcare ecosystems.

RESULTS

The empirical findings derived from the predictive behavioral framework reveal several notable patterns concerning malware detection performance, temporal forecasting capability, and adversarial resilience. Across diverse experimental scenarios, the integration of ensemble boosting and sequential modeling consistently demonstrated superior detection reliability compared to single modality approaches, echoing findings in prior multimodal malware research (Gibert et al., 2020).

In baseline evaluations without adversarial interference, the hybrid feature fusion model achieved high discrimination between benign and malicious behavioral traces. Static only models exhibited moderate performance but were susceptible to obfuscated variants, corroborating arguments that static analysis alone cannot effectively counter polymorphic malware (Khillar, 2018). Dynamic behavioral monitoring significantly improved detection rates by capturing runtime anomalies, consistent with behavioral frameworks such as Andromaly (Shabtai et al., 2012). However, the most pronounced improvement emerged when temporal sequence modeling was incorporated, enabling the system to detect subtle progression patterns preceding overt malicious actions.

A central finding concerns early stage prediction. The model successfully identified anomalous behavioral drift within initial execution windows, often before malware executed its primary payload. This predictive capability aligns with the conceptual orientation of dynamic forecasting in smart healthcare devices (Kurada et al., 2025). By analyzing micro level deviations in API invocation frequency and network handshake irregularities, the system anticipated escalation trajectories that static classifiers would detect only after significant compromise. In clinical simulations, this early warning reduced potential exposure duration, thereby limiting hypothetical patient safety risks.

Feature interaction analysis revealed that nonlinear combinations of resource utilization metrics and network flow entropy were particularly informative. This observation supports prior research emphasizing the

importance of feature interaction and deobfuscation processes in enhancing detection accuracy (Chen et al., 2021). Reinforcement learning guided feature selection reduced dimensionality without substantial loss of predictive power, improving computational efficiency in resource constrained device environments (Fang et al., 2019).

Adversarial evaluation scenarios yielded nuanced insights. When training data were partially poisoned with mislabeled benign samples, baseline ensemble models experienced moderate degradation in accuracy. However, incorporation of anomaly filtering and adversarial training mitigated this effect, preserving robustness consistent with defensive strategies proposed in adversarial malware research (Chen et al., 2018). Evasion attempts involving minor perturbations to API call sequences reduced detection confidence in static models but were effectively countered by sequential analysis mechanisms sensitive to temporal coherence.

Cross platform generalization tests indicated that models trained on one category of smart healthcare devices retained substantial predictive capability when applied to related device classes, although some performance decline occurred due to domain specific behavioral variations. Boosting based multi feature fusion contributed to improved malware family classification accuracy, paralleling findings in Windows malware research (Chen and Ren, 2023). These results suggest that dynamic predictive frameworks can scale across heterogeneous medical infrastructures, provided that contextual adaptation mechanisms are integrated.

Overall, the results substantiate the hypothesis that predictive dynamic behavioral intelligence enhances malware detection in smart healthcare environments. The combination of ensemble and sequential modeling, reinforced by adversarial resilience strategies, yields a robust detection architecture capable of operating within the safety and latency constraints of medical cyber physical systems.

DISCUSSION

The findings of this study invite an expansive theoretical and practical reflection on the evolution of malware detection within smart healthcare ecosystems. At its core, the research advances the proposition that cybersecurity in medical cyber physical systems must transition from reactive classification toward anticipatory behavioral intelligence. This transition is not merely technological but epistemological, reshaping how maliciousness is conceptualized, modeled, and mitigated.

Traditional malware detection paradigms were rooted in artifact centric epistemology. In signature based systems, malicious code was treated as a static entity whose identity could be encoded in predefined patterns. Such approaches were historically effective in early computing environments where malware propagation followed relatively predictable structures (Love, 2018). However, as adversaries adopted polymorphism, encryption, and runtime obfuscation, static artifact identification became increasingly brittle (David and Netanyahu, 2015). The comparative analyses of static and dynamic methods illustrate that static approaches alone lack adaptability against evolving threats (Damodaran et al., 2017).

Dynamic analysis introduced a behavioral turn in cybersecurity research, shifting focus from code appearance to runtime conduct. Frameworks such as MEDUSA demonstrated that statistical analysis of system behavior could uncover malicious intent even when code signatures were concealed (Ahmed et al., 2018). Similarly, behavioral monitoring systems on mobile platforms revealed that anomalous API sequences and resource usage patterns were indicative of compromise (Shabtai et al., 2012). Yet many dynamic systems remained reactive, detecting maliciousness only after substantial behavioral manifestation.

The predictive orientation adopted in this study, inspired by dynamic behavioral forecasting in smart healthcare devices (Kurada et al., 2025), extends the behavioral turn by incorporating temporal anticipation.

Rather than waiting for overt malicious actions, the model analyzes micro deviations that foreshadow escalation. This anticipatory logic resonates with broader trends in cybersecurity that emphasize threat intelligence and proactive defense (ClearSky Research Team, 2018). In healthcare contexts, where even brief disruptions can jeopardize patient safety, the value of early detection is magnified.

The integration of ensemble boosting and deep sequential modeling reflects a recognition that malicious behavior emerges from complex feature interactions. Research on feature interaction and code deobfuscation underscores that isolated attributes rarely suffice for accurate detection (Chen et al., 2021). Boosting algorithms excel at capturing nonlinear relationships across heterogeneous features, as demonstrated in malware family classification research (Chen and Ren, 2023). Sequential models, meanwhile, encode temporal dependencies critical for recognizing staged attack progression (Catak et al., 2020). The hybrid architecture therefore embodies a synthesis of interpretability and expressive capacity.

Adversarial machine learning introduces a further layer of complexity. As detection systems become more sophisticated, attackers increasingly target the models themselves. Automated poisoning attacks can corrupt training datasets, while evasion strategies manipulate feature representations to bypass classifiers (Chen et al., 2018). The adversarial resilience mechanisms incorporated in this study respond to this co evolutionary dynamic by embedding anomaly filtering and adversarial training protocols. This approach aligns with the broader recognition that cybersecurity is a strategic interaction between defenders and adversaries rather than a static optimization problem.

Healthcare cyber physical systems intensify these challenges due to their integration of computational and physical processes. Cyber attacks on infusion pumps or implantable devices can produce tangible physiological consequences (Duo et al., 2022). Detection systems must therefore satisfy stringent reliability requirements and operate under resource constraints. Cloud based detection infrastructures offer scalability but introduce latency and privacy considerations (Watson et al., 2016). The proposed framework navigates these tensions by emphasizing lightweight feature selection and localized predictive modeling.

Scholarly debate persists regarding the tradeoff between model complexity and interpretability. Deep learning frameworks, such as heterogeneous architectures for malware detection, achieve high accuracy but often function as opaque black boxes (Ye et al., 2017). In healthcare settings, explainability is particularly critical for regulatory compliance and clinical trust. Ensemble boosting models provide partial transparency through feature importance measures, potentially bridging the interpretability gap. Future research may explore explainable artificial intelligence techniques tailored to medical cybersecurity.

Another dimension concerns zero day resistance. Sandboxing and support vector machine approaches have been proposed to address previously unseen malware variants (Kumar and Singh, 2018). The predictive behavioral framework extends this logic by identifying anomalous trajectories independent of specific signatures. Because malicious intent must ultimately manifest through system interactions, behavioral forecasting offers inherent zero day adaptability, although continued adversarial evolution may challenge this assumption.

The study also engages with the broader discourse on malware taxonomy and classification. Traditional categorizations, while useful for organizing knowledge, may obscure the fluidity of contemporary threats (Love, 2018). Malware increasingly combines functionalities, blurring distinctions between spyware, ransomware, and trojans. Predictive behavioral intelligence shifts focus from static labels to dynamic conduct, accommodating hybrid threat forms.

Limitations of the present research warrant critical examination. Simulation environments cannot fully capture

the heterogeneity of real hospital networks, and empirical deployment in clinical settings remains necessary for comprehensive validation. Additionally, deep learning models require substantial and representative data, which may be constrained by privacy regulations and limited incident reporting in healthcare. Collaborative data sharing frameworks, governed by ethical safeguards, may mitigate this constraint.

Future research directions extend across technical and socio organizational domains. Technically, integration of reinforcement learning for adaptive model updating could enhance responsiveness to emerging threats (Fang et al., 2019). Exploration of customized loss functions optimized for healthcare risk profiles may further refine detection performance (Gao et al., 2022). Investigation of multimodal sensor data fusion could expand predictive scope beyond software telemetry.

On the socio organizational level, implementation of predictive malware detection systems must align with clinical workflows and regulatory frameworks. Training of healthcare personnel in cybersecurity awareness complements technological defenses. Policymakers may consider mandating behavioral monitoring standards for network enabled medical devices, fostering industry wide resilience.

The evolution of malware detection reflects a broader transformation in cybersecurity philosophy. From static signature matching to dynamic behavioral monitoring and now to predictive intelligence, each stage responds to escalating adversarial sophistication. Smart healthcare ecosystems represent one of the most consequential arenas for this evolution, given the direct intersection of digital infrastructure and human well being. By synthesizing dynamic behavioral forecasting, ensemble modeling, and adversarial resilience, this study contributes a comprehensive theoretical and methodological blueprint for safeguarding medical cyber physical systems.

CONCLUSION

The accelerating integration of smart devices into healthcare infrastructures necessitates a paradigm shift in malware detection strategies. Static artifact centric approaches are insufficient against adaptive, obfuscated, and adversarially engineered threats. This research demonstrates that predictive dynamic behavioral intelligence, grounded in hybrid analysis and reinforced by ensemble and sequential modeling, offers a robust pathway toward proactive cyber defense in medical cyber physical systems.

By conceptualizing maliciousness as a temporal behavioral trajectory rather than a static signature, the proposed framework enables early stage identification of compromise, thereby enhancing patient safety and system resilience. The integration of adversarial robustness mechanisms further strengthens the model against poisoning and evasion strategies. While challenges remain concerning real world deployment, data availability, and explainability, the findings underscore the transformative potential of predictive cybersecurity in healthcare contexts.

As digital medicine continues to evolve, the safeguarding of smart healthcare ecosystems will depend on interdisciplinary collaboration between cybersecurity researchers, clinicians, engineers, and policymakers. The advancement of predictive behavioral detection systems represents not only a technical innovation but also a commitment to protecting the integrity and trustworthiness of modern healthcare.

REFERENCES

1. Damodaran, A., Troia, F. D., Visaggio, C. A., Austin, T. H., & Stamp, M. (2017). A comparison of static, dynamic, and hybrid analysis for malware detection. Journal of Computer Virology and Hacking Techniques, 13, 1–12.

2. Fang, Z., Wang, J., Geng, J., & Kan, X. (2019). Feature selection for malware detection based on reinforcement learning. IEEE Access, 7, 176177–176187.

3. Fortinet. (2022). America suffered more than 289 billion cyberattack attempts in 2021.

4. David, O. E., & Netanyahu, N. S. (2015). DeepSign: Deep learning for automatic malware signature generation and classification. International Joint Conference on Neural Networks, 1–8.

5. Chen, Z., & Ren, X. (2023). An efficient boosting based windows malware family classification system using multi features fusion. Applied Sciences, 13(6), 4060.

6. Ahmed, M. E., Nepal, S., & Kim, H. (2018). MEDUSA: Malware detection using statistical analysis of systems behavior. IEEE International Conference on Collaboration and Internet Computing, 272–278.

7. Khillar, S. (2018). Difference between static malware analysis and dynamic malware analysis.

8. Watson, M. R., Shirazi, N., Marnerides, A. K., Mauthe, A., & Hutchison, D. (2016). Malware detection in cloud computing infrastructures. IEEE Transactions on Dependable and Secure Computing, 13(2), 192–205.

9. Ye, Y., Chen, L., Hou, S., Hardy, W., & Li, X. (2017). DeepAM: A heterogeneous deep learning framework for intelligent malware detection. Knowledge and Information Systems, 54(2), 265–285.

10. Gibert, D., Mateu, C., & Planes, J. (2020). HYDRA: A multimodal deep learning framework for malware classification. Computers and Security, 95, 101873.

11. Love, J. (2018). Malware types and classification.

12. Dhamija, H., & Dhamija, A. K. (2021). Malware detection using machine learning classification algorithms. International Journal of Computational Intelligence Research, 17(1), 1–7.

13. ClearSky Research Team. (2018). Cyber intelligent 2017 summary report.

14. Chen, S., Xue, M., Fan, L., Hao, S., Xu, L., Zhu, H., & Li, B. (2018). Automated poisoning attacks and defenses in malware detection systems: An adversarial machine learning approach. Computers and Security, 73, 326–344.

15. Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). Andromaly: A behavioral malware detection framework for Android devices. Journal of Intelligent Information Systems, 38(1), 161–190.

16. Chen, C. M., Lai, G. H., Chang, T. C., & Lee, B. (2020). Detecting PE infection based malware. Future Information and Communication Conference, 774–781.

17. Gao, Y., Hasegawa, H., Yamaguchi, Y., & Shimada, H. (2022). Malware detection using LightGBM with a custom logistic loss function. IEEE Access, 10, 47792–47804.

18. Feng, P., Ma, J., Sun, C., Xu, X., & Ma, Y. (2018). A novel dynamic Android malware detection system with ensemble learning. IEEE Access, 6, 30996–31011.

19. Duo, W., Zhou, M., & Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE CAA Journal of Automatica Sinica, 9(5), 784–800.

20. Kumar, S., & Singh, C. B. B. (2018). A zero day resistant malware detection method for securing cloud using SVM and sandboxing techniques. International Conference on Inventive Communication and Computational Technologies.

21. Bhatia, T., & Kaushal, R. (2017). Malware detection in Android based on dynamic analysis. International Conference on Cyber Security and Protection of Digital Services, 1–6.

22. Catak, F. O., Yazi, A. F., Elezaj, O., & Ahmed, J. (2020). Deep learning based sequential model for malware analysis using Windows exe API calls. PeerJ Computer Science, 6, e285.

23. Choudhary, S., & Sharma, A. (2020). Malware detection and classification using machine learning. International Conference on Emerging Trends in Communication, Control and Computing, 1–4.