**A Conceptual Framework for Anomaly Malware Detection using Ensemble Machine Learning in Memory-Based Analysis**

Hoi Kah Wei1, a), Ramakrishnan Kannan1, 2, b) and Mohammad Shadab Khan1, 3, c)

1Faculty of Computing and Informatics, Multimedia University, 63100, Cyberjaya, Malaysia

2Centre for Image and Vision Computing (CIVC), CoE for Artificial Intelligence, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.

3Centre of Advanced Analytics, CoE for Artificial Intelligence, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia.

c) Corresponding author: shadab.khan@mmu.edu.my

a) hoi.kah.wei@student.mmu.edu.my

b) kannan.ramakrishnan@mmu.edu.my

**Abstract.** Due to the wealth resources highly accessibility through internet, individuals enable to learn anything desire skill to explore the infinity knowledge and hand-on practice. While there still consist of a portion of people learning unethically to gain profit from other organisations. Gradually, the complexity of the malware becomes higher and the increment of the zero-day attack is surging currently. Evasive malware, such as Trojans and ransomware, is one of the key aspects for zero-day attack that against signature-based detection. The advanced threats would bypass predefined rules by applying techniques like code mutation and fileless execution. By doing so, memory-based analysis has emerged as a potent approach to provide useful insight during dynamic analysis, for detecting anomalies behaviour in system’s memory. To bridge the gap between memory analysis and machine learning techniques used in malware detection tools, this paper presents a conceptual framework that integrates ensemble machine learning for anomaly-based malware detection in memory. Other than that, a comprehensive review of existing machine learning-based malware detection tool was conducted to conceptually support the proposed methodology. The last session will propose a methodology by incorporating machine learning as well as deep learning for model training, the pattern of the malware sample enables to be recognised and identify the classification of the anomaly's malware.

# INTRODUCTION

Antivirus (AV) software such as McAfee, Norton, and Avast is widely used by default computer’s system to protect from malware injection [1]. Modern AV solutions primarily rely on signature-based methods, that wpi;d suspend the abnormal files immediately once the fingerprints match entries in a known malware’s database [2]. However, this approach requires frequently updates to deal with latest discovered malwares. Due to the rapid evolution of malware, signature-based detection fails to identify sophisticated threats which had created loopholes, as well as zero-day attack to allow evasive malware to bypass AV protection. As a result, traditional signature-based methods are becoming significant ineffective through evasive malware.

Dynamic analysis is an effective approach for analysing an infected system. It offers informative insight by monitoring the behaviour of suspicious files during malware execution. However, the approach is time-consuming and computationally intensive [2]. The rapid proliferation and constant evolution of malware families underscore immediate attention for robust classification systems by adapting to unknown threats through hybrid analysis techniques [3].

This paper begins by highlighting the importance of memory forensics in anomalies malicious behaviours that exploit system vulnerabilities. Besides, the past research work in machine learning-based and deep learning-based detection methodology will be comprehensive review and identify the research gap. Other than that, a conceptual framework is proposed to outline an ensemble machine learning–based approach for memory-focused malware detection. Finally, the paper concludes with a discussion of future directions, including the potential for real-time detection and additional insights to guide further research.

# LITERATURE REVIEW

## Overview

In this session, the paper will be comprehensively reviewed for identify the gaps for proposed methodology. With the complexity increment of modern malware, the critical in nature had inspired researchers to explore advanced detection methods beyond traditional static and signature-based approaches. Memory forensics has emerged as a critical technique for analysing volatile system data to identify runtime anomalies that signal malicious activity. This approach enables visibility into malware behaviours that evade themselve through disk-based detection by processing injection, code obfuscation, and fileless execution. Apart from that, machine learning (ML) techniques have gained traction in malware analysis for their ability to learn patterns from large volumes of behavioural data with facilitating automated anomaly detection without relying on predefined signatures. More recently, deep learning (DL) models have further enhanced this capability by extracting high-level representations from raw memory dumps, process traces, and system call sequences. Together, these technologies form a promising foundation for intelligent, adaptive malware detection systems that can generalize to previously unseen threats. This section surveys key research efforts in these areas, focusing on their application across diverse platforms and threat landscapes.

## Machine Learning-based Malware Detection Tool

The research study primarily focuses on dynamic malware detection. Traditional antivirus systems that rely on matching signatures can miss polymorphic and newly discovered threats, highlighting the need for different approaches [4]. They collect the malware report for observing their behaviour via Cuckoo sandbox. The author uses the machine learning technique for classification and detection. The experiment shows the high detection and classification accuracy rate that achieves 100% accuracy under labelled data. Automatic behaviour-based malware detection using machine learning algorithms is considered a game-changing innovation. Guarding computer networks is a top priority, but malware incidents are rising despite existing scanners. Dynamic methods are preferred over static methods because hiding malicious behaviour during execution is much harder than doing so during static analysis. Experts in cybersecurity have been emphasizing the use of machine learning algorithms for malware detection and predicting malware family behaviour.

Early work by [5] provided a comprehensive survey on the effectiveness of supervised learning techniques, such as SVM and ANN, in classifying static PE32 Windows files. Through a systematic approach, the authors demonstrated that supervised machine learning performs well on certain feature sets, particularly PE header features. However, the Bayes Network often showed lower accuracy compared to other methods, likely due to the extremely low probabilities values associated with high-dimensional features like opcode and bytes n-grams [5]. This underscores the trade-off between model complexity and generalizability, a core challenge in static analysis–based malware detection.

[6] highlighted the growing significance of machine learning (ML) in enhancing malware detection capabilities across cybersecurity domains4. The authors demonstrate how the supervised, semi-supervised, and unsupervised approaches detect the malware from large datasets. The survey also emphasizes the importance of preprocessing steps have significantly influence classification performance by further emphasizing preprocessing technique of data cleaning, dimensionality reduction, and imbalance handling. Additionally, hyperparameter optimization is highlighted as a key factor in improving model outcomes. To address challenges of dependence of labelled data together with vulnerability to adversarial manipulation, an ensemble machine learning is introduced as a compelling solution. By combining multiple learners, ensemble methods offer more resilient and accurate detection by enhancing robustness, reducing variance, and mitigating bias. Also, the researchers have suggested that although ML-based detection systems offer considerable promise, it's neccesery to consider of data quality and robustness for real-world deployment.

[7] highlighted the importance of feature selection in minimizing false positives in malware classification. Their method was proposed as a complementary approach to traditional signature-based detection systems. The study demonstrated the significants of feature engineering impacts key performance metrics such as precision and recall. Although the framework aimed to achieve zero false positives, a residual rate persisted. As a result, they underscores the need to align preprocessing techniques with the strengths of specific classifiers to enhance anomaly detection reliability. Additionally, the authors reported a decline in detection accuracy on larger datasets, attributing this to noise introduced by human annotation errors.

A rapid evidence assessment conducted by [8] consolidates current research findings on the use of ML in multiple cybersecurity applications. In malware detection, supervised models such as support vector machines (SVMs) have shown accuracy exceeding 97% when trained on known malware's signatures and behaviours. Beyond general malware,the researcher also claim that ML also enables effective phishing email classification, intrusion detection through anomaly modelling and threat intelligence analysis. These advancements highlight the role of machine learning not only increasing detection speed, but also reducing manual workload by providing automated threat insights. However, limitations including data quality concerns, model interpretability, susceptibility are still remain for adversarial attacks. Additionally, the risk of bias in training datasets still exist. These findings highlight both the promise and the challenges of ML-based detection, reinforcing the importance of robust feature engineering, continuous learning, and interpretability in practical deployment.

Besides, [3] addressed the limitation of traditional malware detection methods in combating modern threats. They propose an innovative approach that utilize the ensemble method with implementing different types of classifiers in memory-based malware detection framework. Benchmarking results show that the proposed ensemble method achieved the highest accuracy (87.88%), outperforming individual models like XGBoost (86.55%) and Random Forest (83.87%). Alternative ensemble methods such as Stacking and Voting Classifiers also performed well but slightly below the proposed model. The study demonstrates that combining high-performing classifiers in an ensemble not only improves detection accuracy but also offers computational efficiency.

A summary of the reviewed articles is provided in Table 1, that apply machine learning-based approaches for malware detection by highlighting the ML technique(s) implementation, key findings, and identified limitations. Together, these studies form the foundation for designing a robust ML based malware detection tool. They reveal the significance of classifier selection, feature engineering, and adaptive learning mechanisms in developing scalable and accurate detection systems capable of handling diverse and evolving threats.

**TABLE 1.** Literature review of machine learning-based malware detection

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **ML Techniques** | **Key Findings** | **Limitations** |
| [4] | Decision Trees, Random Forest, k-NN, SVM | Wide applicability of supervised techniques; shows need for refinement in feature selection | Performance degradation with new, unseen malware variants; reliance on large, labeled datasets |
| [5] | SVM, ANN, Bayesian Networks, Naïve Bayes | High accuracy for SVM and ANN; useful for high-dimensional feature classification | Struggles with high-dimensional features; higher false-negative rates with certain models |
| [6] | SVM, Random Forest, Decision Trees | Demonstrates the importance of high-quality datasets and feature refinement | Supervised models still need refinement for better generalization |
| [7] | Various machine learning classifiers | Focus on feature selection for better detection rates; broad application in malware detection | May be less effective with poor dataset quality; requires careful feature selection for accuracy |
| [8] | Various machine learning models | High adaptability to new data; continuous learning to improve accuracy | Requires large datasets and ongoing training to maintain performance |
| [3] | Gradient Boosting and Random Forest | High accuracy of blended ensemble method and computational efficiency | No mention |

## Deep Learning-Based Malware Detection Tools

Recent literature has explored the use of deep learning techniques, particularly deep neural networks (DNNs), for static malware detection by learning patterns from portable executable (PE) files [9]. These approaches extract structured features from PE headers alongside statistical representations of raw byte content, enabling the model to analyze files without execution. Feature vectors are typically standardized and fed into dense neural networks optimized through techniques like dropout regularization and adaptive optimizers. The high accuracy and low false positive rates on benchmark datasets which demonstrated by researcher shows that deep learning can outperform traditional classifiers like decision trees in both detection performance and efficiency. Nonetheless,   
the generalized to non-Windows platform, interpretability of complex models, and the need for large, well-labeled datasets still marked as challenges remain in the proposed methodology. These findings underscore the potential of deep learning in malware detection, while also highlighting the importance of addressing robustness and reproducibility issues for practical deployment.

[2] introduced the deep learning approach in image-based malware detection, which converts malware binaries into grayscale images and analyses them using convolutional neural networks (CNNs). They proposed an enhanced model by incorporating multi-headed attention mechanisms to improve accuracy for classification by focusing on localized regions through the malware image. This method arcieved platform-independent and computationally efficient by eliminates the need for manual feature engineering or code execution. By conducting the proposed architecture, the Malimg dataset is used to train on the model that consistently achieved high accuracy (up to 99% on average) and demonstrated superior generalizability compared to standard CNNs, especially in detecting challenging or underrepresented malware families. The attention layer proved effective in enhancing feature localization and reducing model complexity by significantly lowering the number of trainable parameters. However, limitations such as dataset imbalance, misclassification of visually similar malware variants, and lack of behavioural insights were acknowledged. On the other hand, the model’s reliance on known malware images that raise concerns about its effectiveness in detecting zero-day threats. Thus, they highlight the need for future work that integrates behavioural analysis or uses more diverse datasets.

A study in [10] investigates the effectiveness of malware detection and classification using various neural network (NN) architectures. The researchers had evaluated and compared between CNNs, RNNs, and ANNs for image-based malware classification. The models were trained by using Kaggle dataset that consist of 10,860 samples, with standard preprocessing and evaluated the prediction using accuracy, precision, recall, and F1-score. The outcome of the evaluation display that CNNs were the most effective approach due to their ability to capture spatial features in malware images. While RNNs and ANNs are struggled with spatial recognition. The study also highlighted limitations, including the need for larger datasets, better hyperparameter tuning, and more specialized architectures for image-based malware detection.

Table 2 provides a summary of the reviewed articles that utilize deep learning-based approaches for malware detection by highlighting the proposed methodologies or frameworks, key findings, analysis, and identified limitations. In the long run, techniques such as Convolutional Neural Networks (CNNs) and attention-based models demonstrate strong capabilities in automatically learning spatial and hierarchical patterns crucial for identifying malicious code. These methods outperform traditional approaches by eliminating manual feature engineering and adapting well to obfuscation and polymorphism. While deep learning has emerged as a powerful paradigm for malware detection and classification, particularly when malware is represented as image data, however, current research also reveals several limitations, including challenges with dataset diversity, class imbalance, and generalizability to zero-day threats [11],[12]. Future work should focus on optimizing model architecture, enhancing training datasets, and integrating behavioural or hybrid analysis to strengthen detection performance in real-world environments.

**TABLE 2**. Literature review of deep learning-based malware detection

|  |  |  |  |
| --- | --- | --- | --- |
| **Author(s) & Year** | **ML Techniques** | **Strengths** | **Limitations** |
| [9] | Deep Neural Networks (DNN) | High true positive rate and low false positives | Requires large, well-labelled datasets |
| [2] | CNN | Effective at capturing complex patterns; improved classification accuracy | Computationally intensive; may require large datasets and resources for training |
| [10] | Neural Networks | Strong feature extraction capabilities; improves detection rates | Requires large training datasets and may struggle with small or imbalanced datasets |

# Proposed framework

The proposed framework primarily aims to achieve higher accuracy while reducing overfitting by carefully managing the data fed into the model during training. The framework is visually represented in Figure 1.

## ****Memory Dump Acquisition****

Memory dumps are essential for analyzing malware behavior at runtime, which can give deeper insights into its structure and functions. Tools like Volatility are commonly used to acquire memory dumps from running systems. These tools allow for the extraction of valuable features such as process lists, network connections, and system calls, all of which are crucial for detecting malicious activity. Several public datasets are available for memory dump analysis, including CICMelMam-2022, MeMalDet and MemMal-D2024. These datasets have been widely used in malware research and can provide a reliable source of labeled and anonymized data for training and evaluating detection models. Leveraging such datasets is important for ensuring the robustness of the proposed model, especially in a real-world setting.

## Data Preprocessing

In this step, data cleaning is performed to handle missing or NaN values, ensuring the dataset is ready for modeling. Feature augmentation may also be applied, depending on the specific requirements of the dataset. Temporal splits are preferred, especially for malware detection tasks, as they simulate real-world scenarios where models are trained on older data and tested on newer data (future attacks). Training and testing datasets are separated, and for temporal splits, the data prior to 2020 might be used for training, with data from 2020 onward used for testing. This approach helps simulate how the model might perform when exposed to future, previously unseen malware.

## Deep Learning-Based Feature Extraction

Deep learning-based models, such as autoencoders, are used to extract features from raw memory dump data. This process performs dimensionality reduction, transforming high-dimensional data into a compact, meaningful representation. The encoder portion of the model is responsible for this task. By reducing the dimensionality, the model focuses on capturing the most relevant patterns in the data, which can be crucial for anomaly detection. In the context of malware detection, this is especially useful because malware evolves over time, and deep learning models can learn complex, non-linear representations that might not be easily captured by traditional feature engineering methods.

## Ensemble Learning Model

Once the features are extracted by deep learning, they are passed through different base classifiers (e.g., Random Forest, SVM, XGBoost). Each base classifier generates class probabilities, indicating the likelihood of the sample being either benign or malicious. After that, these individual prediction output are stacked and fed as inputs for a meta-classifier (such as Logistic Regression, LightGBM, or a simple Neural Network). The meta-classifier combines these base classifier outputs to make a final decision. The stacked method often leading to improved accuracy and robustness compared to single classifier in the model for better prediction.

## Prediction & Evaluation

The final meta-classifier is responsible to finalize the prediction of malware sample into catagories - either malicious or benign. For evaluation the model efficiently and performance, various metrics - accuracy, F1-Score, precision, recall, AUC-ROC will be implemented. By incorporating these evaluation metrics, malware detection models can be assessed more effectively to ensure they generalize well to real-world threats.

A diagram of a software malware detection

AI-generated content may be incorrect.

**FIGURE 1.** The proposed framework

# discussion

Deep learning model plays a crucial role that utilize the latent space feature for learning the obfuscation malware behavior. It captures the underlying structure of the data, which only preserving the most relevant information after input data has been compressed. The approach is important in malware detection where malware behaviour exhibits complex patterns that sometimes might not be captured by traditional feature engineering methods. Thus, the application of the deep learning for feature extraction like autoencoders are necessary. These models is crucial for handling unlabelled data and future malware variants. The ability to detect new, previously unseen malware samples is one of the key strengths of deep learning in this area.

Incontrovertible, the effectiveness of the proposed framework relies heavily with the availability of high-quality, well-labelled memory dump datasets. In practice, vast and diverse datasets might be noisy, incomplete, or biased, that could negatively impact the model’s performance together with its ability to generalize to unseen malware variants. Nevertheless, the process of extracting features from memory dumps, followed by deep learning-based encoding and ensemble classification will cause computational overhead and latency. This shortage may limit the framework’s applicability in real-time detection scenarios. To maintain its effectiveness over time, the framework would require regularly updated datasets to adapt to the evolving nature of malware threats.

# conclusion and future work

The sophisticated threats have increasingly affected the performance of the modern AV software, which using the traditional detection techniques, to detect them. This involves potential harm for significant damage of the system. In response, memory-based analysis has emerged as a critical approach for uncovering hidden and obfuscated malware behaviour. The proposed framework aims to address following challenges by introducing a structured pipeline for reducing bias and data inconsistencies for dataset before feeding them into an ensemble machine learning model.

Notwithstanding its potential, the proposed framework consists of several limitations. It depends heavily on the availability of high-quality, well-labelled memory dump datasets for effective training. In reality, such datasets may contain noisy, incomplete, or biased data, which can hinder the model’s performance and its ability to generalize to new malware types. Besides, the multi-stage execution that ranging from memory dump analysis to deep learning-based feature extraction and ensemble classification, introduces computational latency. This makes real-time detection challenging. Moreover, the effectiveness of temporal analysis relies on continuously updated datasets, which may not always be accessible.

By integrating deep learning as feature extraction, it enhances the robustness of classification and improves detection accuracy against complex malware threats. Despite being conceptual at this stage, the framework still shows great theoretical viability based on knowledge from the trends of current research. In order to evaluate its scalability and practical efficacy, future research will concentrate on empirical validation using real-world datasets.

# References

1. E. Mixon, “Why antivirus is not enough to prevent ransomware” Blumira. (2021), <https://www.blumira.com/blog/does-antivirus-prevent-ransomware>
2. V. Ravi, and M. Alazab, “Attention‐based convolutional neural network deep learning approach for robust malware classification,” Computational Intelligence **39**(1), 145–168 (2023).
3. K. K, D. Harini, P. Thanmai, and M. Seshan, “Malware Detection through Memory Dump Analysis by Enhanced Machine Learning Techniques,” in *2025 International Conference on Data Science, Agents &amp; Artificial Intelligence (ICDSAAI)*, (IEEE, Chennai, India, 2025), pp. 1–6.
4. M.S. Akhtar, and T. Feng, “Evaluation of Machine Learning Algorithms for Malware Detection,” Sensors **23**(2), 946 (2023).
5. A. Shalaginov, S. Banin, A. Dehghantanha, and K. Franke, “Machine Learning Aided Static Malware Analysis: A Survey and Tutorial,” in *Cyber Threat Intelligence*, edited by A. Dehghantanha, M. Conti, and T. Dargahi, (Springer International Publishing, Cham, 2018), pp. 7–45.
6. T. Talaei Khoei, and N. Kaabouch, “Machine Learning: Models, Challenges, and Research Directions,” Future Internet **15**(10), 332 (2023).
7. D. Gavriluț, M. Cimpoeșu, D. Anton, and L. Ciortuz, "Malware detection using machine learning," in Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 735–741 (IEEE, 2009)
8. R. Jones, M. Omar, D. Mohammed, C. Nobles, and M. Dawson, “Harnessing the Speed and Accuracy of Machine Learning to Advance Cybersecurity,” in *2023 Congress in Computer Science, Computer Engineering, &amp; Applied Computing (CSCE)*, (IEEE, Las Vegas, NV, USA, 2023), pp. 418–421.
9. P. Puranik, Static Malware Detection Using Deep Neural Networks on Portable Executables, PhD Thesis, 2019.
10. I.A. Richie, Malware Detection and Classification Using Different Neural Networks, PhD Thesis, 2024.
11. T. Shahzad, and K. Aman, “Unveiling the efficacy of AI-based algorithms in phishing attack detection,” *Journal of Informatics and Web Engineering* 3(2), 116–133 (2024), doi:10.33093/jiwe.2024.3.2.9.
12. S. Mushtaq, T. Javed, and M. Mohd Su’ud, “Ensemble learning-powered URL phishing detection: A performance driven approach,” *Journal of Informatics and Web Engineering* 3(2), 134–145 (2024), doi:10.33093/jiwe.2024.3.2.10.