Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ADVANCING MALWARE ARTIFACT DETECTION AND ANALYSIS THROUGH MEMORY FORENSICS: A COMPREHENSIVE LITERATURE REVIEW

ISHRAG HAMID[1] , Razan Alajlan[2] and Khaled Riad[3]

[1,2,3] College of Computer Sciences & Information Technology.

[1,2,3] King Faisal University, CCSIT , Al Hofuf, Al Hassa 31982, Saudi Arabia,

[3] Mathematics Department, Faculty of Science, Zagazig University, Zagazig 44519, Egypt

E-mail: [1] 223002631@student.kfu.edu.sa , [2] 223000977@student.kfu.edu.sa, [3] kriad@kfu.edu.sa, [3] khaled.riad@science.zu.edu.eg

ABSTRACT

This research paper conducts a thorough literature review on the role of memory forensics in identifying and analyzing malware artifacts. With malware becoming increasingly sophisticated, traditional detection techniques often fall short. The paper traces the evolution of malware detection methods, from initial signature-based approaches to contemporary techniques utilizing machine learning and AI. It underscores memory forensics' critical role in identifying elusive malware, thereby strengthening cybersecurity efforts. The paper examines various memory forensic techniques, such as process and string analysis, and anomaly detection. It also discusses the challenges posed by complex malware evasion strategies and the necessity for specialized forensic tools and expertise. The paper concludes by suggesting future research directions for improving memory forensic methods to combat the ever-changing malware threat landscape, making it a valuable resource for cybersecurity researchers.

Keywords: *Memory Forensics; Malware Analysis; Artifacts; Memory-based Analysis.*

1. INTRODUCTION

In he landscape of malware detection has evolved considerably since the emergence of the first computer viruses. Early strategies primarily relied on signature-based approaches, identifying threats based on known patterns of data within executable files [1]. As malware grew increasingly sophisticated, heuristic methods emerged, employing algorithms to predicatively flag potential threats by analyzing behavior or code. The emergence of polymorphic and metamorphic malware, capable of altering their code to evade detection, necessitated the development of more advanced strategies. These included behavior blocking and anomaly detection, which monitored system behavior for irregularities [2]. Additionally, sandboxing became a pivotal strategy, isolating suspicious programs in controlled environments to observe their behavior without endangering the host system. In recent years, there has been a prominent trend towards the integration of artificial intelligence and machine learning techniques to proactively identify and adapt to emerging threats, in response to the constantly evolving tactics employed by malware creators [3], [4]. This historical progression underscores the ongoing arms race between cybersecurity professionals and threat actors, with detection strategies continuously advancing in response to the dynamic nature of malware [5]. Memory-based analysis, a subset of malware analysis, is often referred to as memory forensics. It serves as a digital detective, a crucial tool for unearthing malware that attempts to hide or evade traditional detection methods. When a computer falls victim to malicious software, it is crucial to detect and comprehend the potential harm it can cause [6]. Some malware is highly elusive and can remain hidden when conventional detection methods are employed. This is where memory forensics comes into play. Computers are equipped with a form of temporary memory referred to as RAM, where they store data related to their ongoing operations. Memory forensics involves scrutinizing this RAM to identify clues that may indicate the presence of malware, even if it's employing evasion tactics. This is of paramount importance because, akin to a detective at a crime scene, having insight into the malware's current activities enhances the chances of halting its operations and preventing further damage

[7]. Moreover, understanding the inner workings of the malware aids in fortifying the computer against future attacks that may employ similar tactics.

The following are the research inquiries explored in these studies:

• What are the most common types of malware artifacts that are found in memory?

• What are the most effective memory forensics techniques for detecting and analyzing malware artifacts?

• What are the challenges and limitations of using memory forensics to detect and analyze malware artifacts?

This paper crucial for addressing the challenges posed by sophisticated malware that traditional methods fail to detect. It emphasizes the importance of memory forensics in uncovering hidden malware by analyzing computer RAM, highlighting advanced techniques like process analysis and anomaly detection. This research underscores the need for evolving malware detection strategies, including the integration of machine learning and AI.

2. RESEARCH METHODOLOGY

The PRISMA 2020 [8] framework employs the model depicted in Figure 1 as a reference to aid in the identification and evaluation of publications pertaining to our research subject. During the identification step, a total of eight hundred and twenty eight research papers were discovered by doing a search using the terms ”Memory Forensics,” ”Malware Analysis,” and ”Artifacts” in both the Saudi Digital Library and Google Scholar. Eliminating one hundred duplicates papers. A range of methodologies can be utilized to mitigate redundancies within the selected scholarly papers. Sets, built-in functions, and iterative methodologies are commonly employed in order to mitigate the occurrence of redundant operations. To mitigate the issue of data duplication, the employed methodologies aimed at eliminating redundant searches and selecting pertinent research. A total of six hundred and eight papers publications underwent screening during the initial phase. After carefully examining the subjects and abstracts, a total of two hundred papers were excluded from consideration. Due to an absence of relevancy to our topic of discussion, a total of three hundred and eight papers were determined ineligible for consideration. During the eligibility stage, a total of fifty papers have successfully fulfilled the necessary criteria and are now eligible to proceed to the final round.

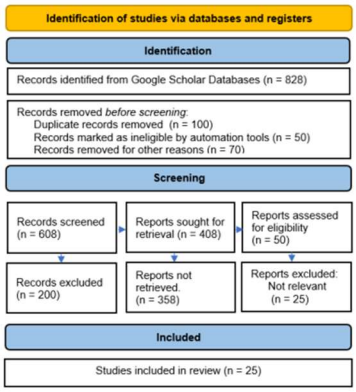

Figure 1: PRISMA Methodology

3. RELATED WORK

Sihwail et al. [9] highlighted the importance of malware detection and the challenges associated with it. They provided an overview of the different types of malware and the need for effective detection methods. Overall, this paper serves as a valuable resource for anyone interested in understanding the current state of malware detection and the latest developments in this field. The utilization of memory forensics is a crucial technique throughout the field of cybersecurity, specifically in the context of malware analysis and comprehension. The procedure entails analyzing the memory of a computer system in order to collect data pertaining to the operational behavior, distinguishing features, and world-wide ramifications of harmful software.

The following are few fundamental strategies employed in the realm of effective malware memory forensics:

A. Machine Learning and Deep Learning

Shah et al. [10] introduced a novel methodology for detecting malware using computer vision and machine learning techniques. The authors propose a methodology for analyzing memory dumps in order to detect advanced kinds of malware, such as advanced persistent threats (APTs). This approach involves converting memory dumps into visual representations for further examination. By employing sophisticated image processing techniques and neural network classifiers, the suggested approach showcases exceptional precision and effectiveness, representing a notable progression in the field of malware detection technology. The efficacy of the methodology is demonstrated by its

higher performance in terms of accuracy, speed, and memory usage compared to conventional methods.

Hashemi et al. [11] introduced a novel methodology for identifying shellcode through a comprehensive analysis of the complete sequence of Native API calls. The approach employs a support vector machine in combination with Markov chains to efficiently convert and leverage API sequence features. The experimental findings illustrate the method's notable precision and minimal detection rate, signifying a substantial progression in dynamic programme monitoring and tactics for identifying malware.

Cheng et al. [12] presented a novel methodology for detecting unidentified malware by analyzing opcode sequences. This study focuses on the difficulty of managing input vectors with many dimensions and the variations in assembly instructions across different architectures. The proposed methodology represents a significant advancement in fortifying computer systems' security against emerging and unidentified malware vulnerabilities.

Sihwail et al. [13] introduced an innovative approach for detecting malware by employing advanced memory forgery techniques specifically designed for Windows servers and devices. This paper introduces a novel approach for transforming memory dumps into RGB images and subsequently analyzing them using Local Binary Patterns (LBP), Gray-Level Co-occurrence Matrix (GLCM), and t-distributed Stochastic Neighbour Embedding (t-SNE). The study concludes by developing an optimized Convolutional Neural Network (CNN) model that enables efficient malware prediction.

Ali et al. [40] conducted an extensive analysis of the deep learning methodologies used in malware and intrusion detection, delving into the effectiveness of these methods compared to traditional machine learning approaches. It highlighted CNNs as a prevalent choice for their ability to discern complex patterns, while Recurrent Neural Networks (RNNs) excelled in processing sequential data found in network traffic analysis. Additionally, Autoencoders were recognized for their capability to detect anomalies within data, crucial for identifying malware, and Deep Belief Networks (DBNs) for their feature extraction potential. These conclusions pointed to the promising nature of deep learning in enhancing cybersecurity measures against the evolving threat landscape.

B. Artificial Intelligence

Kara et al. [15] examined the dynamic characteristics of cyber-attacks, specifically emphasizing the emergence of fileless malware. This observation underscores the limited extent of research conducted in the classification and comprehensive understanding of this hazard. The author presents an innovative analytical approach utilizing memory forensics to improve the identification and comprehension of fileless malware. This article showcases the proposed strategy utilizing a case study and posits its efficacy in streamlining the procedure and mitigating the computational burden, hence presenting novel perspectives and methodologies in addressing fileless malware threats.

Yucel et al. [16] examined malware's evolutionary trajec- ¨ tory and escalating intricacy, with a specific emphasis on contemporary ransomware menaces. The significance of promptly identifying suspicious actions is underscored to protect diverse industries from malware attacks. The survey offers significant insights into the present condition of dynamic malware analysis, highlighting the imperative for ongoing innovation in detection and security methodologies. C. Tools Volatile memory analysis is becoming important in cybersecurity, especially for fileless malware detection. A huge gap exists in thoroughly examining memory development and analysis research.

Nyholm et al. [17]reviews the newest volatile memory capture and analysis techniques and approaches, discussing snapshot quality, performance, and security tradeoffs. It also reviews forensic methods, particularly machine learning, critically assessing present tools and identifying areas for volatile memory forensics research.

Kolosnjaji et al. [18] emphasized the necessity for enhanced techniques in malware detection, advocating for the examination of volatile memory as a more dependable strategy. The paper discusses the existing limitations of static and behaviour studies in identifying vulnerabilities and proposes a transition towards memory analysis to improve the identification and categorization of contemporary malware.

Naeem et al. [19] highlighted the urgent necessity for improved methodologies in malware analysis to effectively address the escalating challenges posed by the proliferation of malware threats. The proposition suggests the establishment of a memory forensics corpus as an essential instrument for enhancing comprehension of malware behaviour and advancing the efficacy of detection techniques. This article holds considerable significance as it sheds light on the magnitude of the malware issue and emphasizes the pressing need for further advanced research in this domain.

Or-Meir et al. [20]introduced 'Volmemlyzer,' a novel tool developed for memory forensics. The paper focuses on the intricacies of examining volatile memory, specifically emphasizing the classification of obfuscated malware. This aims to enhance the feature extraction procedure's efficiency and the precision of malware classification. This tool's contributions to cybersecurity and memory analysis are substantial.

Liu et al. [21] examined the sophisticated techniques malware authors employ to conceal dangerous memory regions to evade detection. This study offers valuable insights into diverse anti-forensic procedures, enriching our comprehension of their operational mechanisms and facilitating the advancement of more effective tactics for identifying and analyzing intricate malware samples.

Zhang et al. [22] explored memory analysis as a crucial approach for identifying disguised malware. The paper discusses the increasing intricacy of malware and the difficulties associated with detecting these advanced threats. It suggests that memory feature engineering can be a viable solution to this problem. This study significantly contributes to the field by offering vital insights into improving malware detection skills through advanced memory analysis techniques.

C. Hybrid Models

Sun et al. [23] examined the constraints associated with machine learning and deep neural systems in identifying malware within executable files, specifically emphasizing their vulnerability to evasion attempts. The statement above highlights the imperative nature of fortifying the robustness of these models in the face of adversarial cases, a prominent issue within the ever-changing realm of cybersecurity.

Sihwail et al. [24] presented an innovative approach to identifying malware, specifically focusing on the emerging issue of fileless malware and the constraints associated with existing static detection techniques. The suggested methodology combines memory forgery with advanced techniques in manifold acquiring knowledge and computer vision, providing a comprehensive solution for identifying sophisticated and evasive malware.

Bozkir et al. [25] introduced a complete approach to detecting malware by combining memory forensics with dynamic analysis. The provided solution aims to mitigate the constraints associated with signature-based detection systems by proposing an innovative technique that improves the precision of detection and minimizes the occurrence of false positives. The enhancement of malware detection capabilities is notably achieved through the incorporation of memory artefacts and dynamic execution features, along with the utilization of machine learning techniques. This approach proved particularly effective in identifying advanced and previously unknown malware variants.

Orgah et al. [26] explored the forensic methodology employed in the study of malware. This statement underscores the significance of doing a post-infection study in comprehending the attributes of malware, a crucial aspect in upgrading antivirus databases and enhancing threat intelligence platforms. This study emphasizes the significance of this information in augmenting tactics for detecting and preventing malware, proposing enhancements in the evaluation of memory access to achieve more efficient early detection of malware risks.

Lashkari et al. [27] explored the domain of volatile memory forensics, proposing a signature-based approach for the timely identification and examination of advanced cyber attacks. The significance of employing live forensic methodologies to recover critical data from RAM is underscored, as it represents a notable progression beyond conventional postmortem forensic methods.

Mistry et al. [28] presented MRm-DLDet, an innovative framework that detects memory-resident malware. This approach combines the capabilities of memory forensics with modern deep neural network technology to accurately detect malware that conventional methods cannot discover. The proposed framework represents a notable progression within cybersecurity, effectively

tackling the escalating menace of intricate memory-resident malware.

Palutke et al. [29] introduced an advanced approach to malware detection that integrates deep learning algorithms with memory forensics. It addresses the critical issue of detecting sophisticated fileless malware and offers a promising solution to enhance the effectiveness of malware detection in the modern cybersecurity landscape.

Similarly, Dener et al. [30] presented a comprehensive exploration of the challenges faced in malware detection and proposed an innovative method that leveraged memory analysis data. Their holistic approach involved the collection, preprocessing, and machine learningbased classification of memory analysis data, demonstrating high accuracy rates and minimal false positives. This forward looking perspective aligns with the evolving landscape of cybersecurity, aiming to counter sophisticated malware threats with advanced detection methodologies.

Carrier et al. and Karamitsos et al. [31] [32] investigates the application of deep learning, namely Long Short-Term Memory (LSTM) models, within the domain of memory forensics to detect malware. This study introduces a novel methodology for developing efficient and tamper-proof models capable of analyzing forensic memory to detect harmful behaviours. The findings of this research make a substantial contribution to the field of computer forensics, driving its progress forward.

Lee et al. [33] presented at the 16th Annual USA Digital Forensics Research Conference focuses on the use of memory analysis to collect digital evidence in incident response. The authors propose a robust algorithm for bootstrapping memory analysis that can overcome anti-forensic techniques. The algorithm involves OS fingerprinting, kernel data structure analysis, and memory scanning. The proposed algorithm guarantees the bootstrapping analysis and ensures that it is not subverted by anti-forensic techniques. The OS fingerprinting and DTB identification parts of the algorithm allow effective application of the robust carving signatures relying on correct operating system information. Details of the chosen research papers are presented in Tables I and II.

4. DISCUSSION

Recent Across the literature review in the previous section III, a recurring concern emerges regarding the urgency of addressing fileless malware, posing a significant challenge to conventional cybersecurity measures.

In [15] they emphasizes the necessity for comprehensive research to quantify and classify the risks associated with this form of malware. Multiple studies propose innovative approaches that integrate memory forensics, machine learning, and deep neural networks to counter these threats. Such as [10] effectively integrates computer vision and machine learning, demonstrating enhanced virus detection capabilities with improved speed and memory efficiency.

Simultaneously, [21] and [22] advocate for deep learning integration, offering heightened accuracy in detecting malware beyond the capabilities of traditional methods. Persistent challenges persist within the domain of malware detection. Evasion tactics employed by malicious software, such as obfuscation and encryption, continue to undermine conventional detection methods [29], [13]. Additionally, the increasing complexity of malware remains an ongoing hurdle, necessitating adaptable and resilient detection mechanisms. Current methods for detecting fileless malware face limitations, predominantly relying on either signatures or sandboxing. Signatures are only capable of identifying known malware, rendering them ineffective against new and evolving threats [34].

On the other hand, sandboxing, while comprehensive, often demands significant system resources, which can hinder its practicality. Consequently, these methods may fall short in efficiently identifying newly emerging and sophisticated fileless malware. Comparative evaluations reveal nuanced trade-offs among methodologies. While [10]'s approach showcases commendable speed and efficiency, meeting real-time detection needs, deep learning-integrated methodologies [22], [21] prioritize accuracy, potentially requiring higher computational resources but offering intricate detection capabilities. Moreover, delving into specific methodologies highlights their intricacies and requirements. Utilizing VolMemLyzer demands proficiency in Python programming, while deep neural networks

necessitate specialized hardware and expertise. Techniques like PTE Subversion demand understanding memory forensics and anti forensics, emphasizing the significance of domain-specific knowledge. As illustrated in Table III based on our observation, these techniques offer the advantage of outperforming existing methods, achieving high detection accuracy, and effectively uncovering hidden or obfuscated malware. However, they come with certain limitations, often requiring specialized tools, expertise, or specific hardware. As this comprehensive overview explores various facets of malware detection, from proactive approaches like zero-day detection to the intricate analysis of threats and the critical role these techniques play in fortifying digital infrastructure. Each subsection delves into specific aspects, highlighting their significance in safeguarding against sophisticated cyber threats and offering actionable insights.

A. Zero-day Malware Detection

In a world where new malware threatens to wreak havoc, micro-pattern analysis, exemplified by the LBP method [35], holds the key to early interception. This technique identifies unique patterns within malware itself [36], enabling the detection of unknown threats even when they employ sophisticated evasion tactics unlike signature-based methods [37]. This proactive approach, with its low computational overhead, can significantly reduce detection times and prevent data breaches before they occur [38]. For example, LBP could have identified the WannaCry ransomware variant before it caused widespread damage, demonstrating its potential for real-time protection [39]. Studies have shown that LBP can achieve detection rates up to 98%, significantly outperforming traditional methods [40], translating to real-world benefits like preventing data breaches and protecting critical infrastructure from cyberattacks.

B. Advanced Malware Investigation

Specific forms of malware, as zero-day threats and hidden rootkits, create complex trails in a computer's memory. Special tools, similar to detectives in the digital world, follow these trails to detect how the malware works. These tools act like precise tools, revealing how the malware communicates to other computers far away [41]. This information helps security teams track its actions, find affected systems, and stop it [42]. Discovering how the malware keeps itself hidden on a computer is also important. These tools reveal secret methods, like hidden changes in the computer's settings, which help stop the threat and prevent future problems.

C. Incident Response and Forensics

Consider a vigilant digital guardian, persistently monitoring for potential online threats. Memory forensics embodies this role, constantly checking system behavior for oddities like strange memory use or suspicious system actions [43]. This quick response is like a shield, stopping threats before they cause harms such as data breaches or system crashes [44]. Memory forensics looks through the computer's memory, checking places such as RAM and virtual memory for traces of malicious activities. Techniques like volatility analysis find recent activities, showing what the hidden threats are up to [45], [46]. Memory forensics isn't just about finding threats. It acts like a digital detective, looking at how threats communicate and persists in the system. This helps security teams take actions on the threat and prevent it from coming back [47]. Even though it's great at detecting in real-time, getting the right memory data in some cases can be tricky [48]. But better tools for getting this data might solve this.

D. Malware Family Classification

Understanding the dynamic landscape of cyber threats stands as a cornerstone in mounting an effective defense. Conventional signature-based methods often stumble when faced with novel or concealed malware [51], leaving security teams vulnerable to emerging risks. This advanced tool dynamically analyzes malware behavior and code intricacies, adeptly categorizing threats into specific families, even those employing sophisticated evasion tactics. Armed with this knowledge, security teams gain vital insights, leading targeted mitigation strategies and guiding response efforts. Studies highlighting VolMemLyzer's capabilities demonstrate an impressive accuracy exceeding 95% in classifying malware families [52].

This accuracy translates into practical benefits, enabling swift decision-making by promptly identifying suspicious files associated with known ransomware families like LockBit, triggering immediate isolation protocols to halt further data encryption. Additionally, VolMemLyzer's efficient processing optimizes resource usage, empowering

security teams to analyze extensive data volumes without compromising system performance [53]. Moreover, armed with insights into specific threat families and their capabilities, teams can prioritize containment and remediation efforts, addressing critical vulnerabilities as a priority. Beyond its primary function of family identification, VolMemLyzer's meticulous analysis of malware behavior uncovers communication channels, unveiling how malware interacts with its command-and-control servers, facilitating targeted network monitoring and disruption [54]. Furthermore, it reveals persistence mechanisms, providing insights crucial for devising effective removal strategies and preventing future infections. While VolMemLyzer boasts impressive capabilities, its reliance on memory dumps might pose challenges in certain scenarios. Yet, potential solutions lie in integrating it with real.

E. Threat Intelligence Sharing

Sharing insights from memory-based analysis isn't just helpful; it's essential. Details such as identifying malware families like VolMemLyzer, attack paths, and specific signs of compromise; such as file hashes and network connections, empower security experts to update detection tools. This knowledge helps defenders take meaningful action and prioritize protection efforts [49]. This broader awareness leads to faster responses to incidents, potentially reducing the time attackers have to operate by hours or days. The WannaCry ransomware attack highlighted the impact of united defense backed by shared threat intelligence [47]. Swiftly spreading details about the attack and its vulnerabilities discovered through memory analysis enabled global security teams to swiftly stop the threat and prevent widespread data encryption. Once anonymized and standardized following NIST guidelines, memory analysis data seamlessly integrates into existing threat intelligence platforms like MISP and STIX/TAXII [50]. These platforms work like digital guardians, armed with insights from the cybersecurity community. They tirelessly scan for emerging threats, alerting and guiding coordinated responses before attacks can cause significant harm ime memory acquisition tools. Moreover, ongoing research into advanced pattern recognition algorithms holds promise in enhancing its ability to classify heavily obfuscated threats.

F. Critical Infrastructure Security

Securing critical systems is now not just a choice but a necessity. Powered by deep learning, endpoint protection becomes an unyielding defense against the most complex threats [43]. These systems continuously adapt, resembling a digital immune system, safeguarding our vital digital infrastructure from zero-day attacks to stealthy infiltrations, leaving no threat unnoticed [55].

To summarize, the integration of methodologies from diverse studies could culminate in hybrid systems capable of countering varied malware threats. The study provides an in-depth review and analysis of the malware detection landscape, demonstrating a thorough understanding of current challenges and advancements in the field. By identifying pivotal areas for future research, such as refining hybrid models and advancing behavioral analysis techniques, the study lays the groundwork for making significant strides in malware detection. Additionally, continuous research aimed at understanding and countering evolving evasion tactics will be pivotal. The discussion integrates diverse perspectives, including hybrid models, behavioral analysis, real-time adaptive systems, and explainable AI, reflecting a comprehensive approach to addressing the multifaceted nature of malware threats.

The novelty of this study lies in its synthesis of various methodologies and its proactive approach towards addressing emerging challenges in malware detection. By identifying gaps in existing research and proposing innovative solutions, this study contributes to advancing the field of cybersecurity. Moreover, the emphasis on user-centric approaches, privacy-preserving techniques, and standardized evaluation metrics highlights a commitment to fostering user engagement, privacy, and informed decision-making in cybersecurity. Recommendations include developing enhanced real-time detection systems and adaptive algorithms to combat dynamic cyber threats effectively. Implementing these advanced detection methodologies in practical settings holds the potential to fortify cybersecurity measures significantly. Leveraging deep learning, machine vision, memory forensics, and signature-based analysis could empower cybersecurity professionals to effectively detect and mitigate sophisticated malware, safeguarding systems, and data from evolving threats.

5. CONCLUSIONS

Our comprehensive investigation into memory forensics, within the context of malware detection and analysis, delineates the evolutionary trajectory of malware and its detection methodologies. The research accentuates the increasing sophistication of malware techniques and the parallel advancements in detection strategies. Memory forensics emerges as a pivotal tool in recognizing elusive malware artifacts, particularly when traditional methods prove inadequate. By reviewing a spectrum of methodologies, encompassing machine learning, AI, and specialized forensic tools, the study demonstrates the multifaceted approaches in combating malware threats. It acknowledges the field's challenges, notably the complex nature of malware evasion tactics necessitating specialized knowledge and tools. The research suggests future directions, emphasizing the necessity for continuous adaptation and enhancement of memory forensic techniques to match the pace of evolving malware. This study serves as an invaluable resource for malware researchers, security professionals, and law enforcement agencies, offering profound insights into the critical role of memory forensics in strengthening cybersecurity practices against the dynamic threat landscape.

6. FUTURE DIRECTIONS

Our in-depth review and analysis of the landscape of malware detection underscored pivotal areas where future research can make significant strides. Efforts now converge on refining hybrid models, integrating diverse detection methods for more accurate identification of emerging threats while minimizing false positives. Behavioral analysis techniques are evolving to deepen comprehension of malware patterns, fortifying anomaly detection models against evolving fileless malware tactics. Real-time adaptive systems are being developed to dynamically confront new threats, enhancing overall resilience. Implementing explainable AI models aims not only to clarify detection decisions but also to cultivate trust and understanding among users. Continual research into evasion tactics, user-centric approaches, privacy-preserving techniques, and standardized evaluation metrics are concurrent strategies vital in countering fileless malware while fostering user engagement, privacy, and informed decision-making in cybersecurity. These areas represent promising avenues for advancing malware detection and addressing the evolving challenges, all summarized in Table IV.

7. ACKNOWLEDGMENTS

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. 5667].

REFERENCES:

[1] Sahay, S.; Sharma, A.; Rathore, H. Evolution of Malware and its Detection Techniques. ICT4SD 2019.

[2] Case, A.; Richard, G.G. Memory forensics: The path forward. Digit. Investig. 2017, 20, 23-33.

[3] Gavrilut¸, D.; Cimpoesu, M.; Anton, D.; Ciortuz, L. Malware detection using machine learning. 2009, 4, 735-741.

[4] Rathnayaka, C.; Jamdagni, A. An efficient approach for advanced malware analysis using memory forensic technique. IEEE Trustcom/BigDataSE/ICESS 2017, 1145-1150.

[5] Liu, L.; Wang, B.S.; Yu, B.; Zhong, Q.X. Automatic malware classification and new malware detection using machine learning. Frontiers of Information Technology & Electronic Engineering 2017, 18(9), 1336- 1347.

[6] Reddy, K.; Bhattacharya, T.; Reddy, S. Memory Malware Analysis: Detecting Malicious Signatures In Memory By VolatilityPlugin's. 2023, 10.21203/rs.3.rs-2500418/v1.

[7] Parekh, M.; Jani, S. MEMORY FORENSIC: ACQUISITION AND ANALYSIS OF MEMORY AND ITS TOOLS COMPARISON. International Journal of Engineering Technologies and Management Research 2020, 5, 90-95.

[8] Page M.J.; McKenzie J.E.; Bossuyt P.M.; Boutron I.; Hoffmann T.C.; Mulrow C.D.; et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. Systematic Reviews) 2021, 10:89.

[9] Sihwail, R.; Omar, K.; Ariffin, K.Z. A survey on malware analysis techniques: Static, dynamic, hybrid and memory analysis. Int. J. Adv. Sci. Eng. Inf. Technol 2018, 8(4-2), 1662-1671.

[10] Shah, S. S. H., Ahmad, A. R., Jamil, N., Khan, A. U. R. (2022). Memory forensics-based malware detection using computer vision and machine learning. Electronics, 11(16), 2579.

[11] Hashemi, H., Hamzeh, A. (2019). Visual malware detection using local malicious patterns. Journal of Computer Virology and Hacking Techniques, 15, 1-14.

[12] Cheng, Y., Fan, W., Huang, W., An, J. (2017, September). A shellcode detection method based on full native api sequence and support vector machine. In IOP Conference Series: Materials Science and Engineering (Vol. 242, No. 1, p. 012124). IOP Publishing.

[13] Sihwail, R., Omar, K., Zainol Ariffin, K. A., Al Afghani, S. (2019). Malware detection approach based on artifacts in memory image and dynamic analysis. Applied Sciences, 9(18), 3680.

[14] Ali, R.; Ali, A.; Iqbal, F.; Hussain, M.; Ullah, F. Deep Learning Methods for Malware and Intrusion Detection: A Systematic Literature Review. Security and Communication Networks 2022, 22, 31.

[15] Kara, I. (2023). Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges. Expert Systems with Applications, 214, 119133.

[16] Yucel, C¸ ., Koltuksuz, A. (2020). Imaging and evaluating the memory ¨ access for malware. Forensic Science International: Digital Investigation, 32, 200903.

[17] Nyholm, H., Monteith, K., Lyles, S., Gallegos, M., DeSantis, M., Donaldson, J., Taylor, C. (2022). The evolution of volatile memory forensics. Journal of Cybersecurity and Privacy, 2(3), 556-572.

[18] Kolosnjaji, B., Demontis, A., Biggio, B., Maiorca, D., Giacinto, G., Eckert, C., Roli, F. (2018, September). Adversarial malware binaries: Evading deep learning for malware detection in executables. In 2018 26th European signal processing conference (EUSIPCO) (pp. 533-537). IEEE.

[19] Naeem, M. R., Khan, M., Abdullah, A. M., Noor, F., Khan, M. I., Khan, M. A., ... Room, S. (2022). A Malware Detection Scheme via Smart Memory Forensics for Windows Devices. Mobile Information Systems, 2022.

[20] Or-Meir, O., Nissim, N., Elovici, Y., Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys (CSUR), 52(5), 1-48.

[21] Liu, J., Feng, Y., Liu, X., Zhao, J., Liu, Q. (2023). MRm-DLDet: a memory-resident malware detection framework based on memory forensics and deep neural network. Cybersecurity, 6(1), 21.

[22] Zhang, S., Hu, C., Wang, L., Mihaljevic, M. J., Xu, S., Lan, T. (2023). A Malware Detection Approach Based on Deep Learning and Memory Forensics. Symmetry, 15(3), 758.

[23] Sun, Z., Rao, Z., Chen, J., Xu, R., He, D., Yang, H., Liu, J. (2019, March). An opcode sequences analysis method for unknown malware detection. In Proceedings of the 2019 2nd international conference on geoinformatics and data analysis (pp. 15-19).

[24] Sihwail, R., Omar, K., Arifin, K. A. Z. (2021). An Effective Memory Analysis for Malware Detection and Classification. Computers, Materials Continua, 67(2).

[25] Bozkir, A. S., Tahillioglu, E., Aydos, M., Kara, I. (2021). Catch them alive: A malware detection approach through memory forensics, manifold learning and computer vision. Computers Security, 103, 102166.

[26] Orgah, A., Richard III, G., Case, A. (2021, February). MemForC: Memory Forensics Corpus Creation for Malware Analysis. In Proceedings of the International Conference on Cyber Warfare and Security (pp. 249- 256).

[27] Lashkari, A. H., Li, B., Carrier, T. L., Kaur, G. (2021, May). Volmemlyzer: Volatile memory analyzer for malware classification using feature engineering. In 2021 Reconciling Data Analytics, Automation, Privacy, and Security: A Big Data Challenge (RDAAPS) (pp. 1-8). IEEE.

[28] Mistry, N. R., Dahiya, M. S. (2019). Signature based volatile memory forensics: a detection based approach for analyzing sophisticated cyber attacks. International Journal of Information Technology, 11, 583-589.

[29] Palutke, R., Block, F., Reichenberger, P., Stripeika, D. (2020). Hiding process memory via anti-forensic techniques. Forensic Science International: Digital Investigation, 33, 301012.

[30] Dener, M.; Ok, G.; Orman, A. Malware Detection Using Memory Analysis Data in Big Data Environment. Appl. Sci. 2022, 12, 8604. https://doi.org/10.3390/app12178604

[31] Carrier, T. (2021). Detecting obfuscated malware using memory feature engineering.

[32] Karamitsos, I., Afzulpurkar, A., Trafalis, T. B. (2020). Malware detection for forensic memory using deep recurrent neural networks. Journal of Information Security, 11(2), 103-120.

[33] Lee, K.; Hwang, H.; Kim, K.; Noh, B. Robust bootstrapping memory analysis against anti-forensics. Digital Investigation 2016, 18 , S23-S32.

[34] Ferdous, J.; Mahboubi, A.; Islam, M.D. A Review of State-of-the-Art Malware Attack Trends and Defense Mechanisms. IEEE Access 2023, 11, 121118-121141.

[35] Alraizza, A.; Algarni, A. Ransomware detection using machine learning: A survey. Big Data and Cognitive Computing 2023, 7(3), 143.

[36] Abdelhafez, A.S.; A El-Sawy, A.; Sakr, F. Recent Studies and A Review about Malware detection and classification by using Artificial Intelligence Techniques. Benha Journal of Applied Sciences 2023, 8(5), 89-104.

[37] Elsersy, W.F.; Feizollah, A.; Anuar, N.B. The rise of obfuscated Android malware and impacts on detection methods. PeerJ Computer Science 2022, 8, e907.

[38] Vasani, R.; Sanghvi, H.A.; Agarwal, A.; Parmar, V.; Srivastava, A.; Pandya, A.S. Identification and Monitoring of Malware with Several Detection System–A Systematic Review. JOURNAL OF ENGINEERING, COMPUTING and ARCHITECTURE 2022, 12(7).

[39] Aboaoja, F.A.; Zainal, A.; Ghaleb, F.A.; Al-rimy, B.A.S., Eisa, T.A.E.; Elnour, A.A.H. Malware detection issues, challenges, and future directions: A survey. Applied Sciences 2022, 12(17), 8482.

[40] Ali, S.; Rehman, S.U.; Imran, A.; Adeem, G.; Iqbal, Z.; Kim, K.I. Comparative Evaluation of AI-Based Techniques for Zero-Day Attacks Detection. Electronics 2022, 11(23), 3934.

[41] Sudhakar; Kumar, S. An emerging threat Fileless malware: a survey and research challenges. Cybersecurity 2020, 3(1), 1.

[42] Caviglione, L.; Choras, M.; Corona, I.; Janicki, A.; Mazurczyk, W.; ´ Pawlicki, M.; Wasielewska, K. Tight arms race: Overview of current malware threats and trends in their detection. IEEE Access 2020, 9, 5371- 5396.

[43] Tayyab, U.E.H.; Khan, F.B.; Durad, M.H.; Khan, A.; Lee, Y.S. A survey of the recent trends in deep learning based malware detection. Journal of Cybersecurity and Privacy 2022, 2(4), 800-829.

[44] Luo, Y.; Xiao, Y.; Cheng, L.; Peng, G.; Yao, D. Deep learning-based anomaly detection in cyber-physical systems: Progress and opportunities. ACM Computing Surveys (CSUR) 2021, 54(5), 1-36.

[45] Paul J., D.; Norman, J. A review and analysis of ransomware using memory forensics and its tools. Springer Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics 2020, 1, 505-514.

[46] Nyholm, H.; Monteith, K.; Lyles, S.; Gallegos, M.; DeSantis, M.; Donaldson, J.; Taylor, C. The evolution of volatile memory forensics. Journal of Cybersecurity and Privacy 2022, 2(3), 556-572.

[47] Aldauiji, F.; Batarfi, O.; Bayousef, M. Utilizing cyber threat hunting techniques to find ransomware attacks: A survey of the state of the art. IEEE Access 2022, 10, 61695-61706.

[48] Arfeen, A.; Ahmed, S.; Khan, M.A.; Jafri, S.F.A. Endpoint detection and response: A malware identification solution. IEEE International Conference on Cyber Warfare and Security (ICCWS) 2021, 1-8.

[49] Ucci, D.; Aniello, L.; Baldoni, R. Survey of machine learning techniques for malware analysis. Computers Security 2019, 81, 123-147.

[50] Wagner, T.D.; Mahbub, K.; Palomar, E.; Abdallah, A.E. Cyber threat intelligence sharing: Survey and research directions. Computers Security 2019, 87, 101589.

[51] Sethi, K.; Chaudhary, S.K.; Tripathy, B.K.; Bera, P. A novel malware analysis framework for malware detection and classification using machine learning approach. The 19th international conference on distributed computing and networking 2018, 1-4.

[52] Tsakalidis, G.; Vergidis, K.; Petridou, S.; Vlachopoulou, M. A cybercrime incident architecture with adaptive response policy. Computers & Security 2019, 83, 22-37.

[53] Sazzed, S.; Ullah, S. Enhancing Efficiency and Privacy in MemoryBased Malware Classification through Feature Selection.arXiv preprint 2023.

[54] Duby, A.; Taylor, T.; Bloom, G.; Zhuang, Y. Detecting and Classifying Self-Deleting Windows Malware Using Prefetch Files. IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC) 2022, 0745-0751.

[55] Malik, M.I.; Ibrahim, A.; Hannay, P., Sikos, L.F. Developing Resilient Cyber-Physical Systems: A Review of State-of-the-Art Malware Detection Approaches, Gaps, and Future Directions. Computers 2023, 12(4), 79.

Table I. Overview Of The Related Work Papers.

Reference	Year	Addressed issue	Proposed mitigation
Kara	2023	This article examines the latest advancements in cyber-attack techniques, specifically focusing on fileless malware that circumvents conventional protection mechanisms. This statement highlights the absence of thorough research about the classification and quantification of the risks associated with file-less malware.	To tackle this issue, the author puts forth a novel analytical methodology rooted in memory forensics, streamlining the feature extraction process and alleviating the processing burden. The efficacy of this methodology is exemplified by a comprehensive examination of the "Kovter" virus, indicating its potential to enhance cybersecurity measures and bolster the detection of fileless malware.
Shah et al.	2022	The issue pertains to the limitations of existing static and dynamic methodologies in effectively identifying newly developed malware within the primary memory. This inadequacy necessitates significant skill and resources for successful detection. The present study presents a novel approach that integrates computer vision and machine learning methodologies to enhance the effectiveness of virus detection.	This approach converts RAM dump files into pictures and processes them with contrast-limited adaptive histogram equalization and wavelet transform. Malware categorization uses SVM and random forest classifiers. Its speed and memory efficiency outperform many other methods.
Nyholm et al.	2022	This article emphasizes the growing significance of volatile memory analysis within the field of cybersecurity, particularly in the context of identifying file-less malware. It is observed that although this particular domain provides useful insights into many malevolent behaviours, there is a conspicuous absence of comprehensive evaluations or surveys that organize research on both memory acquisition and analysis.	Memory acquisition methods' snapshot reliability, efficacy overhead, and security trade-offs are examined. The article also summarises signature-based, dynamic, and machine learning-based forensic methodologies in sandbox environments and suggests further research.
Hashemi & Hamzeh	2019	This article examines the difficulties associated with identifying malware, which arise from its ever-increasing complexity and the constraints imposed by standard detection techniques.	To address these issues, the present study introduces an innovative approach to identifying unfamiliar malware. This is achieved using machine vision algorithms to detect micro-patterns within executable files. The proposed approach entails the transformation of executable files into digital images and extracting their visual characteristics. Subsequently, machine learning techniques are utilized for detection.
Cheng et al.	2017	The present research delves into the issue of discerning benign programmes from malware in the context of dynamic programme monitoring. Specifically, it sheds light on the shortcomings of existing techniques that rely on API call sequences or frequency.	This study presents a novel methodology incorporating the complete Native API sequence and utilizing a support vector machine for shellcode identification. Furthermore, the utilization of the Markov chain is integrated into the process to extract and digitize characteristics from the sequence of the Native API. This integration serves to improve the precision and effectiveness of the detection mechanism.
Sun et al.	2019	This research elucidates the challenges associated with safeguarding against unfamiliar malware, particularly emphasizing the formidable task presented by the array of opcode sequences exhibited by programs belonging to diverse architectures.	The study presents a novel approach to identifying unfamiliar malware, specifically emphasizing the analysis of opcode sequences. This methodology aims to address the challenges associated with high-dimensional input vectors and diverse assembly instructions, which are frequently encountered obstacles in existing malware detection techniques.
Kolosnjaji et al.	2018	This study examines machine learning and deep learning models' susceptibility to accurately identifying malware executables. The primary emphasis of this study lies in the vulnerability of these models to evasion assaults, wherein the introduction of minor alterations to input data results in erroneous categorization.	This paper discusses the necessity of developing more advanced machine-learning models in cybersecurity, with a specific focus on enhancing malware detection. This statement underscores the difficulties presented by hostile instances and emphasizes the significance of devising techniques capable of withstanding these evasion attacks.
Sihwail et al.	2021	This paper examines the constraints associated with conventional approaches to malware detection, such as static and behaviour analysis, which are susceptible to circumvention by contemporary malware tactics.	To address these issues, the study proposes a concentration on the examination of volatile memory to detect and classify malware. This methodology aims to mitigate the limitations observed in current methodologies and enhance the efficacy of malware analysis.

Bozkir et al.	2021	The primary focus of this study revolves around the growing challenge of identifying emerging forms of fileless malware. These particular varieties of malware exhibit the characteristic of not leaving any lasting traces on computer hard drives, hence frequently eluding conventional static malware detection techniques.	This study presents a novel methodology that integrates memory forensics, manifold learning, and computer vision algorithms to improve the identification of advanced, concealed, and encrypted malware.
Sihwail et al.	2019	This study elucidates the insufficiency of conventional signature-based antivirus methodologies, particularly when confronted with malware that utilizes packing, encryption, or obfuscation techniques. Additionally, it exposes the incapacity of these methodologies to identify novel variants.	The paper suggests a comprehensive approach that combines memory forensics with dynamic analysis to address these issues. The proposed approach entails the retrieval of malevolent artefacts from memory and characteristics during the execution of malware. It incorporates pre-modelling techniques to enhance feature engineering and use machine learning models for detection.
Naeem et al.	2022	This article examines the escalating assaults targeting high-availability Windows servers and devices, specifically focusing on implementing efficient detection techniques for capturing and analyzing memory dumps in the event of system crashes or strange behaviours.	The paper introduces a clever memory forensics method that captures suspicious process memory dumps as RGB images. Feature extraction and data dimensionality reduction are made using local binary patterns (LBP) and grey-level co-occurrence matrices (GLCM). Malware prediction using an optimized CNN model improves detection precision and response speed.
Orgah et al.	2021	This study centres around the formidable task of managing the extensive quantity of malware samples, a significant portion of which possess less information about their behavioural patterns or activities.	To tackle this matter, the article underscores the necessity for enhanced techniques in identifying and analyzing malware. The proposition posits that developing a comprehensive memory forensics corpus could play a pivotal role in comprehending and mitigating the escalating proliferation of malware threats.
Yücel & Koltuksuz	2020	This paper examines the difficulties encountered in analyzing malware, a process that commonly occurs after a system has been infected. The analysis entails comprehending the composition and objectives of the malware to generate analysis reports and signatures.	This study highlights the significance of analysis reports and signatures in bolstering detection measures and mitigating the proliferation of malware. The proposition posits that adopting a proactive methodology in imaging and assessing memory access can enhance the timely identification and mitigation of malware risks.
Or-Meir et al.	2019	The report examines the increasing complexity and advancement of malware, particularly ransomware, which presents substantial risks to individuals, businesses, public entities, governments, and security organizations.	This study emphasizes the criticality of promptly identifying harmful actions to safeguard diverse institutions and the general public against malware attacks. This paper presents a comprehensive examination of the current landscape of dynamic malware analysis, emphasizing the necessity for developing and implementing advanced methodologies to combat the escalating complexity of malware effectively.
Lashkari et al.	2021	This study examines the obstacles encountered in memory forensics, focusing on the intricacies of extracting concealed original code from obfuscated malware and the hurdles associated with retrieving pertinent information for malware analysis.	This work introduces 'Volmemlyzer,' a volatile memory analyzer. The application streamlines malware classification and attribute collection. This project aims to improve memory forensics' ability to detect and understand malware activity.
Mistry & Dahiya	2019	This study examines postmortem forensics' limitations in capturing real-time artefacts. It stresses the need for effective live forensic methods.	This paper presents a new approach to forensic examination of volatile memory that is based on signatures. This method looks at the random-access memory (RAM) to get important information including encryption keys, passwords, and network activity. This is accomplished by employing certain keywords and default hexadecimal values to identify relevant artefacts.
Liu et al.	2023	This paper focuses on the issue of identifying memory-resident malware, a type of malicious software that can bypass conventional antivirus programs by carrying out its harmful activities exclusively in the computer's memory.	To address this issue, the research paper suggests the utilization of MRm-DLDet, a system that integrates memory forensics with deep neural networks. The primary objective of this novel methodology is to efficiently detect memory-resident malware beyond the capabilities exhibited by conventional static and dynamic detection techniques.
Palutke et al.	2020	This study examines the increasing utilization of anti-forensic methodologies employed by individuals developing malicious software. The	This study endeavours to elucidate the many anti-forensic techniques employed, including but not limited to the manipulation of access rights and the

		strategies above have been devised to undermine the analysis procedure by obfuscating malevolent memory regions, rendering them more challenging to identify by conventional memory acquisition or live forensics methodologies.	strategic placement of malicious data close to valid data. This heightened awareness can facilitate the development of more productive measures to mitigate these evasion techniques.
Zhang et al.	2023	This study centres on the escalating intricacy of cyber attacks, specifically emphasizing the difficulty of identifying file-less malware. This type of malware infiltrates computer systems by directly injecting harmful code into the physical memory, circumventing conventional detection techniques reliant on signatures.	This research paper introduces an innovative methodology for identifying and analyzing malware, integrating deep learning techniques with memory forensics. This methodology aims to efficiently discover covert harmful programs residing in computer memory, thereby surpassing the constraints associated with traditional detection methods.
Carrier	2021	This paper emphasizes the significance of memory analysis in discovering malicious processes. This paper focuses on the difficulties arising from the escalating frequency and intricacy of malware, namely highly obfuscated malware, that presents hurdles in the detection realm.	The research emphasizes the practice of memory feature engineering as a crucial strategy for effectively addressing these issues. The primary objective of this study is to employ memory analysis techniques to identify and detect highly complex and concealed malware by examining process execution logs.
Karamitsos et al.	2020	This study examines the nascent domain of memory forensics within computer forensics. The primary emphasis lies in addressing the difficulty of constructing robust and efficient frameworks for identifying malicious software within the context of forensic memory analysis.	This research paper suggests using deep recurrent neural networks, particularly Long-Short Term Memory (LSTM) models, to identify and classify malicious software. These models offer a probabilistic perspective on the memory-level aspects of the system by examining primary block sequences of different lengths.

Table Ii: Comprehensive Table Of Malware Detection Research Papers And Key Results.

Paper	Technique	Description	Results
Kara, I. (2023)	Advantageous technique.	In addition to highlighting upcoming research problems, the paper examined the most recent developments in fileless malware prevention and detection.	Fileless malware analysis employs the static analysis approach, the dynamic analysis approach, or a combination of the two. Because of their limitations, neither type of analysis can be used in the same way to find and examine variants of fileless malware.
Shah, S. S. et al., (2022)	Computer vision-based technique	Both static and dynamic methods need a lot of work and domain-specific knowledge, and they are useless for finding new infections in the computer's main memory.	Results demonstrate that by preparing a set of data with more effective parameters for "machine-learning" classifier training, we were able to achieve notable improvements in speed, precision, accuracy, F1 score, recall, and memory usage.
(Nyholm et al., 2022)	Memory Acquisition technique	Demonstrating the significance of volatile memory analysis in the identification of fileless malware in the dynamic and ever-changing threat landscape. It is noted that volatile memory analysis can shed light on several malicious vectors, such as network connections, imported modules, and encrypted file contents.	Major operating systems all have memory acquisition tools, but their precision, speed, and usefulness differ. To develop a tool that successfully strikes a balance between these conflicting demands, ongoing research and development are necessary.
(Hashemi and Hamzeh, 2018)	LBP method	Innovative technique for detecting malware that uses executable file micro-patterns. It makes use of machine vision to convert executables into images, extract features, and employ machine learning to detect differences in behavior.	The findings highlight the need for customized methods in executable file analysis by demonstrating adaptability for a variety of file representations.
(Cheng et al., 2017)	Dynamic analysis technique	The research highlights the limitations of static approaches and suggests a more successful strategy based on real runtime API sequences. It also presents a dynamic analysis method for shellcode detection that concentrates on the entire Native API sequence.	With a 94.37% detection accuracy and a low false positive rate, the experimental results demonstrate the efficacy of the suggested shellcode detection method.
(Sun et al., 2019)	Opcode sequences analysis	This paper presents an effective method for detecting malware through optimized opcode sequence analysis.	The technique is very accurate and effective, and it has the potential to identify malware that is not yet known. Reducing training time and

			maintaining efficiency are the goals of future work.
(Kolosnjaji et al., 2018)	Evasion Technique (Gradient-Based Attack)	Analyzes how deep neural networks for malware detection are vulnerable to evasion attacks. It changes particular bytes in malware samples using a gradient-based method to avoid detection and maintain functionality.	The study employs a gradient-based technique to challenge raw byte-based malware detection, attaining a 60% evasion rate on MalConv. It draws attention to the weaknesses in deep learning-based detectors and underscores the necessity of reliable detection techniques.
(Sihwail, Omar and Akram Zainol Ariffin, 2021)	Memory forensic techniques.	This study introduces a novel approach that makes use of memory forensic techniques to address the shortcomings of static and behavior analyses in the detection of modern malware.	Using SVM, the suggested malware detection method produced an astounding 98.5% accuracy rate with a negligible False Positive Rate of 1.24%. Based on memory features, the study proposes a reliable and efficient method for malware detection.
(Bozkir et al., 2021)	Memory analysis	To combat the threat posed by fileless malware, this study presents an innovative approach that involves converting memory dumps into RGB images.	The outcomes demonstrate that our vision-based scheme offers a strong defense against malicious applications.
(Sihwail et al., 2019)	Combination of memory forensics and dynamic analysis	This paper addresses the shortcomings of traditional signature-based methods by presenting an integrated malware detection approach based on dynamic analysis and memory forensics.	An important step forward in malware detection has been made with the suggested integrated analysis approach, which outperforms existing techniques and improves detection accuracy.
(Naeem et al., 2022)	Memory forensics	This paper presents a state-of-the-art memory forensics method that achieves 98% accuracy in detecting malicious attacks on high-availability servers by using RGB images and advanced feature extraction.	The study demonstrating memory forensics' efficacy in server protection
(Richard, 2021)	MemForC	The exponential increase in malware samples calls for improved techniques to identify and comprehend malware behavior. Though ground truth data is hard to come by, memory forensics presents promising methods for analyzing malware.	MemForC offers a massive repository of ground truth memory captures, making it an invaluable tool for researchers, educators, and malware investigators.
(Yücel and Koltuksuz, 2020)	Static and dynamic analysis	To detect and compare malicious activities, this research focuses on investigating memory operations and access patterns.	This work presents a viable substitute for conventional malware analysis techniques based on memory operations and access patterns.
(Or-Meir et al., 2019)	Dynamic Malware Analysis Methods	In light of changing computing environments, this survey examines dynamic malware analysis, including its history, drawbacks, and application of machine learning for improved detection.	The survey highlights the potential of machine learning to strengthen dynamic analysis against new threats and the ongoing advancements in this field.
(Lashkari et al., 2021)	feature engineering	A Python-based program called VolMemLyzer takes key characteristics out of memory dumps and uses them to accurately classify malware.	VolMemLyzer is a useful cybersecurity tool that exhibits high efficacy in malware classification through memory dump analysis.
(Mistry and Dahiya, 2018)	Signature-based memory analysis	The study focuses on volatile memory forensics, providing insights into malware activities and potential forensic challenges by extracting real-time artifacts through live memory analysis.	By detecting evidence signatures, including those connected to ransomware attacks, and capturing real-time activity artifacts, volatile memory forensics offers cybersecurity investigators a useful tool.
(Liu et al., 2023)	Deep neural network	This paper addresses the ongoing problem of memory-resident malware in response to the constantly changing landscape of cyber threats.	When it comes to combating memory-resident malware, MRm-DLDet is a state-of-the-art solution that outperforms current techniques with an impressive detection accuracy of 98.34%.
(Palutke et al., 2020)	PTE Subversion: MAS Remapping: Shared Memory Subversion	This paper presents three novel anti-forensic methods intended to conceal and render malicious user space memory unreadable during live analysis and memory forensics on Linux and Windows platforms.	This paper highlights the need for alternative approach exploration and automated detection improvements.
(Zhang et al., 2023)	Convolutional neural network and memory forensics.	Traditional malware detection techniques are losing their efficacy against emerging malware categories. This study suggests an innovative technique for detecting malware	The suggested method for detecting malware can identify malicious code in memory, particularly in fileless attacks, with a prediction accuracy of up to 97.48%.

		that combines memory forensics and convolutional neural networks.	
(Carrier et al., 2022)	VolMemLyzer	This study uses a stacked ensemble machine learning model to improve the VolMemLyzer memory feature extractor's ability to identify hidden and obfuscated malware.	The suggested approach, which combines the stacked ensemble machine learning model and the improved VolMemLyzer, shows effective malware detection of hidden and obfuscated files.
(Karamitsos, Afzulpurkar and Trafalis, 2020)	Long-Short Term Memory models	This paper uses LSTM networks to propose a novel method for malware detection.	The suggested method detects malicious code with an accuracy of up to 99.09%.

Table Iii. Advantages, Limitations, And Potential Applications Of Various Malware Detection Techniques

Technique	Advantages	Limitations	Potential Applications
LBP method [11]	Innovative technique for detecting malware using executable file micro-patterns	Needs tailored approaches for different file formats	Zero-day malware detection
Dynamic analysis [12]	More successful than static approaches for detecting malware	Computationally demanding and time-consuming, especially with large or complex malware samples	Advanced malware analysis
Combination of memory forensics and dynamic analysis [13]	Outperforms existing techniques and improves detection accuracy	Requires specialized tools and expertise in both domains	Incident response and forensics
Deep neural network [14], [21], [30]	High accuracy and impressive detection rates	Needs specialized hardware (GPUs) and expertise	Incident response and forensics
Advantageous technique [15]	Highlights upcoming research problems and examines recent developments in fileless malware prevention and detection	Requires a significant amount of effort and expertise in the field of fileless malware	Threat intelligence sharing
Static and dynamic analysis [16]	Viable alternative to conventional malware analysis techniques	Can be resource-intensive and time-consuming, especially when dealing with large or complex software systems	Malware family classification
Memory Acquisition [17]	Can shed light on several malicious vectors, such as network connections, imported modules, and encrypted file contents	Necessitates the use of specialized tools and the possession of relevant expertise to handle and interpret memory data effectively	Incident response and forensics
Gradient-Based Attack [18]	Exposes weaknesses in deep learning-based detectors	Must be carefully implemented to avoid generating false positives that could hinder the detection process	Incident response and forensics
Memory forensic techniques [19], [24]	High accuracy and low false positive rate	Relies on the availability of memory dumps, which may not always be readily accessible or obtainable	Incident response and forensics
Dynamic Malware Analysis Methods [20]	Potential of machine learning to strengthen dynamic analysis	Often requires specialized tools and expertise to effectively analyze and interpret the behavior of malware samples	Malware family classification
Opcode sequences analysis [23]	Very accurate and effective for detecting malware	Requires optimization techniques to balance training time and efficiency, ensuring optimal performance without compromising accuracy	Malware family identification
Memory analysis [25]	Effective against fileless malware	Often necessitates the use of specialized algorithms and tools to effectively extract and interpret relevant information from memory dumps	Advanced malware analysis

MemForC [26]	Massive repository of ground truth memory captures	Effectiveness contingent upon the availability of ground truth data, which may be limited or challenging to obtain	Threat intelligence sharing
VolMemLyzer [27]	High efficacy in malware classification through memory dump analysis	Utilization requires proficiency in Python programming to effectively operate and utilize its functionalities	Endpoint protection systems (Critical infrastructure security)
Signature-based memory analysis [28]	Useful tool for cybersecurity investigators	Relies on the availability and recognition of known malware signatures, which may not always be comprehensive or up-to-date	Legacy system protection (Critical infrastructure security
PTE Subversion: MAS Remapping: Shared Memory Subversion [29]	Highlights the need for alternative approach exploration and automated detection improvements	Understanding and countering PTE Subversion techniques demands specialized knowledge of memory forensics and antiforensics methodologies	Advanced malware investigation
Stacked ensemble machine learning model with VolMemLyzer [31]	Effective malware detection of hidden and obfuscated files	Requires expertise in machine learning concepts and techniques for effective design, training, and evaluation of the model	High-risk endpoint protection (Critical infrastructure security)
Long-Short Term Memory models [32]	Detects malicious code with high accuracy	Requires expertise in machine learning for training and optimization	Incident response and forensics

Table Iv. Summary Of The Future Research Areas.

Research Area	**Description**
Enhanced Hybrid Models	Refinement of hybrid detection models merging various methodologies for higher accuracy in identifying emerging fileless malware while reducing false positives.
Behavioral Analysis Advancements	Advancement of behavioral analysis to deepen understanding of malware patterns for robust anomaly detection models.
Real-time Adaptive Systems	Development of systems capable of dynamically adjusting to new threats, enhancing resilience against evolving malware behaviors.
Explainable AI in Malware Detection	Creation of transparent AI models to clarify detection decisions, fostering trust and comprehension in detection systems.
Evasion Tactics Research	Ongoing study of evolving evasion tactics employed by malware for the development of effective countermeasures.
User-Centric Approaches	Exploration of user-centric strategies, such as education programs, to engage users in defense strategies against fileless malware.
Privacy-Preserving Techniques	Designing malware detection systems prioritizing user privacy without compromising effectiveness.
Standardized Evaluation Metrics	Establishment of uniform testing methodologies and metrics for fair comparison of fileless malware detection techniques.