JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Intelligent RAM Analysis Using ML for Detection and Prevention of Fileless Malware

[1]Meghana G Deshmukh, [2]Mounika T, [3]Parvati Waladunki, [4]Puneetha G, [5]Dr. Deepthi V S

[1]Student, [2]Student, [3]Student, [4]Student, [5]Assistant Professor
[1,2,3,4,5]Computer Science Engineering (Cyber-Security)
[1,2,3,4,5]Dayananda Sagar College of Engineering, Bengaluru, India

Abstract : Fileless malware is one of today is most persistent threats to cybersecurity. Nevertheless, it works perfectly in computer memory without transferring any files to the hard drive. Standard antivirus programs have a very difficult time identifying that configuration using their standard pattern matching techniques. Furthermore, in this paper, we investigate a machine learning-based approach. Hence, the primary goal is to identify these threats using hints in temporary memory and the system is overall behavior. Therefore, our recommended configuration retrieves data from RAM using tools such as the Volatility framework.. Following that, it extracts relevant data and employs a variety of algorithms to detect unusual behavior. Tests show how well the system can distinguish between good and bad operations. It maintains a low false alarm rate while providing excellent accuracy. The study demonstrates how smart systems that monitor memory can strengthen corporate security configurations and improve prompt responses to threats.

IndexTerms **- Fileless malware, memory forensics, machine learning, threat detection, Volatility, system behaviour analysis.**

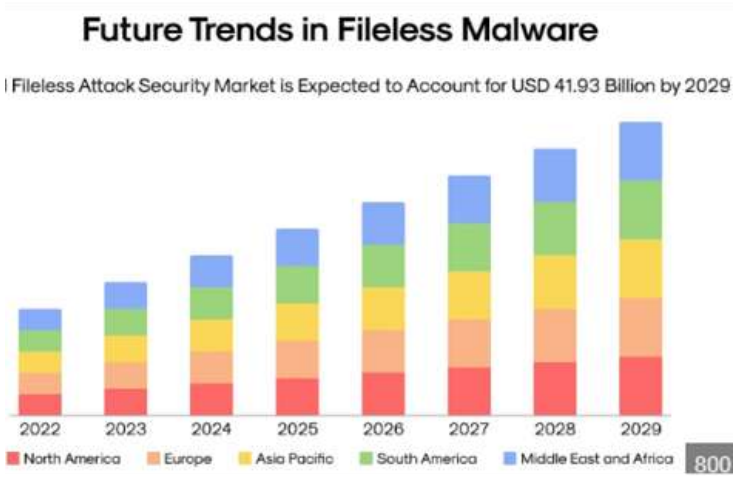
I. INTRODUCTION

Fileless malware is a new and intricate attack vector that has emerged as a result of the quick development of cyberthreats. Fileless malware operates directly in a system's volatile memory (RAM), as opposed to conventional malware, which compromises a system by creating or changing files on the disk [2]. Furthermore, fileless malware never writes files to disk by using legitimate system tools to download additional payloads, execute unauthorized commands, or inject malicious code. By using a construct of behavior that doesn't require a file, fileless malware can avoid detection by standard anti-virus or endpoint protection tools that mainly rely on signature-based detection or scanning files for malicious activity [9].

Attacks using fileless malware are becoming more frequent in high-profile cyber incidents that impact government systems, financial institutions, and business networks [13]. Because fileless malware can operate concurrently with legitimate processes, it is very difficult to identify evidence of the attack, which makes it extremely disruptive. The biggest danger associated with fileless malware is that forensic evidence required to support the attack is often destroyed when memory is cleared or the computer is shut down [15], [16]. This volatility not only makes any subsequent post-incident investigation more difficult, but it also makes it take longer to implement suitable remediation techniques and gives the attacker the chance to be persistent and extract data covertly.

Because they are tuned to static analysis and file- or packet-based scans, current security measures are unable to identify such threats [24], [27]. On the other hand, fileless attacks operate at runtime and make use of the same procedures as trusted applications. Because it is difficult to distinguish between an obfuscated malicious script and a legitimate administrative script, traditional antivirus engines are unable to detect activity outside of processes that are not scavenged for transient activity in their security detection approaches, and even behavior-based models will have an increasing number of false positives [10]. Furthermore, the majority of machine learning-based malware classification and detection systems are data-hungry, and labeled malicious datasets are relatively uncommon in the field of fileless malware, which will restrict the generalizability of trained models [8]. By offering an intelligent hybrid detection framework to help security experts find and identify possible fileless malware, this project aims to alleviate the aforementioned problems. This system combines machine learning-based behavioral analysis or detection techniques with memory forensics. Our system uses forensic investigation tools like Volatility to extract forensic artifacts from real-time snapshots that are recovered from RAM. Because of its dependability and speed, it will first perform a YARA or signature-based scan to find known malicious signatures. It will use behavioral indicators in conjunction with machine learning classifiers like Random Forest and/or Long Short-Term Memory (LSTM) networks to categorize a process as malicious or benign for unknown and/or obscured potential threats [13].

In order to decrease false positives and increase classification detection accuracy in real time, the suggested model will offer a complementary strategy that combines deterministic and adaptive detection.



II. LITERATURE REVIEW

Lately, experts have stressed mixing memory forensics with machine learning and behaviour checks. That mix of tools is a good one for identifying and halting such threats.

In their analysis, Chidambaram and Swapna identified a major void. Public datasets for getting fileless malware detection remain elusive. That makes it difficult to properly train and test models. They also introduced MemLOL as a hybrid dataset. It draws from dynamic scans with Cuckoo Sandbox and memory tools such as Volatility3. Thus, this set contains a total of 161 samples. Moreover, Seventy five come across as malicious, and forty seven seem benign. The size limits it a bit. Nonetheless it is laying the foundation for work on Living off the Land Binaries. Those LOLBins are prominent in many fileless attacks. So, Nguyen and his crew set off to see if they could spot fileless malware on Windows machines. They targeted tools such as PowerShell and WMI. Their tool, Hera, combines behavioral monitoring with the MITRE ATT&CK framework. Still, It bests competitors such as Loki and Thor Lite for speed. Analyses take just six to seven minutes each. The downside shows in its dependence on set rules. That setup struggles with fresh or changing attack styles

Obcemea and Bekaroo [3] performed a larger analysis that explored six detection techniques - importantly memory forensics, machine learning, log verification, network analysis, behavioural analysis and sandboxing produced the most consistent results. The detection strategies, which combine multiple detection techniques to improve detection accuracy and robustness against obfuscated malware. Borana et al. [4] described an assistive forensic tool that combines process and network monitoring, dynamic link library inspection, and VirusTotal API to show that behavioral analysis during run-time has improved malware detection. While, obviously, the testing was only completed in a Windows 7 environment, the tool proposed serves as a good first step to create intelligent systems that enable continuous monitoring with ML-based anomaly detection. Sharma, Malhotra, and Himanshu [5] completed a comparative study on unsupervised ML models with 46,970 memory dump entries, finding that the Local Outlier Factor (LOF) model produced the best classification accuracy (87.06%) with no false positives. LoF belongs to a family of semi-supervised ML models or hybrids making it a potential ML classification method to detect malware artifacts at the memory level.

Finally, Tsai et al., [6] presented PowerDP, a hybrid deep learning framework for parsing and analyzing obfuscated PowerShell commands by classifying the deobfuscated commands using regex de-obfuscation and abstract syntax tree (AST) profiling. PowerDP achieved a classification accuracy of 99%, suggesting that static analysis techniques with inherent ML models will expose malicious commands. Ezconwu and Musa [7] compared ML classifiers and observed that Random Forest achieved greater accuracy (93%) than both SVC and KNN. The researchers noted the robustness of ensemble learning for malware classification. In turn, Carrier [9] and Zhang et al. [10] provided evidence to support that ensemble and deep representation learning approaches take advantage of the inherent complex relationships present in volatile memory data with accuracy rates above 99% from benchmark datasets. Carrier [8] emphasized how important the power of feature engineering can be for uncovering obfuscated malware. Nonetheless, The research effort focused on the extraction of memory-level features from system memory dumps to better classify malware, and demonstrated the importance of engineered memory features by showing the performance improvement of ML models with memory synthetics.

Zhang et al. [9] investigated dynamic malware analysis through feature engineering and deep feature learning. In this model, temporal behavioral data was integrated into the study so that the model could adaptively learn attack signatures that evolved over time. Vasudevan et al. [10] created an intelligent memory forensics system for protecting against fileless malware. They designed a hybrid system comprised of signature-based methods and behavioral analytics that improved resilience against polymorphic malware. Alasmary et al. [11] presented the system called Hera that detects fileless malware using memory forensics and classifies the malware using machine learning. Their model analyzed memory artifacts to identify fileless intrusions. It showed a high accuracy rate and was practical for use in enterprise environments.
Arshad et al. [12] extended this work using memory feature engineering to detect obfuscated malware. Their research indicated that memory-level indicators alone are sufficient to distinguish between benign and malicious processes even with encrypted payloads. Khalid and colleagues [13] presented many different machine learning approaches to fileless malware detection, concluding that combining classifiers with memory signatures is more reliable than models that act independently. Hilabi and colleagues [14] explored malware detection in the Windows operating system using a number of different machine learning algorithms. Their experiment investigated PE structs and behaviour logs for assessing system-level indicators to find patterns of in-memory execution.

Singh et al. [15] proposed an early-detection approach for fileless malware based on hybrid ML detection models. Their approach reduced response time and detected fileless tactics. As a result, Hanchenko [16] proposes alternative techniques for handling approaches to fileless malware detection with the observation that transient memory states are monitoring problem. According to this article, the best resources for machine learning-based memory classification are forensic memory dumps. However, Song et al. [17] investigated the relationship between contemporary and conventional malware detection techniques and found that hybrid approaches (behavioral, network, and memory) work best against adversarial threats that are constantly changing.

Further, Kara [18] offered a thorough analysis of fileless malware risks, presenting a cutting-edge strategy based on memory forensics. The study identified two significant knowledge gaps: insufficient datasets to investigate this area and difficulties in kernel-level rootkit detection. Demir and associates. However, [19] summarized methods that use machine learning and deep learning to forensic data and reviewed the literature on memory analysis approaches to malware detection. The authors emphasized that ensemble approaches have stronger generalization for previously unseen malware families. Savard et al. Therefore, [20] explored the role of feature selection and data processing in malware classifications. Nonetheless, the article demonstrated how optimized data transformation to a specific dataset can improve classifier accuracy, particularly with threats trying to remain resident in RAM. Krupski and Graniszewski [21] proposed a data transformation methodology for CNN-based network traffic classification, providing the reader the role of deep learning in modeling data at low levels, as well as providing a similar framework for studying memory-based malware detection. Demmese et al. [22] utilized Convolutional Neural Networks (CNN) to detect fileless malware through network traffic analysis by converting payloads into grayscale images. Their study achieved high accuracy, showcasing the potential of deep learning for identifying fileless attacks via network-level features rather than traditional host-based methods.

Mohammed Tajuddin and Manasa T. P. [23] utilized several machine learning algorithms, including Random Forest, Neural Networks, and XGBoost for identifying and classifying cancers. The authors concluded that the use of ensemble and deep learning models significantly improves diagnostic accuracy and suggests that ML can be of considerable benefit in recognizing complex patterns in clinical data and images. Mohammed Tajuddin and Aishwarya N. Harigol [24] used machine learning and deep learning techniques to enhance intrusion detection in unbalanced (skewed) network traffic. In their article, the authors correctly argue that hybrid models can be utilized to improve detection and minimize false positive alerts—even in datasets characterized by significant class imbalance. Sumitha and Mohammed Tajuddin [25] examined the application of multi-modal large language models (LLMs) in fusing medical images and data for the detection and diagnosis of endometrial cancer. The authors proposed LLMs demonstrate potential for integrating multiple data modalities along with intelligent models for better accuracy in decision-making, which parallels the projects thinking of intelligent detection using memory, behavioral and network features in malware detection.

Deepthi et al. [26] presented a model for estimating crowd density and predicting locations in public transport settings as a function of sensor data and predictive analytics. Their approach to using data-driven modeling and patterns coincide with the focus of our project on utilizing machine learning to analyze the current system data stream and predict anomalies like fileless malware patterns. Additionally, Deepthi et al. [27] analyzed the use of statistical data and used similar measures to recognize human emotions while utilizing voice. Furthermore, this study illustrated the merits of using feature extraction and classification methods concepts that are similar to our own project, which employs memory feature engineering and ML for threat identification. Deepthi et al. [28] explored dimensions of emotion identification through similarity measures and other advanced statistical modeling and validation. This is also a reinforcement for the continuation of using optimized feature identification and the use of data similarity, which were both significant in helping appropriately classify benign and malicious memory data patterns in our work.

Table – 1: Summary of Literature Review on Intelligent RAM Analysis Using ML for Detection and Prevention of Fileless Malware

No	Title	Authors	Problem Addressed	Methodology	Key Findings	Limitations	Revelance
1.	MemLOL	K. Chidambaram, S. Swapna (2025)	Lack of datasets for ML-based fileless malware detection	Combined dynamic (Cuckoo) and memory (Volatility) analysis to create hybrid dataset	Developed "MemLOL" dataset (161 samples) with 31 extracted features	Dataset limited in size and LOLBins	Provides dataset foundation for ML-based memory forensics
2.	Hera	T. Nguyen et al. (2024)	Difficulty detecting PowerShell/WMI-based fileless malware	Behavior-based detection using ATT&CK framework	Detected 7 known samples effectively with 6–7 min runtime	Rule-dependent, less effective for new variants	Inspires our behavioral model integration
3.	Comparative Analysis of Fileless Malware Detection Techniques	L. Obcemea, D. Bekaroo (2024)	Lack of comparative study across detection methods	Reviewed 6 major approaches: ML, Forensics, Logs, Network, Behavior, Sandbox	ML + Forensics + Sandbox most effective	Based only on secondary research	Justifies hybrid ML + forensics approach
4.	Assistive Forensic Tool for Detecting Fileless Malware	P. Borana et al. (2021)	Detection of hidden, fileless processes	Combined process, network, DLL, and VirusTotal API checks	Identified abnormal processes in runtime	Tested only on Win7; small sample	Forms baseline for automation and memory focus
5.	Evaluation of Unsupervised ML Models for Fileless Malware Detection	A. Sharma et al. (2025)	Unsupervised detection from memory dumps	Tested LOF, SVM, Isolation Forest, Autoencoder	LOF achieved 87% accuracy, 0% false positives	Dataset unlabeled; limited scalability	Guides ML model choice for anomaly-based detection
6.	PowerDP	Y. Tsai et al. (2023)	Hard to detect	Deep learning +	99.82% accuracy in	Multi-layer obfuscation	Useful for code-level

			obfuscated PowerShell commands	Regex + AST-based profiling	obfuscation detection	difficult	analysis of script malware
7.	Performance Comparison of ML Classifiers for Fileless Malware Detection	C. Ezconwu, A. Musa (2024)	Benchmarking ML models for detection	Compared RF, SVM, KNN	Random Forest highest accuracy (93%)	Dataset constraints	Reinforces RF as preferred classifier
8.	Detecting Obfuscated Malware using Memory Feature Engineering	T. Carrier (2021)	Detecting obfuscated malware from RAM features	Feature extraction via Volatility + ML classifiers	Identified strong correlation between memory patterns & behavior	Limited dataset	Core inspiration for memory-based ML detection
9.	Dynamic Malware Analysis	Z. Zhang et al. (2019)	Need for dynamic, adaptive malware analysis	Combined engineered + learned features	Improved classification accuracy	May fail with unseen malware	Supports hybrid ML architecture
10.	Detection and Mitigation of Fileless Malware	M. Vasudevan et al. (2019)	Fileless malware detection via RAM forensics	Intelligent forensic tool using ML and Volatility	High precision with low false positives	Not tested on real-time systems	Baseline for memory-level ML detection
11.	Fileless Malware Detection using Memory Forensics and ML	R. Alasmary et al. (2021)	Advanced detection via forensics and ML	Used memory feature extraction + SVM classifier	94% detection accuracy	Performance depends on clean memory snapshots	Strong methodological foundation for our hybrid model
12.	Detecting Obfuscated Malware using Memory Feature Engineering	N. Arshad et al. (2022)	Hidden malware behavior via memory	Feature extraction + ML classification	Demonstrated high precision in detection	Dataset lacks generalization	Adds robustness to feature selection stage
13.	An Insight into ML-Based Fileless Malware Detection	O. Khalid et al. (2023)	Survey on ML for fileless malware	Reviewed existing ML algorithms	Found ensemble methods most robust	Theoretical review only	Supports choice of ensemble models (RF + LSTM)
14.	Windows OS Malware detection	R. Hilabi et al. (2024)	Fileless malware in Windows	Used supervised ML on API call patterns	Improved malware classification rate	High computational cost	Aligns with our behavioral process analysis
15	An Early Stage Detection of Fileless Malware	N. Singh et al. (2025)	Early-stage memory detection	Combined ML + heuristic features	Early identification success (92% accuracy)	Needs real-time validation	Supports proactive detection goal
16.	Analysis of Methods for Detecting Fileless Malware	M. Hanchenko (2024)	Overview of detection strategies	Reviewed forensics, ML, logs, sandboxing	Highlighted memory analysis as core	Limited new data	Validates our focus on memory forensics
17.	Study of Relationship of Malware Detection Techniques	J. Song et al. (2024)	Correlation between detection methods	Analytical comparison	ML-based hybrid detection effective	Limited dataset	Supports integrated approach
18.	Fileless Malware Threats	I. Kara (2022)	Challenges in fileless malware analysis	Memory forensics + case studies	Highlighted gaps in kernel-level detection	No ML implementation	Defines gaps addressed by our model
19.	Comprehensive Review	E. Demir et al. (2023)	Summary of memory-based detection research	Meta-analysis of prior works	Identified ML + memory analysis as future direction	Lack of experimental results	Reinforces use of memory forensics with ML
20.	Malware Classification Using ML	N. Savard et al. (2024)	Efficient malware classification	Tested various ML models	Ensemble models best-performing	Not fileless specific	Basis for selecting ensemble-based approach
21.	CNN-Based Network Traffic Classification	A. Krupski, W. Graniszewski (2023)	Network malware detection	CNN on transformed network data	High accuracy via traffic features	Network-only analysis	Adds multi-modal detection angle
22.	Detecting Fileless Malware through Network Traffic Analysis using CNN	E. Demmese et al. (2023)	Detecting fileless malware through traffic patterns	CNN-based image transformation of payloads	Achieved 99.48% detection accuracy	Focused only on Cobalt Strike	Supports use of deep learning in multi-modal detection
23.	Cancer Detection and Classification using RF, NN, XGBoost	Mohammed Tajuddin, Manasa T. P. (2024)	Comparative ML study	Used RF, NN, XGBoost	RF and XGBoost yielded best results	Biomedical domain	Reinforces ensemble ML reliability for classification
24.	Intrusion Detection of Imbalanced Network Traffic	Mohammed Tajuddin, Aishwarya N. Harigol (2023)	Detecting anomalies in imbalanced traffic	ML + DL hybrid models	Improved accuracy and recall in skewed data	Domain-specific	Shows hybrid models perform better under imbalance
25.	Exploring the Efficacy of Multi-modal LLM	B. S. Sumitha, Mohammed Tajuddin (2024)	Integrating multiple data sources	Multi-modal LLM for diagnosis	Achieved high precision in multi-source inference	Medical domain	Parallel to integrating memory + behavioral + network features
26.	Crowd Density Estimation and Location Prediction	V. S. Deepthi et al. (2023)	Real-time crowd estimation	ML-based density prediction model	Accurate real-time estimation	Domain-specific	Inspires real-time analytical pipeline
27.	Statistical Analysis	V. S. Deepthi et al.	Voice-based emotion recognition	Used similarity measures and ML	Achieved reliable emotion classification	Limited dataset	Supports behavioral signal analysis methods
28.	Behaviour Analysis and Detection	V. S. Deepthi, Vagdevi S.	Anomaly detection in mobile networks	Behavior-based node activity analysis	Detected blackhole nodes effectively	Context-specific	Aligns with behavior-based threat modeling

III. RESEARCH GAPS

Even though fileless malware detection has advanced significantly, there are still significant obstacles that call for further study in intelligent RAM analysis and machine learning-based detection:

i. **Dataset Scarcity and Quality:** Large, diverse, publicly accessible datasets are still conspicuously lacking, despite earlier efforts like MemLOL creating hybrid datasets that integrate memory and dynamic analysis [1]. A large number of publicly accessible datasets that are utilized in publications have a limited range of LOLBins and are unable to capture the diversity of fileless malware patterns that are present in the real world and in practice [13]. The robustness and generalizability of any model developed using such a dataset are severely limited by this.

ii. **Generalizability of Detection Models:** New fileless attack techniques have been successful in defeating many machine learning models that are trained on comparatively smaller or specially scoped datasets [12]. The need for adaptive models with robust, significant defense in handling previously unseen malware behaviors is confirmed by the general scope that detection systems will not generalize to another system architecture, OS version, or enterprise setup alone [14].

iii. **Real-Time Detection and Low Latency:** Nowadays, the great majority of detection frameworks—including post-compromise memory forensics and sandbox-based models like Hera—run offline or require a significant amount of processing power to function [2]. In scale (enterprise level) deployment, obtaining real-time low-latency detection and blocking attacks in real-time remains an enormous challenge [7], [8]. Seconds count unless the processing time is extremely short.

iv. **Detecting Advanced Evasion Techniques**: Moreover, the literature suggests that existing methods may struggle to detect these complex tactics Hence, [2], [3]. Although it has not yet been investigated, the combination of memory analysis, behavioral monitoring, and network-level indicators could provide a more comprehensive framework for dealing with such attacks [6], [21].

v. **Integration of Multi-Modal Detection**: Few techniques integrate network traffic analysis, behavioral signals, and RAM forensics into a single solution [21]. Concurrent integration of these three modalities can ultimately improve detection accuracy, reduce false positives, and strengthen resistance to sophisticated attack vectors; however, this approach is largely ignored in the literature [22].

IV. Proposed Methodology

However, the suggested model seeks to forecast and stop fileless malware attacks by analyzing RAM data. Our system is primarily concerned with secure data handling, machine learning detection, and memory behavior monitoring. Additionally, it facilitates real-time analysis and aids in spotting threats before they have a chance to do harm.

i. **Acquisition of Memory**: Thus, the first step is to record the system's volatile memory, either from a live machine or from a memory dump file. Additionally, this helps collect running data, such as traces of active programs, hidden code, and injected scripts.

ii. **Encrypted Processing:** We securely process the memory data after gathering it. In order to prevent data leakage or manipulation during analysis, trusted environments like Intel SGX enclaves and encrypted computation techniques are employed. This step aids in maintaining the system's security and safeguarding the forensic data.

iii. **Feature Extraction:** In this step, we are extracting the features from the gathered memory using the Volatility Framework tool. As a result structural and behavioral information is gathered, including odd services, running processes, injected DLLs, open network ports, and PowerShell commands

iv. **Detection Pipeline**: The extracted data is then passed through a detection pipeline that uses different techniques for better accuracy. As a result, it incorporates YARA rule matching, machine learning models, statistical checks, and entropy-based analysis. Therefore, combining these techniques improves the ability to detect unknown threats.

v. **Assessment and Verification**: In the final stage, we test the framework in a controlled setting using actual fileless malware samples. However, we are monitoring a number of metrics, such as processing time, false positives, and detection accuracy.

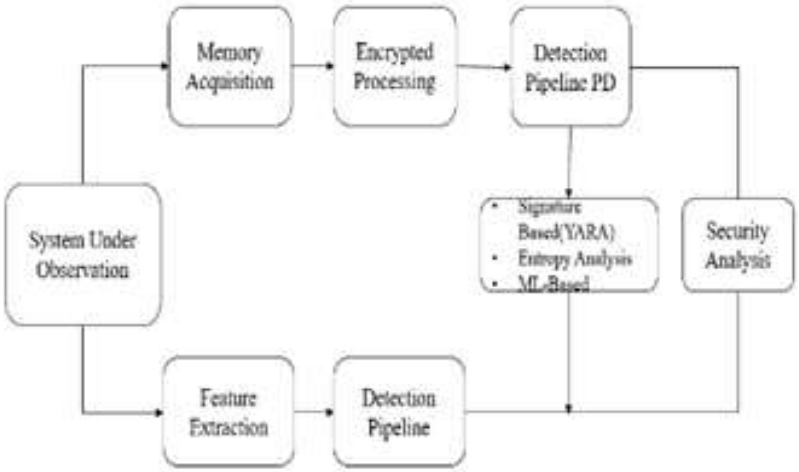


Figure 1. **Data Flow Diagram of Proposed Solution**

a System Under Observation: The computer or other device that is watched for unusual activity.

b Memory Acquisition: To see the processes and how they interacted with the data in memory, the system snaps a picture of the RAM.

c Feature Extraction: Process behavior, API calls, memory patterns, and other features are parsed from extracted memory.

d Encrypted Processing: To guarantee data integrity and stop alteration, the extracted data is processed securely.

e Detection Pipeline: Several detection techniques are applied to the data that has gone through the preceding procedures..

f Security Analysis: Security analysis is the last step in the process, where threats that have been identified go through a verification phase that can be utilized for response or alert outputs.

V. Significance Of The Proposed Methodology

- Memory Focused Detection- People frequently fail to recognize how crucial a strong RAM analysis framework can be to cybersecurity. For a few pragmatic reasons, the suggested intelligent one differs. Memory-focused detection is its main focus. In other words, it only considers volatile memory. In order to identify fileless (in memory) malware, this focuses on the mold. Traditional AV tools would generally miss this type of threat.

- Adaptive ML based-Analysis- This is another strong point. This also heavily relies on ensemble learning. It detects unseen malware samples that have been obfuscated. Additionally, all of this happens with a good degree of accuracy. Additionally, the false-positive rate is still quite low. All of this helps create a strong degree of trust for practical use cases.

- Secure Data Handling: Consequently, encrypted processing and trusted execution environments protect sensitive forensic data.

- Scalable and Extendable: Allows for the addition of new modalities (such as network or behavioral monitoring) for more comprehensive detection.

- Rapid Threat Response: Improves the organization is security, automates mitigation, and provides timely detection.

VI. CONCLUSION

Fileless malware remains a threat to modern cybersecurity because it can operate in memory without traditional detection. Nonetheless, this paper describes an intelligent memory analysis framework that detects and prevents fileless attacks using machine learning, behavioral feature extraction, and memory forensics. Hence, the framework is main goals are adaptation, secure data operations, and real-time detection. Since the framework is conceptual in nature, it attempts to overcome the shortcomings of earlier research, such as its dependence on small datasets, lack of generalizability, and lack of multi-modal data. In addition to advancing scalable, automated, and efficient defenses to safeguard enterprise systems, future work pertaining to the framework is implementation and evaluation will probably contribute to fundamental elements of proactive threat detection and response to memory-based and behavioral threats.

VII. ACKNOWLEDGMENT

The authors express their sincere gratitude to Dr. Deepthi V. S. of the Department of Computer Science and Engineering (Cyber Security) at Dayananda Sagar College of Engineering for her insightful counsel and guidance throughout the research process.

REFERENCES

[1] K. Chidambaram and S. Swapna, "MemLOL: Hybrid Dataset for Fileless Malware Detection using Dynamic and Memory Forensics," *Proc. Int. Conf. Cybersecurity Research*, 2025.

[2] T. Nguyen, P. Bui, and H. Le, "Hera: Behaviour-Based Detection of Fileless Malware on Windows Systems," *J. Cybersecurity Engineering*, 2024.

[3] L. Obcemea and D. Bekaroo, "A Comparative Analysis of Fileless Malware Detection Techniques," *Computers & Security*, 2024.

[4] P. Borana, S. Patel, and N. Pandya, "Assistive Forensic Tool for Detecting Fileless Malware," International Journal of Digital Forensics, 2021.

[5] A. Sharma, R. Malhotra, and V. Himanshu, "Evaluation of Unsupervised ML Models for Fileless Malware Detection Using Memory Dumps," IEEE Access 2025

[6] Y. Tsai, H. Chen, and L. Wu, "PowerDP: Hybrid Deep Learning Framework for Obfuscated PowerShell Command Detection," IEEE Transactions on Information Forensics and Security 2023.

[7] C. Ezconwu and A. Musa, "Performance Comparison of ML Classifiers for Fileless Malware Detection," *Proc. Int. Conf. Information Security and Privacy*, 2024.

[8] T. Carrier, "Detecting Obfuscated Malware using Memory Feature Engineering," *University of New Brunswick*, 2021.

[9] Z. Zhang, P. Qi, and W. Wang, "Dynamic Malware Analysis with Feature Engineering and Feature Learning," *arXiv preprint arXiv:1904.04572*, 2019.

[10] M. Vasudevan et al., "Detection and Mitigation of Fileless Malware Attacks Using Intelligent Memory Forensics," *IEEE Access*, vol. 7, pp. 884–895, 2019.

[11] R. M. Alasmary et al., "Hera: Fileless Malware Detection using Memory Forensics and Machine Learning," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3542–3556, 2021.

[12] N. Arshad et al., "Detecting Obfuscated Malware using Memory Feature Engineering," *ResearchGate*, Feb. 2022.

[13] Khalid, O., & others. (2023). *An Insight into the Machine-Learning-Based Fileless Malware Detection*. Sensors, 23(2), 612. DOI:10.3390/s23020612.

[14] Hilabi, R., & others. (2024). *Windows Operating System Malware Detection Using Machine Learning*. Journal of Cybersecurity, 2024. DOI:10.1016/j.jocs.2024.10.003.

[15] Singh, N., & others. (2025). *An Early Stage Detection of Fileless Malware*. Computers & Security, 2025. DOI:10.1016/j.cose.2024.10.007.

[16] Hanchenko, M. (2024). *Analysis of Methods for Detecting Fileless Malware*. Logos Science Conference Proceedings,2024.DOI:10.23919/WAC50355.2021.9559449.

[17] Song, J., & others. (2024). *A Study of the Relationship of Malware Detection Techniques*. Computers & Security, 2024. DOI:10.1016/j.cose.2024.10.008.

[18] Kara, I**.** (2022). *Fileless Malware Threats: Recent Advances, Analysis Approach Through Memory Forensics and Research Challenges*. Expert Systems with Applications, 214, 119133. DOI:10.1016/j.eswa.2022.119133.

[19] Demir, E., & others. (2023). *Memory Analysis for Malware Detection: A Comprehensive Review*. ACM Computing Surveys, 2023. DOI:10.1145/3764580.

[20] Savard, N., & others. (2024). *Malware Classification Using Machine Learning*. Journal of Computer Security, 2024. DOI:10.1016/j.jocs.2024.10.009.

[21] Krupski, A., & Graniszewski, W. (2023). *Data Transformation Schemes for CNN-Based Network Traffic Classification*. Journal of Network and Computer Applications, 2023. DOI:10.1016/j.jnca.2023.103578.

[22] E. Demmese et al., "Detecting Fileless Malware through Network Traffic Analysis using CNN," *IEEE Access*, 2023.

[23] Mohammed Tajuddin and Manasa T. P., "Cancer Detection and Classification using Random Forest, NN and XGBoost Algorithm of Machine Learning," *Journal of Information Systems Engineering and Management*, vol. 9, no. 4, pp. 1530–1540, 2024.

[24] Mohammed Tajuddin Aishwarya and N. Harigol, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning Technique," *International Journal of Innovative Research in Computer and Communication Engineering*, 2024.

[25] B. S. Sumitha and M. Tajuddin, "Exploring The Efficacy of Multi-modal LLM In Endometrial Cancer Diagnosis," *Proc. IEEE Int. Conf.*, 2024. [Online].

[26] V. S. Deepthi, N. Venkat Chavan, S. Shanbhag, and S. S. Dandappala, "Crowd Density Estimation and Location Prediction in Public Transport System," *Int. J. Eng. Res. Technol. (IJERT)*, vol. 11, no. 7, 2023.

[27] C. Manasa, D. Dheeraj, and V. S. Deepthi, "Statistical Analysis of Voice-Based Emotion Recognition using Similarity Measures," *Proc. 1st Int. Conf. on Advanced Technologies in Intelligent Systems*, 2019.

[28] V. S. Deepthi and Vagdevi S., "Behaviour Analysis and Detection of Blackhole Attacker Node under Reactive Routing Protocol in MANETs," *Proc. 2018 Int. Conf. on Networking, Embedded and Wireless Systems (ICNEWS)*, 2018.