Jurnal Komputer dan Elektro Sains, Vol.4 No.1, March 2026, 1-5
https://ejournal.sultanpublisher.com/index.php/komets

Received : January 12, 2026; Revision: March 29, 2026; Accepted: April 01, 2026; Publication: April 01, 2026.

E-ISSN: 3021-8462, DOI: https://doi.org/10.58291/komets.v4i1.537

Digital Forensics for Cyberattack Detection in VM Migration: A Conceptual Framework

Taufik Hidayat[1], Nadim Ibrahim[2]
[1]Department of Computer Engineering, Universitas Wiralodra, Indramayu, Indonesia
[2]Department of Communication Engineering and Informatics, Arab International University, Damascus, Syria

Corresponding Author: Taufik Hidayat (e-mail: thidayat.ft@unwir.ac.id)

ABSTRACT
Virtual machine (VM) migration is widely used in cloud environments because it helps systems stay flexible and use resources more efficiently. At the same time, it can introduce security concerns, especially when forensic investigation is needed. Most previous studies look at areas like intrusion detection or memory forensics, but they are usually treated separately and not in relation to VM migration. In this work, a digital forensic framework is proposed for VM migration scenarios. The idea is to bring several steps together, such as monitoring, collecting data, analyzing it, and reporting the findings. One important point is the migration phase itself, since system states are moving between hosts and some activities may not be fully visible during this process. The framework is discussed conceptually by looking at how these parts interact and how it can address some of the limitations found in earlier work. In general, combining detection and forensic analysis in this way can help make investigations more consistent. This study can also be used as a starting point for further work and practical use in cloud systems.

KEYWORD Digital forensics; virtual machine; cloud forensics; intrusion detection.

1. INTRODUCTION

Cloud computing has become a crucial component of contemporary IT infrastructure due to its rapid growth in recent years. This is made feasible in large part by virtualization. On a single physical device, it enables the operation of several VMs. Each the VMs can have a different operating system installed, which increases your options and optimizes resource utilization. This requirement is particularly crucial for Infrastructure as a Service (IaaS), since system requirements might fluctuate rapidly. There are certain advantages to virtualization settings, but there are also new security issues. Despite their logical separation, the VMs share the same physical resources. Careless individuals may attempt to access other virtual VMs in a multi-tenant environment or exploit pre-existing security flaws. Thus, security is still a major concern for virtualized systems [1, 2].

Attacks frequently use process injection. This technique allows malicious code to enter legitimate processes, which, from the perspective of the system, appears to be regular activity. This makes it more difficult to locate, particularly if it relies solely on conventional techniques like rule-based or signature-based detection. These techniques often perform well against known threats, but they are less effective in thwarting novel or altered attacks. Due to its ability to view straight into the system's memory, memory forensics is growing in popularity. This makes it easier to overcome these issues.

Additionally, virtual machine introspection (VMI) has emerged as one of the most widely used techniques. VMI allows you to monitor the process from outside the guest operating system, typically via the hypervisor. Hiding suspicious behavior becomes more difficult as a result. VMI can be used to identify several types of anomalous behavior, including process injection. However, it can be challenging to implement in the real world because it requires low-level access and specific tools [3, 4]. However, most existing studies do not consider the migration process of VM. In live migration scenarios,VM can move from one host to another without interrupting running services. During this process, the memory state is transferred between hosts in multiple steps, which makes it difficult to obtain a consistent and reliable forensic snapshot. This issue remains insufficiently explored in current digital forensic research. This becomes more critical in live migration scenarios. While the mechanism helps maintain system performance and availability, it can also introduce security and forensic issues, such as data inconsistency, integrity problems, and the possibility that malicious processes, including process injection, remain undetected during migration.

In the context of VM migration, process injection does not only happen at a single stage. It can begin before migration at the source host, continue while memory is being transferred, or remain after the VM arrives at the destination. Since memory is moved step by step, some injected processes may not be immediately visible, especially without continuous monitoring. This makes it difficult to clearly connect

attack detection with the migration process, which is still rarely discussed in existing studies.

Due to these issues, virtualized environments need a more cohesive approach for digital forensic investigations. Many studies still treat forensic frameworks, memory analysis, and intrusion detection as separate topics, which makes it harder to see the investigation process as a whole [5, 6]. This study introduces a digital forensic framework tailored to VM migration scenarios. It brings together several key elements, such as monitoring, migration handling, data collection, analysis, detection, and reporting, into a single workflow. With these components combined, the framework helps provide a clearer and more practical way to conduct forensic investigations, especially in environments where system conditions can change quickly.

2. RESEARCH METHODS

This study employs a systematic methodology aimed at the formulation of a conceptual framework for digital forensics with VM migration environments to fulfill the research objectives and address identified deficiencies.The research method looks at existing methods in a systematic way and builds an integrated model that helps with forensic investigation in virtualized systems [7].

2.1. Research Design

This study uses a qualitative and conceptual approach to develop a digital forensic framework for virtual machine migration environments. The overall research process is illustrated in Figure 1 to show how the framework is developed step by step. The study reviews previous work in digital forensics, VM security, and intrusion detection to understand existing challenges and limitations [8]. The focus is mainly on VM migration, where security risks and forensic issues may arise.

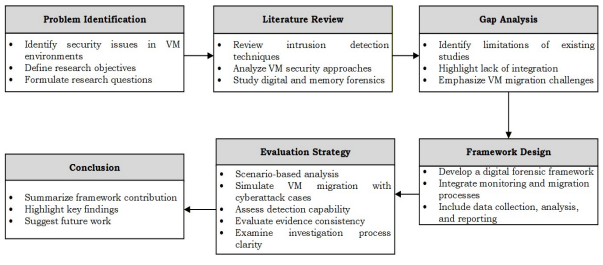

Fig. 1. Research Methodology Overview

Figure 1 provides a general overview of the research methodology used in this study. The first step involves examining security issues in virtual machine environments to define the main research objectives. This is followed by a literature review on intrusion detection, VM security, and digital forensics, along with the identification of existing challenges. The next step is to identify existing gaps, particularly the lack of integration between forensic processes and virtual machine migration. Based on these observations, a conceptual framework is developed by combining several key components, such as monitoring, data collection, analysis, and reporting.

In addition, an evaluation approach is considered using scenario-based analysis. The framework can be examined through VM migration cases involving potential cyberattacks, such as process injection occurring before, during, or after migration. Its effectiveness is assessed using several metrics, including detection capability, consistency of forensic evidence, and the clarity of the investigation process across different stages.

2.2 Literature Analysis

This part looks at a few studies that have to do with digital forensics and the security of virtual machines. Most of the work that has been done before has been on things like intrusion detection, memory forensics, and virtual machine introspection. Some research uses VMI and memory analysis to find attacks like process injection. This method lets you watch from outside the virtual machine, which makes it harder for attackers to hide what they're doing. But it usually needs low-level access and isn't easy to use in real life [9, 10].

Machine learning techniques are widely used for intrusion detection. Methods such as Support Vector Machine (SVM) and Random Forest are commonly applied to identify anomalous patterns in network traffic. However, most of these approaches are still limited to network-based data and do not fully consider virtual machine environments. Several limitations remain. Many studies do not integrate forensic analysis with detection mechanisms, and VM migration is often overlooked despite the risks associated with system transitions. For this reason, a more unified approach is needed. Table 1 summarizes the differences among existing studies and highlights their limitations.

Table 1. Summary of related studies

Study	Approach	Focus	Limitation
[11]	VMI and memory forensics	Process injection detection	Complex implementation, no ML integration
[12]	Machine Learning	Network intrusion detection	Not applied to VM environment
[13]	ML-based IDS	Cyberattack Detection	Limited to network data
[14]	Machine learning and deep learning	Cloud intrusion detection	Not focused on VM migration and forensic analysis
[15]	Cloud Forensics	Cloud security investigation	Lack of unified framework
[16]	Digital Forensics Framework	Cloud forensic readiness	Not focused on VM migration

Recent studies have examined various methodologies, including VM introspection, machine learning, and cloud-based intrusion detection (refer to Table 1). All of the methods work well to find cyber threats, but most of them only look at certain areas, like

cloud security or network monitoring. For instance, machine learning is often used to look at network traffic, while VMI is more focused on what happens at the system level. Most of the time, these methods are made separately. They are still not widely used in virtual machine environments, especially when moving to a new one. This means that forensic investigation in dynamic virtualized systems needs a more integrated framework [9, 17].

2.3 The proposed framework

This study looks at how digital forensic processes can be applied in virtual machine migration. Instead of treating detection and analysis as separate tasks, the idea here is to connect them within one framework so the investigation process becomes easier to follow. The framework is built around several main activities that occur during the VM lifecycle. It starts with observing system behavior, where things like running processes and memory usage are monitored to spot unusual activity. When migration happens, attention shifts to how data and system states move between hosts, since this stage can introduce risks such as data loss, corruption, or unauthorized access if not managed properly.

Thereafter, relevant data such as logs, memory snapshots, and network traffic are collected. These data are then examined to identify patterns that may indicate suspicious behavior. Rather than focusing on a single method, the framework combines different perspectives, such as statistical analysis, machine learning techniques (for example, supervised methods to classify anomalies and unsupervised approaches to explore patterns), and expert reviews, to make the analysis more consistent. These approaches are suitable for identifying anomalies in VM migration, where system behavior can change dynamically and differ from typical network-based patterns. Figure 2 shows how these parts are connected and how the process flows from one step to another.

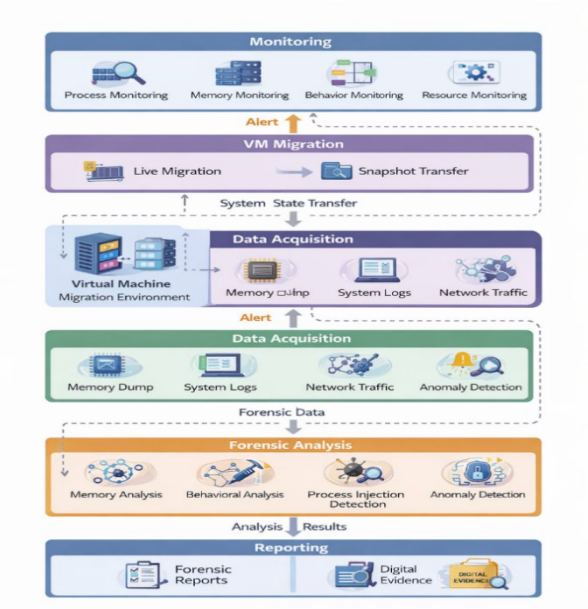

Fig. 2. Digital Forensic Framework VM Migration

Figure 2 shows the proposed digital forensic framework for VM migration and how the main parts are connected. The process starts with monitoring system activity to spot unusual behavior. In practice, this may add some extra load, especially during migration. To keep this under control, monitoring is not done all the time but focuses only on certain events. This way, useful forensic data can still be collected without affecting system performance too much. During migration, system states are moved from one host to another, which can introduce new risks. The data acquisition stage collects relevant evidence, such as logs and memory data. This data is then examined to find patterns that may indicate suspicious activity. The results are interpreted in the detection stage and recorded in the reporting stage to support further investigation.

3. RESULTS AND DISCUSSION

This part shows the results of the proposed framework and talks about how useful it is for filling in the research gaps that were found. The main topic of the discussion is how the framework brings together important parts of digital forensics in virtual machine migration environments and how it makes existing methods better, as described in the literature. Instead of doing an experimental evaluation, the results are looked at from a conceptual point of view by looking at the structure, functionality, and applicability of the proposed framework.The analysis shows that the framework can help with forensic investigations in virtualized systems that are dynamic and spread out.

3.1 Framework Analysis

This study develops a conceptual framework for digital forensics in virtual machine migration environments. The framework brings together several key processes, including monitoring, data collection, analysis, detection, and reporting, into one flow to support investigation activities. Rather than using experimental evaluation, this work focuses on how the framework is structured and how each part contributes to the overall process. The discussion emphasizes the ability of monitoring to capture VM activity, particularly during migration when system states transition between hosts. This stage is important because it may expose potential security risks.

The framework links data collection and analysis, which makes it easier to follow the investigation process. This lets you see strange activity, like processes or access that shouldn't happen. After that, the steps for finding and reporting the results help make sense of them and keep a clear record. The framework helps forensic work in virtual machine environments that are always changing in this way.

3.2 Comparison with Existing Studies

This part explains how the proposed framework compares with previous research. Researchers have looked at approaches such as machine learning for intrusion detection, virtual machine introspection VMI, and digital forensics, but they usually treat these as separate methods. For example, machine learning is often used to analyze network traffic and find unusual

patterns. It can be effective for detection, but it is not always related to forensic investigation, and VM migration is often overlooked. VMI observes system activity at a lower level, which is a different approach. It can provide detailed information, though the data is often complex and not always easy to use for more advanced analysis

Existing forensic frameworks do offer structured investigation steps, but they are generally not built for dynamic virtual environments. Issues such as VM migration, including data transfer and state consistency, are often not fully addressed. The framework proposed in this study takes a different approach by combining monitoring, data collection, analysis, and migration awareness into a single structure. By doing so, it supports both detection and investigation within VM environments. A comparison with existing approaches is presented in Table 2.

Table 2. Comparison of the proposed framework

Aspect	ML-based IDS	VMI-based Approach	The Digital Forensic Framework	Proposed Framework
Focus Area	Network Detection	Low-level Monitoring	Investigation Process	Integrated Forensic System
VM migration support	-	-	-	✓
Forensic Capability	Limited	Limited	Moderate	Comprehensive
Integration Level	Low	Low	Medium	High
Complexity	Moderate	High	Moderate	Moderate
Real-time Monitoring	✓	✓	-	✓

Table 2 demonstrates that the proposed framework provides a more comprehensive approach than existing methods by integrating monitoring, forensic analysis, and migration awareness within a single model. Unlike previous studies that focused on specific aspects, the proposed framework supports both detection and investigation processes in virtual machine (VM) environments.

3.3 Implications

The proposed framework has implications for both research and practical use in digital forensics. It brings together several processes into one structure, which can be useful for studying forensic approaches in virtualized environments, especially when migration is involved. From a practical side, the framework can help investigators understand how forensic steps can be applied during VM operations. By combining monitoring, data collection, and analysis, it supports a clearer way to identify and examine potential security incidents. It also emphasizes the role of migration in forensic analysis. Taking this aspect into account can enhance evidence handling and facilitate improved decision-making when addressing security concerns in cloud systems. Specifically, the framework addresses risks unique to live migration, such as the exposure of data during transfer between hosts, potential inconsistencies in system state before and after migration, and the increased difficulty of maintaining evidence integrity when virtual machine instances move across physical boundaries. By incorporating these considerations into the forensic workflow, the framework provides a more comprehensive basis for investigation in dynamic virtualized environments.

4. CONCLUSION

This study presents a digital forensic framework for virtual machine migration. The framework brings together several steps, such as monitoring, data collection, analysis, and reporting, so the investigation process becomes easier to follow. Most previous work looks at detection and forensic analysis separately. In this study, more attention is given to what happens during migration, when system states move between hosts. At this point, some activities, especially those related to memory and running processes, may not be fully captured. This situation can create gaps in the forensic process, and this is the main issue addressed in this work. By focusing on this stage, the framework helps give a clearer picture of system behavior during migration and supports a more consistent analysis in virtual environments.For future work, the framework can be tested in more concrete cases. For example, it can be used to see how well anomalies are detected during migration, how much impact monitoring has on performance, or how it behaves under different migration conditions.

5. REFERENCES

[1] B. Borisaniya and D. Patel, "Towards virtual machine introspection based security framework for cloud," *Sādhanā,* vol. 44, no. 2, p. 34, 2019.

[2] J. Dykstra and A. T. Sherman, "Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques," *Digital Investigation,* vol. 9, pp. S90-S98, 2012.

[3] B. D. Payne, "Virtual Machine Introspection," in *Encyclopedia of Cryptography, Security and Privacy*: Springer, 2025, pp. 2735-2737.

[4] T. Dangl, B. Taubmann, and H. P. Reiser, "RapidVMI: Fast and multi-core aware active virtual machine introspection," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1-10.

[5] T. Dangl, B. Taubmann, and H. P. Reiser, "Agent-based file extraction using virtual machine introspection," in *Nordic Conference on Secure IT Systems*, 2020: Springer, pp. 174-191.

[6] B. K. R. Alluri and G. Geethakumari, "A digital forensic model for introspection of virtual machines in cloud computing," in *2015 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, 2015: IEEE, pp. 1-5.

[7] S. Lim, B. Yoo, J. Park, K. Byun, and S. Lee, "A research on the investigation method of digital forensics for a VMware Workstation's virtual machine," *Mathematical and computer modelling,* vol. 55, no. 1-2, pp. 151-160, 2012.

[8] S. K. A. Manoj and D. L. Bhaskari, "Cloud forensics-a framework for investigating cyber attacks in cloud environment," *Procedia Computer Science,* vol. 85, pp. 149-154, 2016.

[9] M. M. Alshabibi, A. K. Bu dookhi, and M. Hafizur Rahman, "Forensic investigation, challenges, and issues of cloud data: A systematic literature review," *Computers,* vol. 13, no. 8, p. 213, 2024.

[10] S. Park, Y. Kim, G. Park, O. Na, and H. Chang, "Research on digital forensic readiness design in a cloud computing-based smart work environment," *Sustainability,* vol. 10, no. 4, p. 1203, 2018.

[11] D. Tank, M. J, H. P, D. Keraliya, J. R, and S. J, "Utilizing Virtual Machine Introspection and Memory Forensics to Identify Different Forms of Process Injection in a Virtualized Environment," *International Research Journal of Multidisciplinary Scope,* vol. 06, pp. 896-918, 01/01 2025, doi: 10.47857/irjms.2025.v06i02.03576.

[12] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *IEEE access,* vol. 7, pp. 41525-41550, 2019.

[13] I. Ullah and Q. H. Mahmoud, "A two-level flow-based anomalous activity detection system for IoT networks," *Electronics,* vol. 9, no. 3, p. 530, 2020.

[14] S. S. H. Shah, A. R. Ahmad, N. Jamil, and A. u. R. Khan, "Memory Forensics-Based Malware Detection Using Computer Vision and Machine Learning," *Electronics,* vol. 11, no. 16, p. 2579, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/16/2579.

[15] A. K. Sood and R. J. Enbody, "Targeted cyberattacks: a superset of advanced persistent threats," *IEEE security & privacy,* vol. 11, no. 1, pp. 54-61, 2012.

[16] V. R. Kebande, P. P. Mudau, R. A. Ikuesan, H. S. Venter, and K.-K. R. Choo, "Holistic digital forensic readiness framework for IoT-enabled organizations," *Forensic Science International: Reports,* vol. 2, p. 100117, 2020/12/01/ 2020, doi: https://doi.org/10.1016/j.fsir.2020.100117.

[17] N. K. Sharma and G. R. M. Reddy, "Multi-Objective Energy Efficient Virtual Machines Allocation at the Cloud Data Center," *IEEE Transactions on Services Computing,* vol. 12, no. 1, pp. 158-171, 2019, doi: 10.1109/TSC.2016.2596289.