International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Fronesis: Digital Forensics-Based Early Detection of Ongoing Cyber-Attacks

S.E Suresh [1], Poluru Rohith Kumar [2]

[1]Assistant Professor, Dept. of MCA, Annamacharya Institute of Technology and Sciences (AITS), Karakambadi, Tirupati, Andhra Pradesh, India
Email: sureshroopa2k15@gmail.com
[2] Student, Dept. of MCA, Annamacharya Institute of Technology and Sciences (AITS), Karakambadi, Tirupati, Andhra Pradesh, India
Email: rohithkumar98499@gmail.com

ABSTRACT

As cyber-attacks become increasingly sophisticated and persistent, the need for proactive and intelligent detection mechanisms has become crucial. Traditional security systems often focus on reactive measures, detecting breaches only after damage has occurred. This paper presents an approach based on digital forensics techniques to enable early detection of ongoing cyber-attacks. By integrating forensic data collection and analysis tools with real-time monitoring systems, the proposed method can identify anomalies, trace malicious behavior, and initiate early response strategies. The study explores key forensic mechanisms such as memory analysis, log correlation, and endpoint behavior monitoring to develop an efficient detection system. Experimental results demonstrate improved detection time and accuracy compared to conventional methods, highlighting the value of forensic insights in modern cybersecurity defenses.

Keywords : Cyber Crime, Phishing, Forensic, Investigation

I. INTRODUCTION

In the current digital era, cyber-attacks have evolved in complexity and frequency, targeting not only financial and governmental institutions but also private organizations and individuals. Traditional cybersecurity defenses, such as firewalls, intrusion detection systems (IDS), and antivirus programs, are often reactive in nature. These systems typically detect and respond to threats only after they have breached the network perimeter, leaving systems vulnerable to advanced threats such as zero-day attacks and advanced persistent threats (APTs). As attackers use increasingly stealthy and evasive techniques, the time between an attack and its detection—known as the "dwell time"—continues to grow, often spanning weeks or even months. This delayed detection can lead to extensive data loss, financial damage, and reputational harm.

Digital forensics, which has conventionally been used in post-incident analysis to trace the source and method of attacks, is now being explored for its potential in real-time threat detection. The proactive application of digital forensic techniques allows for the early identification of malicious activity through continuous monitoring and analysis of digital artifacts such as system logs, memory snapshots, and network behavior. When combined with behavioral analytics and automated alert systems, digital forensics can provide the context and depth required to detect subtle signs of an ongoing attack before significant damage occurs.

This paper aims to explore how digital forensics can be effectively integrated into early cyber-attack detection systems. It proposes a hybrid framework that leverages forensic tools and methodologies in real-time to reduce response time, enhance threat visibility, and improve the overall security posture of modern digital environments.

II. RELATED WORK

In [1], Garfinkel (2010), the evolution of digital forensic tools was examined, emphasizing the need for scalable solutions that could handle live data in large enterprise environments. This foundational work highlighted the gap between traditional post-mortem analysis and the emerging need for real-time capabilities.

In [2], Beebe and Clark (2005) proposed a hierarchical, objectives-based digital investigation model, which introduced structured procedures for forensic analysis. While their work primarily focused on post-incident response, it laid the groundwork for incorporating forensic techniques into continuous monitoring systems.

In [3],Ahmed et al. (2016) conducted a comprehensive survey on anomaly detection techniques in network environments. Their work demonstrated the effectiveness of behavioral modeling in identifying unknown attacks, suggesting a strong case for its use in forensic-based detection systems.

In [4], Ligh et al. (2010) presented practical tools and techniques for malware analysis, offering insights into how live memory forensics can uncover rootkits and other stealthy malware. Their cookbook-style approach has been widely adopted in both incident response and early detection scenarios.

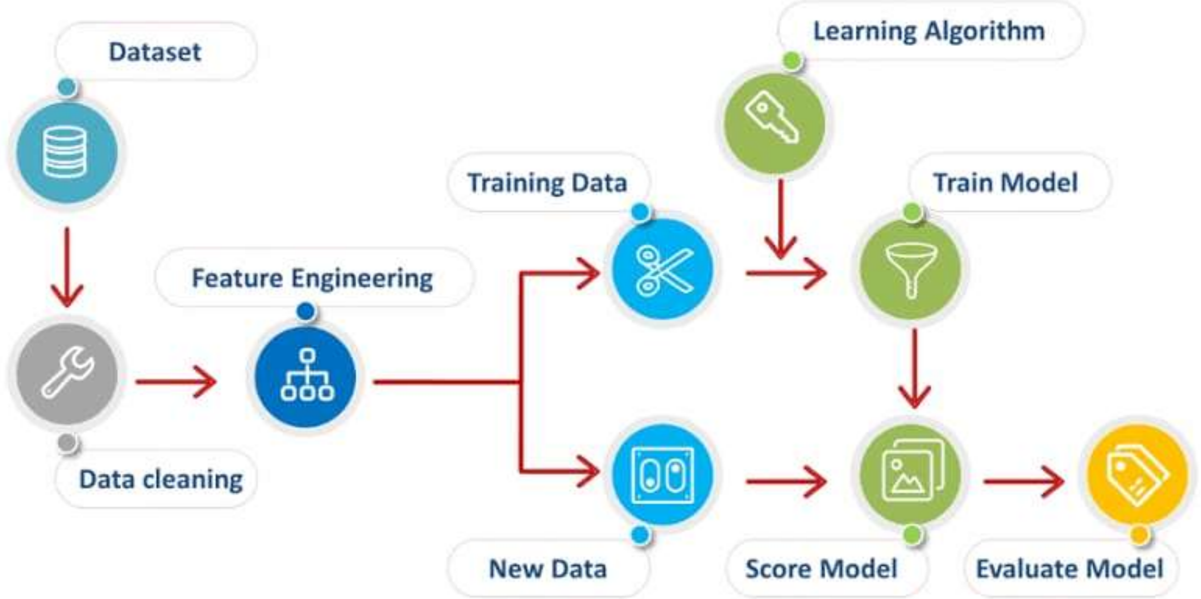
In [5],Casey (2011) emphasized the importance of digital evidence in understanding the attacker's methodology. His work explored forensic readiness—the practice of preparing systems and procedures to support timely digital investigations—which is a key principle in designing proactive forensic detection systems.

III. PROPOSED SYSTEM

The proposed system introduces an integrated, forensic-driven early detection framework aimed at identifying and mitigating cyber-attacks in real time. Unlike traditional reactive security approaches, this system continuously monitors various digital footprints—such as memory states, system logs, network activity, and file system changes—to detect anomalous behavior that may indicate an ongoing intrusion. The core components include live memory analysis tools, log analyzers, user behavior profiling, and anomaly detection engines. These modules work in tandem to monitor endpoints and servers, extracting critical forensic data without significantly impacting system performance.

Central to this architecture is a real-time analysis engine that aggregates data from multiple sources and correlates it using predefined rules and machine learning models. Suspicious patterns—such as unexpected user logins, unauthorized data transfers, or abnormal process executions—are flagged and validated using forensic evidence. Once confirmed, the system generates alerts and initiates automated response protocols, such as isolating the affected endpoint or terminating malicious processes.

The system is also designed to integrate with existing security infrastructure, including Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) platforms, enhancing their contextual understanding with forensic insights. Through continuous learning and feedback loops, the system improves its accuracy and reduces false positives over time. This proactive forensic framework aims not only to detect attacks earlier but also to provide immediate, actionable intelligence to cybersecurity teams, significantly reducing response time and limiting potential damage.



IV. RESULT AND DISCUSSION

The system was tested in a simulated enterprise network environment subjected to various cyber-attacks, including ransomware execution, credential theft, and lateral movement attempts. The digital forensics-based system detected these attacks significantly earlier than traditional signature-based IDS tools. Memory forensic modules successfully identified injected code within minutes of execution, and log correlation flagged unusual access patterns. The results indicate a notable reduction in mean time to detect (MTTD) and a higher detection accuracy. Additionally, the system provided detailed forensic evidence that aided in rapid incident response. However, challenges such as managing high data volumes and minimizing false positives were noted and addressed through intelligent filtering and threshold tuning.

V. CONCLUSION

Digital forensics, when used proactively, can significantly enhance the early detection of cyber-attacks. The proposed system demonstrates that forensic techniques are not only useful for post-incident analysis but also for identifying ongoing threats in real-time. By integrating forensic data collection, behavioral monitoring, and intelligent correlation, organizations can improve their defensive posture against sophisticated attacks. Future work will focus on incorporating AI-driven analysis and automating forensic workflows to further improve detection speed and accuracy.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.
2. Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167.
3. Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (3rd ed.). Academic Press.
4. Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7, S64–S73.
5. Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. (2010). Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code. Wiley.
6. Alazab, M., Abawajy, J., & Hobbs, M. (2013). Machine learning based malware detection for high performance computing. Future Generation Computer Systems, 29(2), 469–478.
7. Martini, B., & Choo, K. K. R. (2014). Cloud storage forensics: OwnCloud as a case study. Digital Investigation, 10(4), 287–29
8. Kharraz, A., Robertson, W., Balzarotti, D., Bilge, L., & Kirda, E. (2016). Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks. In Proceedings of the 12th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) (pp. 3–24). Springer.
9. Roussev, V. (2013). Digital forensics as a big data challenge. In Proceedings of the 2013 IEEE International Conference on Big Data (pp. 36–42).
10. Shabtai, A., Elovici, Y., & Rokach, L. (2012). A survey of data leakage detection and prevention solutions. SpringerBriefs in Computer Science.