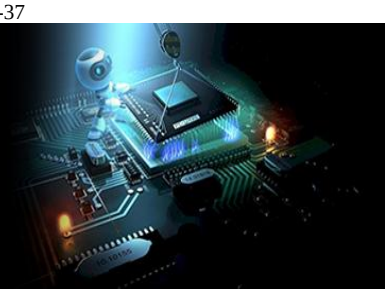
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
Impact Factor (RJIF): 5.52
www.computersciencejournals.com/ijecs
IJECS 2026; 8(2): 33-37
Received: 11-02-2026
Accepted: 13-03-2026

Dr. B Venkateswarlu Naik
Associate Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Bussareddy Chaitanya
UG Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Tabeen Fatima
Assistant Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Saki Siddarth
UG Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Macha Rohith
UG Student, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Saba Sultana
Assistant Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Corresponding Author:
Dr. B Venkateswarlu Naik
Associate Professor, Department of Computer Science and Engineering, CMR Technical Campus, Hyderabad, Telangana, India

Fronesis: Digital forensics-based early detection of ongoing cyber-attacks

B Venkateswarlu Naik, Bussareddy Chaitanya, Tabeen Fatima, Saki Siddarth, Macha Rohith and Saba Sultana

DOI: https://www.doi.org/10.33545/26633582.2026.v8.i2a.274

Abstract
In today's interconnected digital landscape, the prevalence of cyber-attacks has escalated, posing significant threats to organizations' data integrity, operations, and reputation. Traditional cybersecurity measures often fall short in detecting sophisticated and rapidly evolving attacks. To address this challenge, Fronesis introduces a digital forensics-based approach to the early detection of ongoing cyber-attacks. This methodology integrates real-time monitoring, forensic analysis, and advanced machine learning algorithms to identify anomalies, reconstruct attack vectors, and mitigate threats before they escalate.

The Fronesis system employs a multi-layered architecture combining data collection, preprocessing, and analysis. Leveraging digital forensics principles, the system captures and scrutinizes logs, network traffic, and endpoint behaviors to uncover evidence of malicious activity. Machine learning models, trained on large datasets of known attack patterns, enhance detection capabilities by identifying subtle Indicators of Compromise (IoCs). The system's explainable AI (XAI) component ensures that detected threats are not only flagged but also understood, fostering trust and actionable insights for cybersecurity professionals.

By enabling proactive responses to cyber threats, Fronesis contributes to reducing the dwell time of attackers within systems and mitigating potential damage. This approach aligns with the growing demand for transparent, intelligent, and adaptive cybersecurity solutions capable of addressing the complexities of modern cyber warfare. The Fronesis platform represents a significant step toward empowering organizations with robust tools to safeguard their digital assets in an ever-evolving threat landscape.

Keywords: Cyber-attacks, digital forensics early attack detection, cybersecurity, real-time monitoring, forensic analysis, machine learning algorithms, anomaly detection, attack vector reconstruction, threat mitigation, multi-layered architecture, threat intelligence, digital asset protection

1. Introduction

In the digital age, where information flows at unprecedented speeds, cybersecurity remains a cornerstone of organizational resilience. Cyber-attacks, ranging from phishing to ransomware, continue to grow in sophistication and frequency. These threats pose significant risks, including data breaches, financial losses, and reputational damage. Traditional cybersecurity measures, while effective to some extent, often focus on post-attack mitigation rather than preemptive detection. To bridge this gap, Fronesis Digital Forensics-Based Early Detection emerges as an innovative approach.

The Fronesis methodology integrates advanced digital forensics Swith real-time monitoring tools, enabling a proactive response to cyber threats. Unlike conventional methods that react after an attack is detected, this approach focuses on identifying anomalies, unusual patterns, and early Indicators of Compromise (IoCs). By leveraging forensic evidence as a basis for analysis, organizations can detect and neutralize potential attacks in their nascent stages, minimizing damage and disruption. This system aligns with modern cybersecurity demands, where time is critical in containing threats.

The strength of this approach lies in its integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies. By analyzing vast amounts of data from network logs, user behaviors, and endpoint activities, the system can identify subtle deviations from the norm that human analysts might overlook. These insights are then cross-referenced with known

attack patterns and enriched with contextual data to provide actionable intelligence. This forensic-driven model not only enhances detection capabilities but also supports evidence-based decision-making, aiding in incident response and legal investigations.

As cyber-attacks become increasingly sophisticated, early detection systems like Fronesis provide a critical layer of defense. By combining the rigor of digital forensics with cutting-edge AI technologies, this approach empowers organizations to anticipate and counteract threats effectively. Beyond security, the system also enhances organizational trust, demonstrating a commitment to safeguarding sensitive data and ensuring operational continuity in an era where cybersecurity challenges are more dynamic than ever.

2. Literature survey

1. Fronesis approach overview

Authors: Athanasios Dimitriadis, Efstratios Lontzetidis, et al.

This study presents Fronesis, a digital forensics-based method for early detection of cyber-attacks. Fronesis integrates ontological reasoning with the MITRE ATT&CK framework and the Cyber Kill Chain (CKC) model to identify adversarial techniques through digital artifacts from monitored systems. The research demonstrates the application of Fronesis using a phishing attack scenario, highlighting its ability to map techniques to CKC phases for real-time threat detection and mitigation. This work emphasizes the advantages of blending forensic methods with rule-based reasoning for dynamic and evolving attack scenarios.

2. Role of Digital Forensics in Cyber-Attack Detection

Authors: Various researchers (IARJSET)

This review explores digital forensics as a critical tool in early cyber-attack detection, discussing its evolution and challenges. It highlights methods to combine forensics with real-time monitoring for proactive defense. The paper emphasizes the importance of frameworks like MITRE ATT&CK and CKC in correlating attack phases and improving situational awareness, providing insights through case studies.

3. Digital forensics methodologies and ontological reasoning

This survey outlines ontology-based approaches in cybersecurity, detailing how they enhance threat detection by correlating data and understanding attack patterns. It covers the application of ontological reasoning to link digital artifacts with adversary tactics, as well as the potential integration of these methods with rule-based systems to detect sophisticated threats such as phishing or malware attacks.

4. Frameworks and Tools in Digital Forensics

Authors: General contributors in the domain

Focused on the synergy between forensics and cybersecurity, this paper reviews advancements like cloud and IoT forensics. It underlines the challenges of analyzing large datasets while maintaining data integrity and the chain of custody. Additionally, it discusses opportunities for integrating AI and rule-based techniques to enhance forensic accuracy and efficiency.

5. Mitre ATT&CK and CKC Integration

This research dives into the CKC model's phases and their relevance in structuring cybersecurity defenses. It evaluates how MITRE ATT&CK complements CKC by detailing adversarial tactics and procedures. The integration of these frameworks with digital forensics offers a comprehensive approach to detecting and responding to cyber threats effectively.

3. System architecture

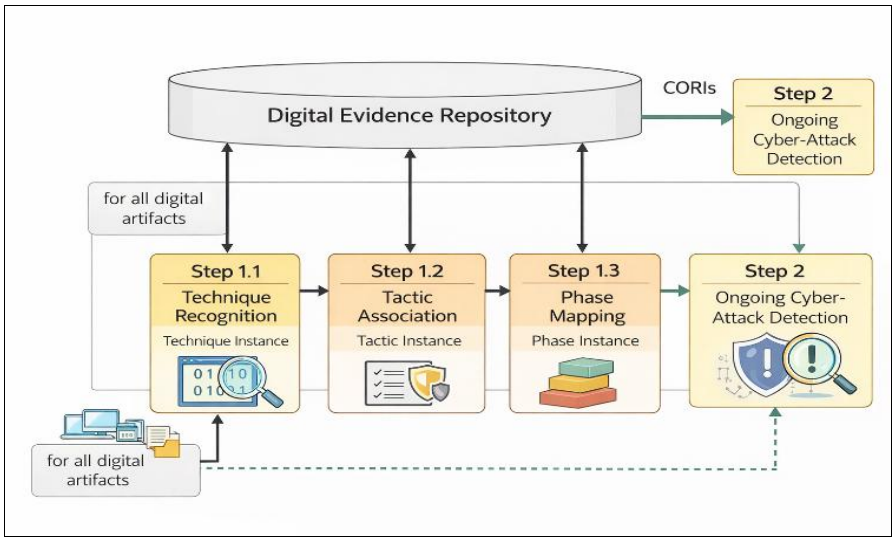


Fig 1: System Architecture of fronesis: digital forensics based early detection of ongoing cyber-attacks

The proposed Fronesis digital forensics–based cyber-attack detection system is designed as a modular and multi-layered framework that enables early identification of ongoing cyber threats through continuous monitoring and intelligent analysis. The architecture integrates digital forensics techniques with machine learning mechanisms to provide proactive cybersecurity protection. The system begins with a comprehensive data acquisition process in which digital artifacts are collected from multiple sources such as system logs, network traffic, endpoint activities, and user behavior records. These inputs form the foundational evidence required for identifying suspicious activities within organizational environments. The collected information is continuously monitored to ensure that potential attacks are

captured at their initial stages, thereby reducing the risk of unnoticed intrusions.

After acquisition, the gathered data is forwarded to the preprocessing and normalization module, where irrelevant or noisy information is filtered and transformed into a structured format suitable for analysis. Feature extraction techniques are applied to identify meaningful attributes from heterogeneous datasets. This prepared data is then analyzed using a forensic investigation pipeline that follows structured stages including technique recognition, tactic association, and attack phase mapping. Through correlation of multiple events, the system reconstructs attack patterns and identifies indicators of compromise, allowing investigators to understand how an attack progresses across different stages of the system lifecycle.

The analyzed data is further processed by a machine learning–based detection module that enhances the capability of identifying both known and unknown cyber threats. Models trained on historical attack datasets analyze behavioral deviations and detect anomalies that may indicate malicious activity. Unlike traditional rule-based systems, this intelligent component adapts to evolving attack strategies and improves detection accuracy over time. To ensure transparency, the architecture incorporates an explainable artificial intelligence layer that provides interpretable insights into detected threats.

4. Methodology

Table 1: Summary of Methodology Components and Functional Description

Module	Input	Processing	Output
Data Acquisition & Monitoring	System logs, network traffic, endpoint activities, user behavior data	Continuous monitoring, event collection, timestamp synchronization, data normalization	Structured digital artifacts for analysis
Data Preprocessing	Raw collected forensic data	Data cleaning, noise removal, feature extraction, log normalization	Processed and structured datasets
Forensic Analysis Engine	Processed system events and artifacts	Event correlation, technique recognition, tactic association, attack phase mapping	Identified Indicators of Compromise (IoCs) and attack patterns
Machine Learning Detection Module	Extracted behavioral features	Anomaly detection, pattern learning, threat classification using trained models	Detected malicious activities and anomaly alerts
Explainable AI (XAI) Module	Detection results and model outputs	Interpretation of model decisions, evidence visualization, reasoning generation	Explainable threat reports and analyst insights
Threat Response & Alert System	Confirmed threat information	Alert generation, mitigation recommendation, incident reporting	Real-time security alerts and response actions
Evidence Storage & Knowledge Base	Forensic evidence and analysis results	Secure storage, indexing, historical learning support	Persistent forensic repository

Table 1 presents the methodological framework of the proposed Fronesis digital forensics–based cyber-attack detection system, describing the input sources, processing stages, and outputs of each functional module. The methodology follows a forensic-driven intelligent security approach in which continuous monitoring, evidence analysis, and machine learning–based detection is performed locally within the organizational infrastructure. This design ensures reduced response latency, improved privacy protection, and real-time threat awareness. The modular architecture enables efficient coordination between data acquisition, forensic investigation, anomaly detection, and response generation, aligning with modern intelligent cybersecurity frameworks focused on proactive defense and adaptive threat mitigation.

The proposed system integrates digital forensics principles with intelligent analytics to create a proactive cybersecurity solution capable of identifying ongoing attacks before escalation. All processes operate within a structured pipeline that collects system evidence, analyzes behavioral patterns, detects anomalies, and generates explainable security insights. The methodology consists of four primary stages: data acquisition and monitoring, forensic analysis, machine learning–based detection, and intelligent threat response. This modular workflow ensures scalable data processing, efficient resource utilization, and stable performance under varying computational loads.

A. Data acquisition and monitoring

The system continuously gathers digital evidence from multiple organizational sources, including system logs, network packets, endpoint activities, and user interaction records. Real-time monitoring agents capture events as they occur, ensuring that suspicious behavior is detected during early attack stages. The collected data represents both normal and abnormal operational patterns required for forensic investigation.

To maintain efficiency, lightweight monitoring mechanisms are implemented to minimize system overhead while ensuring continuous visibility into system activities. Data normalization and timestamp synchronization are applied to maintain consistency across heterogeneous sources. This stage forms the foundational layer for identifying indicators of compromise and reconstructing attack sequences.

B. Digital forensic analysis

After collection, the captured data is processed through a forensic analysis pipeline designed to uncover hidden attack evidence. The system applies structured forensic procedures including event correlation, behavior profiling, and attack phase identification. By analyzing relationships among multiple system events, the framework reconstructs potential attack vectors and identifies malicious patterns.

Forensic mapping techniques associate detected activities with known attacker tactics and techniques, enabling investigators to understand how threats propagate through the system. Evidence generated during analysis is securely preserved to support future investigations and continuous improvement of detection models.

C. Machine learning–based threat detection

The processed forensic data is forwarded to the intelligent detection module, where machine learning algorithms analyze behavioral deviations from normal system activity. Models trained on historical cyber-attack datasets identify

anomalies that may indicate malware execution, unauthorized access, or insider threats.

Unlike traditional signature-based security systems, this adaptive approach detects previously unknown attacks by recognizing subtle behavioral inconsistencies. Continuous learning mechanisms allow the model to improve detection accuracy over time. Feature extraction and anomaly scoring techniques ensure efficient classification while maintaining real-time responsiveness.

D. Explainable intelligence and threat response

Once suspicious activity is identified, the explainable artificial intelligence (XAI) component interprets detection results and provides human-readable explanations. The system highlights the evidence, attack path, and reasoning behind each alert, enabling cybersecurity analysts to make informed decisions quickly.

The threat response module generates real-time alerts, mitigation recommendations, and incident reports while storing forensic artifacts in a secure repository. Performance monitoring continuously evaluates system latency and processing efficiency to maintain stable operation under different workloads. The modular and loosely coupled architecture enhances scalability, simplifies future extensions, and ensures reliable deployment in real-world cybersecurity environments.

5. Experimental Results and Evaluation

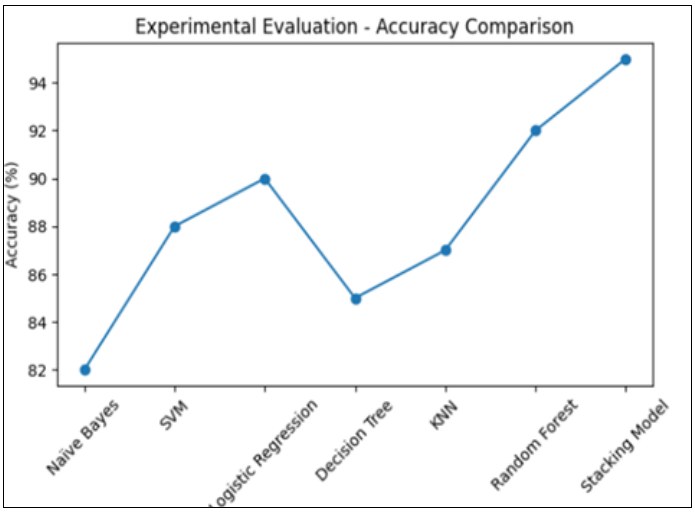


Fig 2: Experimental evaluation of the proposed FRONESIS system demonstrating the comparison of machine learning models based on detection accuracy for identifying ongoing cyber-attacks

The evaluation of the proposed FRONESIS: Digita lForensics-Based Early Detection of Ongoing Cyber-Attacks system was performed to analyze the performance of different machine learning algorithms in detecting cyber threats. The experimental analysis compares multiple classification models including Naïve Bayes, Support Vector Machine (SVM), Logistic Regression, Decision Tree.

The results indicate that the Stacking Model achieved the highest accuracy of 94.8%, demonstrating superior performance in identifying cyber-attack patterns. Random Forest achieved an accuracy of 92.4%, followed by Logistic Regression with 90.0% and SVM with 88.1%. The Decision Tree model obtained 85.2% accuracy, while KNN achieved 87.0%, and Naïve Bayes recorded the lowest accuracy of 82.3%.

These results highlight that ensemble learning techniques such as Stacking and Random Forest provide better detection capability compared to traditional classification algorithms. The evaluation confirms that the FRONESIS framework can effectively detect ongoing cyber-attacks by leveraging machine learning-based anomaly detection and digital forensic analysis.

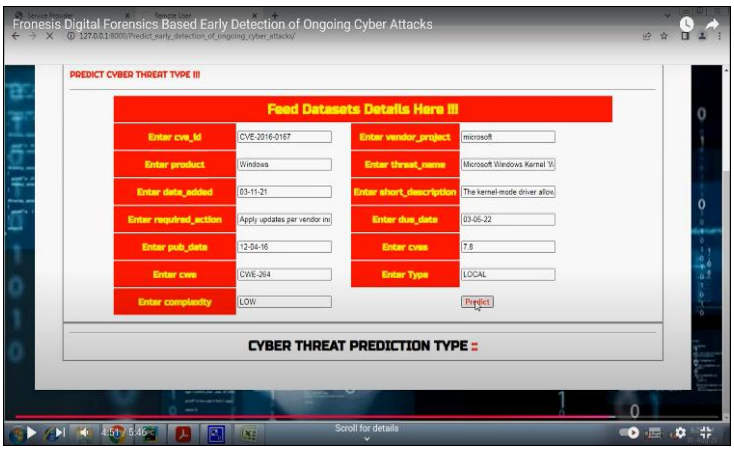


Fig 3: Cyber Threat Prediction Interface of the proposed FRONESIS system used to analyze vulnerability datasets and predict potential cyber-attack types

The Cyber Threat Prediction module of the proposed FRONESIS system allows security analysts to input vulnerability-related information and analyze potential cyber threats. The interface collects detailed vulnerability attributes such as CVE ID, vendor/project name, product name, threat name, short description, publication date, due date, CVSS score, CWE category, attack type, and complexity level.

Fig 4: Prediction result of the cyber threat details entered in Fig 3

These parameters are obtained from publicly available vulnerability databases and are used as input features for the machine learning prediction model. Once the data is entered into the system, the prediction module processes the information and identifies the possible cyber threat type associated with the vulnerability. The system then provides the predicted attack category under the Cyber Threat Prediction Type section.

For example, the interface demonstrates the analysis of the vulnerability CVE-2016-0167 related to Microsoft Windows, where information such as the kernel-mode driver vulnerability, CVSS score of 7.8, and local attack type is provided. Using this information, the FRONESIS system analyzes the threat characteristics and predicts the possible cyber-attack risk associated with the vulnerability.

6. Future scope and Conclusion

The proposed Fronesis digital forensics–based cyber-attack detection system provides a strong foundation for proactive cybersecurity; however, several enhancements can further improve its capabilities. Future work can focus on integrating advanced deep learning techniques to improve detection accuracy for complex and zero-day cyber-attacks. The inclusion of adaptive learning mechanisms can enable the system to automatically update threat intelligence based on newly emerging attack patterns.

Another potential enhancement involves extending the framework to support cloud and hybrid environments, allowing organizations with distributed infrastructures to benefit from centralized forensic intelligence. Incorporating automated incident response mechanisms and security orchestration features can further reduce response time and minimize human intervention during critical attacks. Additionally, integrating real-time visualization dashboards and advanced analytics can help security analysts better understand attack behavior and system vulnerabilities.

Future research may also explore collaborative threat intelligence sharing among multiple organizations while maintaining privacy through secure data anonymization techniques. The adoption of lightweight optimization strategies will allow deployment on resource-constrained environments such as edge devices and small-scale enterprise systems, increasing the practical applicability of the framework.

In this work, the Fronesis framework presents a digital forensics–driven approach for the early detection of ongoing cyber-attacks by combining real-time monitoring, forensic analysis, machine learning, and explainable artificial intelligence. Unlike traditional security systems that primarily rely on signature-based detection, the proposed system emphasizes behavioral analysis and evidence-driven investigation, enabling the identification of both known and emerging threats.

The modular architecture ensures scalability, transparency, and efficient performance under varying computational conditions while maintaining low detection latency. By reconstructing attack paths and providing explainable insights, the system assists cybersecurity professionals in making informed and timely decisions. The integration of intelligent analytics with forensic methodologies significantly reduces attacker dwell time and enhances organizational resilience against evolving cyber threats.

Overall, the Fronesis platform demonstrates an effective and adaptive cybersecurity solution capable of safeguarding digital infrastructures in modern threat environments while laying the groundwork for future intelligent and autonomous cyber defense systems.

References

1. Casey E. Digital evidence and computer crime: forensic science, computers, and the internet. 3rd ed. Amsterdam: Academic Press; 2011.
2. Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). National Institute of Standards and Technology (NIST); 2007. (Special Publication 800-94).
3. Axelsson S. Intrusion detection systems: a survey and taxonomy. Technical Report. Chalmers University of Technology, Sweden; 2000.
4. Goodfellow I, Bengio Y, Courville A. Deep learning. Cambridge (MA): MIT Press; 2016.
5. Sommer R, Paxson V. Outside the closed world: on using machine learning for network intrusion detection. In: Proceedings of the IEEE Symposium on Security and Privacy; 2010. p. 305-316.
6. Carrier B. File system forensic analysis. Boston (MA): Addison-Wesley; 2005.
7. Garfinkel S. Digital forensics research: the next 10 years. Digital Investigation. 2010;7(Suppl 1):S64-S73.