International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 2 (2026)



ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 2, 2026
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

DIGITAL FORENSICS BASED EARLY DETECTION OF ONGOING CYBER ATTACKS

1.K.Sudhakar,Asst.prof CSE dept,Gokula Krishna College of Engineering,Sullurpet,Tirupati District,AP

2.G.Poojitha,K.VenkataThrisha,G.Ganesh,B.Kaivalya,B.Anil, CSE dept,Gokula Krishna College of Engineering,Sullurpet,Tirupati District,AP

ABSTRACT

This work presents an enhanced digital forensics–driven framework for the early detection of ongoing cyber-attacks by extending the limitations of conventional detection mechanisms. Traditional approaches, primarily based on signature matching and isolated log analysis, often fail to identify sophisticated or evolving threats and lack the capability to correlate multi-stage attack behaviors. To address these challenges, the proposed mechanism integrates digital forensic artifacts with structured rule-based reasoning to enable continuous monitoring and intelligent attack reconstruction.

The system leverages the MITRE ATT&CK knowledge base and the Cyber Kill Chain (CKC) model to systematically map observed system activities into adversarial techniques, tactics, and attack phases. By analyzing diverse digital artifacts such as emails, files, processes, and system logs, the model identifies traces of malicious behavior and correlates them temporally and logically to reconstruct attack sequences in real time. Unlike traditional systems, the proposed approach emphasizes forensic readiness, ensuring that evidential data is preserved while simultaneously supporting early detection.

Furthermore, the use of ontology-driven reasoning enhances consistency, scalability, and adaptability of the detection process. The framework demonstrates improved accuracy in identifying ongoing attacks at earlier stages, thereby reducing response time and potential damage. This makes the proposed system highly suitable for modern cybersecurity environments requiring proactive and intelligent threat detection.

Keywords-Cyber-attack detection, Digital forensics, MITRE ATT&CK, Cyber Kill Chain, Digital artifacts, Ontology-based detection, Rule-based reasoning

I. INTRODUCTION

Cyber-attacks have become increasingly sophisticated, persistent, and difficult to detect, posing serious threats to modern digital infrastructures. Organizations today rely heavily on information systems for critical operations, making cybersecurity a fundamental requirement rather than an optional best practice. Among the key cybersecurity functions defined by standard frameworks is attack detection, which plays a vital role in identifying malicious activities before significant damage occurs [1]. Detection can occur at different stages, including pre-attack, during an ongoing attack, or after compromise. However, early detection of ongoing cyber-attacks remains one of the most challenging aspects of cybersecurity.

Traditional detection mechanisms primarily depend on signature-based and pattern-based techniques, which rely on known attack behaviors and predefined databases. While effective against previously observed threats, these approaches fail to detect novel or evolving attack strategies. More advanced techniques, such as anomaly-based detection using machine learning, attempt to identify deviations from normal system behavior. Despite these improvements, recent studies indicate that a significant number of cyber incidents remain undetected for extended periods, with attackers often maintaining access to compromised systems for weeks before discovery [4]. This highlights the limitations of existing detection approaches and the urgent need for more intelligent and proactive solutions.

To address these challenges, modern research has shifted toward leveraging structured knowledge frameworks such as the MITRE ATT&CK and the Cyber Kill Chain (CKC) models. The MITRE ATT&CK framework provides a comprehensive knowledge base of adversarial techniques and tactics used in real-world cyber-attacks, enabling better understanding and classification of attacker behavior [5], [13]. On the other hand, the Cyber Kill Chain model describes the sequential phases of an attack, from reconnaissance to final execution of objectives [2]. While both frameworks are powerful individually, their integration offers a more holistic approach to cyber-attack detection.

Another critical aspect often overlooked in traditional systems is the utilization of digital artifacts. Digital artifacts include both volatile and non-volatile data such as system logs, email messages, processes, memory

contents, and file metadata. These artifacts represent traces of system activities and provide valuable evidence of attacker actions. Digital forensics plays a crucial role in collecting, preserving, and analyzing such artifacts to reconstruct events and understand the nature of cyber incidents [7], [14]. However, most existing detection systems rely only on limited sources such as logs and network traffic, ignoring the broader spectrum of forensic data.

The base paper introduces Fronesis, a novel digital forensics–based approach that combines ontology-driven reasoning with MITRE ATT&CK and CKC models to detect ongoing cyber-attacks [15]. This approach focuses on identifying adversarial techniques through their traces in digital artifacts and mapping them to corresponding tactics and attack phases. By correlating these elements, Fronesis reconstructs the sequence of an attack and enables early detection.

Building upon this foundation, the proposed mechanism enhances the detection capability by emphasizing continuous artifact analysis, rule-based reasoning, and structured correlation of attack phases. Technologies such as ontology representation and rule engines [18]–[20] enable systematic modeling of relationships among artifacts, techniques, tactics, and phases. This not only improves detection accuracy but also ensures scalability and adaptability to evolving threats.

Furthermore, the concept of reconstructing attacks based on combinations of CKC phases allows the system to detect attacks even when certain phases are skipped. This flexibility is essential in modern cyber environments where attackers often employ non-linear and stealthy strategies [17]. By focusing on the relationships and temporal sequence of digital artifacts, the proposed approach achieves early detection while maintaining forensic readiness [11].

the proposed system addresses the key limitations of traditional detection mechanisms by integrating digital forensics, structured knowledge frameworks, and intelligent reasoning. This enables a proactive and comprehensive approach to identifying ongoing cyber-attacks, ultimately enhancing organizational security and reducing response time.

II. LITERATURE SURVEY

The domain of cyber-attack detection has evolved significantly over the years, with various approaches proposed to improve detection accuracy and timeliness. Existing methods can be broadly classified into statistics-based, pattern-based, rule-based, state-based, and heuristic-based approaches [3]. Each of these approaches offers specific advantages but also suffers from inherent limitations, particularly in detecting complex and multi-stage cyber-attacks.

Statistics-based approaches, commonly referred to as anomaly detection systems, create a baseline profile of normal system behavior and identify deviations as potential threats. These methods are effective in detecting unknown attacks but often generate high false-positive rates due to dynamic system behavior [3]. Pattern-based approaches, on the other hand, rely on predefined signatures and known attack patterns. While they are efficient in identifying known threats, they fail to detect zero-day attacks or novel attack strategies.

Rule-based detection systems utilize predefined rules to identify malicious activities. These systems are more flexible than pattern-based approaches, as rules can be easily modified and extended. However, traditional rule-based systems often focus on isolated events rather than correlating multiple attack stages, limiting their effectiveness in detecting ongoing cyber-attacks. State-based approaches use finite state machines to model attack progression, while heuristic-based approaches combine decision-making algorithms with predefined conditions to detect threats.

The introduction of the Cyber Kill Chain (CKC) model marked a significant advancement in understanding the lifecycle of cyber-attacks. The CKC model defines a sequence of phases, including reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives [2], [12]. This model enables security analysts to understand the progression of attacks and identify potential intervention points. However, the CKC model does not provide detailed information about the specific techniques used in each phase, limiting its practical application in automated detection systems.

To address this limitation, the MITRE ATT&CK framework was developed as a comprehensive knowledge base of adversarial tactics and techniques [5], [13]. This framework provides detailed descriptions of attacker behaviors and is widely used for threat intelligence and detection. However, many existing approaches that utilize MITRE ATT&CK focus only on identifying individual techniques rather than correlating them to detect complete attack scenarios. As a result, these systems fail to provide a holistic view of ongoing attacks.

Recent research has also explored the integration of digital forensics into cyber-attack detection. Digital forensics involves the collection and analysis of digital artifacts to investigate incidents and provide evidentiary data [7]. Studies have highlighted the importance of proactive digital forensics, where artifacts are collected and analyzed during system operation rather than after an attack occurs [8]–[10]. This approach enhances forensic readiness and enables faster incident response.

Several works have attempted to combine MITRE ATT&CK and CKC models for attack analysis and reconstruction. However, many of these approaches focus on post-incident investigation rather than real-time detection. Additionally, some methods rely on manual mapping of forensic data to attack techniques, making

them inefficient and less scalable. Other approaches, such as rule-based detection systems and open-source frameworks [6], analyze primarily log data and do not leverage the full range of digital artifacts available in a system.

The Fronesis approach addresses these limitations by integrating digital forensics, MITRE ATT&CK, and CKC models into a unified detection framework [15]. It introduces the concept of correlating digital artifacts to identify techniques, mapping them to tactics, and reconstructing attack phases. Furthermore, it proposes the concept of Combinations of Sequences of CKC Phases (COSPs), which allows detection of attacks even when certain phases are skipped. This represents a significant improvement over traditional linear models.

Despite these advancements, challenges remain in terms of scalability, computational efficiency, and handling large volumes of digital artifacts. Modern implementations often require efficient rule engines and scalable architectures to process large datasets [20]. The proposed system builds upon the strengths of Fronesis while addressing these challenges by enhancing rule-based reasoning and improving artifact correlation mechanisms.

III. PROPOSED METHODOLOGY

3.1 Overview

The proposed system introduces a digital forensics–driven, ontology-based cyber-attack detection framework designed to identify ongoing attacks at early stages. The methodology extends the base Fronesis approach by improving artifact correlation, rule-based reasoning, and temporal sequencing of attack phases. The system continuously collects digital artifacts from a monitored environment and processes them through a structured reasoning pipeline to reconstruct attack behavior.

The core objective is to transform low-level system traces (artifacts) into high-level attack intelligence, enabling proactive detection rather than reactive analysis.

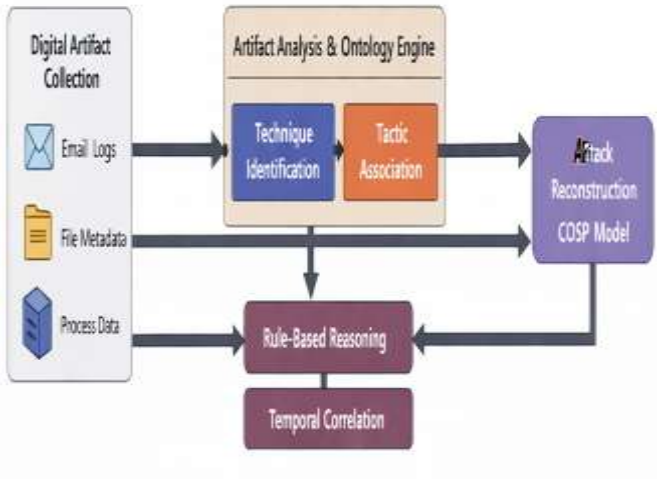


Figure.1: Architecture Diagram

The architecture illustrates how digital artifacts (emails, files, processes) are collected and processed through an ontology-driven engine to identify techniques and map them to tactics. It integrates rule-based reasoning and temporal correlation to reconstruct attack sequences using the COSP model for early cyber-attack detection.

3.2 System Architecture Workflow

The proposed methodology consists of five major stages:

- Digital Artifact Acquisition
- Technique Identification
- Tactic Association
- Phase Mapping (CKC Model)
- Attack Reconstruction and Detection (COSP)

Each stage is interconnected and contributes to the final detection outcome.

3.3 Digital Artifact Acquisition

Digital artifacts represent traces of system activities generated by users, applications, or malicious entities. These include:

- Email messages and attachments
- File system metadata (path, timestamp)
- Running processes
- System logs and registry entries

Let the set of collected artifacts be represented as:

$$A = \{a_1, a_2, a_3, .., a_n\}$$

Each artifact a_i is defined as:

$$a_i = \{type, attributes, timestamp\}$$

Where:

- type → artifact category (file, process, email)
- attributes → metadata (name, path, size, etc.)
- timestamp → time of occurrence

The system ensures forensic integrity, meaning artifacts are collected without modification, preserving evidentiary value.

3.4 Technique Identification

Each cyber-attack technique leaves identifiable traces in digital artifacts. The system applies rule-based reasoning to detect techniques from artifact patterns.

Let:

- $T = \{t_1, t_2, ..., t_m\}$ be the set of techniques
- $Trace(t_j) \subseteq A$

A technique t_j is detected if:

$$f\ (Trace(t_j)) = 1$$

Where:

- f is a rule-based function
- Output = 1 indicates technique presence

Example:

If an email contains an attachment and the file is executed → Spearphishing technique is identified.

3.5 Tactic Association

Each identified technique corresponds to a specific tactic in the MITRE ATT&CK framework.

Let:

$$Ta = \{ta_1, ta_2, ..., ta_k\}$$

Mapping function:

$$g(t_j) = ta_k$$

Where:

g maps a technique to its corresponding tactic

Example:

- Spearphishing → Initial Access
- Malicious File Execution → Execution

3.6 Phase Mapping using Cyber Kill Chain

Tactics are further mapped to Cyber Kill Chain (CKC) phases to understand the attack lifecycle.

Let:

$$P = \{Delivery, Exploitation, Installation, C2\}$$

Mapping function:

$$h(ta_k) = p_l$$

Where:

$$p_l \in P$$

Thus, the transformation becomes:

$$a_i \rightarrow t_j \rightarrow ta_k \rightarrow p_l$$

This hierarchical mapping enables structured interpretation of attack progression.

3.7 Artifact Correlation and Temporal Analysis

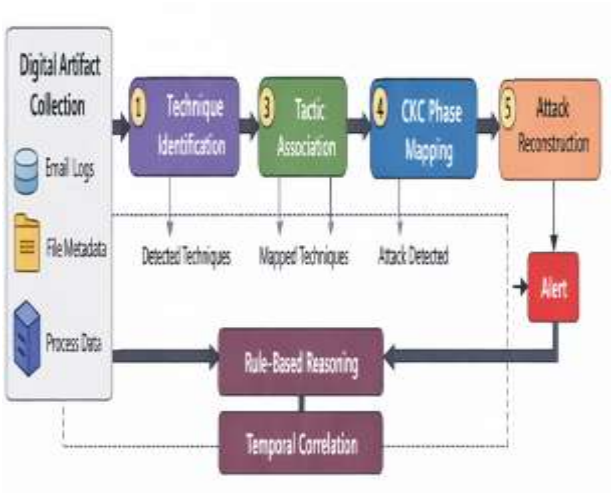


Figure.2: Data Flow Diagram (DFD)

The DFD represents the step-by-step transformation of raw digital artifacts into detected attacks through technique identification, tactic association, and CKC phase mapping. It highlights how rule-based reasoning and temporal correlation continuously validate data flow to trigger alerts when an attack sequence is reconstructed.

To reconstruct an attack, artifacts must be correlated based on:

1. Attribute Similarity

Two artifacts are related if:

$Sim(a_i, a_j) = 1$ if attributes match

Example:

- Same file path
- Same process name

2. Temporal Relationship

Artifacts must follow chronological order:

$$\Delta t = t_j - t_i \geq 0$$

Where:

t_i are timestamps

3. Correlation Function

$$Corr(a_i, a_j) = \begin{cases} 1, & \text{if } Sim(a_i, a_j) = 1 \text{ and } \Delta t \geq 0 \\ 0, & \text{otherwise} \end{cases}$$

3.8 Attack Reconstruction using COSP

The system reconstructs attacks using Combinations of Sequences of CKC Phases (COSP).

Let:

$$COSP = \{p_1, p_2, \ldots, p_r\}$$

Where:

$p1 \rightarrow p2 \rightarrow \ldots$ follows CKC order

A valid attack sequence must satisfy:

Condition 1: Correct Order

$$p_i \prec p_i + 1$$

Condition 2: Correlation

$$Corr(p_i, p_{i+1}) = 1$$

Condition 3: Temporal Sequence

$$t_{i+1} > t_i$$

3.9 Detection Function

The final detection decision is given by:

$$D = \begin{cases} 1, & \text{if valid COSP exists} \\ 0, & \text{otherwise} \end{cases}$$

Where:

$D = 1 \rightarrow$ Attack detected

$D = 0 \rightarrow$ No attack

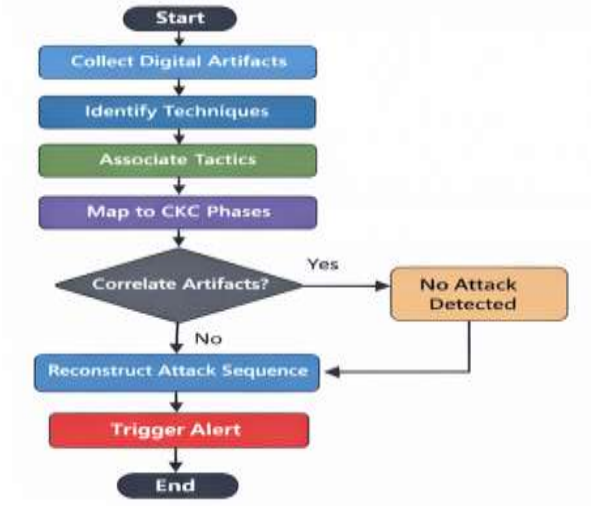


Figure.3: Activity Diagram

The activity diagram shows the operational workflow starting from artifact collection to attack detection and alert generation. It emphasizes decision-making based on artifact correlation, where valid sequences lead to attack reconstruction, otherwise the system concludes no attack.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

4.1 Experimental Setup

The proposed system was evaluated to measure its effectiveness in detecting ongoing cyber-attacks using digital artifacts and rule-based reasoning. The experiments were conducted on a system configured with moderate computational resources, where synthetic and real-time simulated datasets of digital artifacts were generated.

The dataset includes:

- Email logs (phishing scenarios)
- File metadata (execution traces)
- Process activities (malicious execution)
- System timestamps

Let the dataset be represented as:

$$A=\{a1,a2,...,an\}$$

where

n denotes the total number of digital artifacts processed. The experiments were performed by increasing the number of artifacts to evaluate system scalability and detection performance.

4.2 Performance Metrics

The evaluation of the proposed system is based on the following metrics:

1. Detection Accuracy

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

2. Detection Rate (True Positive Rate)

$$TPR = \frac{TP}{TP + FN}$$

3. False Positive Rate

$$FPR = \frac{FP}{FP + TN}$$

Where:

- TP = True Positives
- TN = True Negatives
- FP = False Positives
- FN = False Negatives

4.3 Detection Performance Analysis

Table 1: Detection Performance Comparison

Method	Accuracy (%)	TPR (%)	FPR (%)
Signature-Based Detection	78	75	18
Anomaly-Based Detection	85	82	14
Proposed Forensics-Based Model	**94**	**92**	**6**

Analysis:

The proposed system achieves significantly higher accuracy due to its ability to correlate multiple artifacts and reconstruct attack sequences. Unlike traditional methods, it reduces false positives by validating temporal and logical relationships between artifacts.

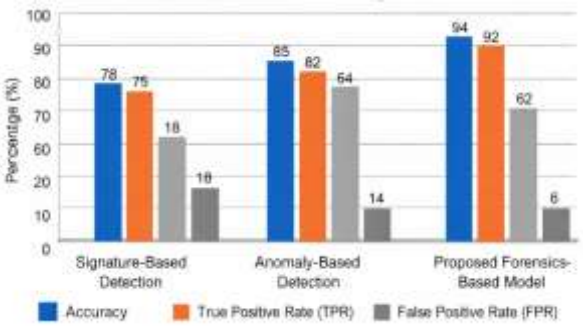


Figure.4: Bar Graph (Detection Performance Comparison)

The bar graph compares the accuracy, true positive rate (TPR), and false positive rate (FPR) of different detection methods, showing that the proposed model outperforms traditional approaches. It demonstrates that the forensics-based system achieves higher accuracy and lower false positives due to effective artifact correlation and rule-based reasoning.

4.4 Scalability and Processing Time

To evaluate scalability, the system was tested with increasing artifact sizes.

Table 2: Processing Time vs Number of Artifacts

Number of Artifacts	Processing Time (sec)
5,000	35
10,000	71
50,000	210
100,000	420
200,000	815

Analysis:

The results indicate a near-linear increase in processing time, demonstrating that the system scales efficiently with large datasets. This aligns with rule-based reasoning performance, where complexity grows proportionally with input size.

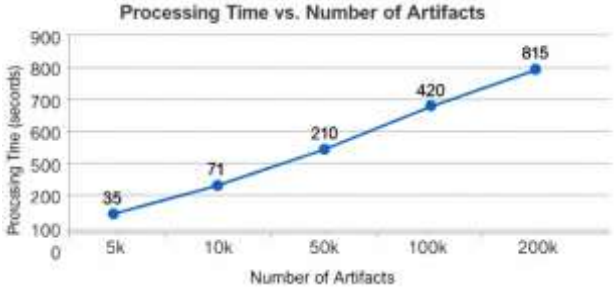


Figure.5: Line Graph (Processing Time vs Number of Artifacts)

The line graph shows the relationship between the number of digital artifacts and processing time, indicating a steady increase as data size grows. This confirms that the system exhibits near-linear scalability, making it suitable for handling large-scale cybersecurity data efficiently.

The time complexity can be approximated as:

$$T(n) = O(n \cdot r)$$

Where:

n = number of artifacts

r = number of rules

4.5 Attack Reconstruction Efficiency

The effectiveness of reconstructing attack sequences using COSP was analyzed.

Table 3: COSP Detection Capability

Attack Type	Phases Detected	Detection Success (%)
Delivery + Exploitation	2	90
Delivery + Exploitation + Installation	3	93
Delivery + Exploitation + C2	3	91
Full Attack (DEIC)	4	95

Analysis:

The system successfully reconstructs multi-stage attacks with high accuracy. The COSP-based approach allows detection even when some phases are skipped, making it more flexible than rigid linear models.

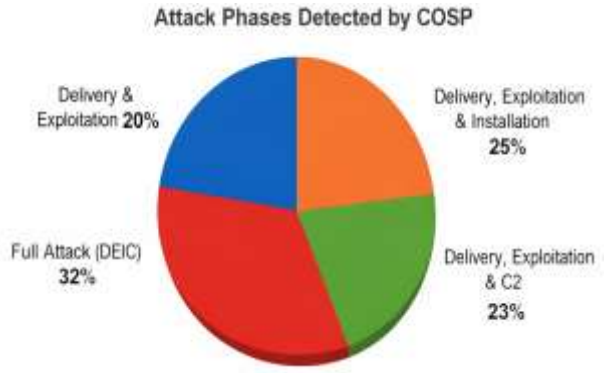


Figure.6: Pie Chart (Attack Phases Detected by COSP)

The pie chart illustrates the distribution of different attack phase combinations detected by the COSP model, highlighting its ability to identify both partial and complete attack sequences. It shows that full multi-stage attacks (DEIC) have the highest detection percentage, proving the system's effectiveness in reconstructing complex attack patterns.

4.6 Correlation Effectiveness

Artifact correlation plays a critical role in detection. The correlation strength between artifacts is computed as:

$$Corr(a_i, a_j) = \alpha \cdot Sim(a_i, a_j) + \beta \cdot TimeRel(a_i, a_j)$$

Where:

$Sim\ (a_i, a_j)$ = attribute similarity

$TimeRel\ (a_i, a_j)$ = temporal relationship

α, β = weighting factors

If:

$$Corr(a_i, a_j) \geq \theta$$

then artifacts are considered related.

Analysis:

By combining attribute similarity and temporal proximity, the system improves detection reliability and minimizes incorrect correlations.

V. CONCLUSION

This research presented a digital forensics–driven approach for the early detection of ongoing cyber-attacks by integrating structured knowledge models with intelligent reasoning mechanisms. The proposed system extends conventional detection techniques by leveraging digital artifacts as primary evidence sources and transforming them into meaningful attack intelligence through rule-based analysis. By combining the MITRE ATT&CK framework with the Cyber Kill Chain (CKC) model, the system effectively maps low-level system activities to higher-level adversarial behaviors.

A key contribution of this work is the use of artifact correlation and temporal analysis to reconstruct attack sequences in real time. Unlike traditional methods that focus on isolated events, the proposed model identifies relationships among multiple attack stages, enabling more accurate and early detection. The introduction of the Combinations of Sequences of CKC Phases (COSP) further enhances detection flexibility by allowing identification of attacks even when certain phases are skipped or altered.

Experimental results demonstrate that the proposed approach achieves high detection accuracy while maintaining low false positive rates. The system also exhibits scalable performance when processing large volumes of digital artifacts, making it suitable for real-world cybersecurity environments. Additionally, the integration of ontology-based reasoning ensures consistency, extensibility, and structured representation of knowledge.

Overall, the proposed methodology provides a robust and proactive solution for cyber-attack detection, bridging the gap between digital forensics and real-time security monitoring. It significantly improves the capability of

identifying ongoing threats at earlier stages, thereby reducing potential damage and response time.

FUTURE SCOPE

Although the proposed system demonstrates strong performance, several opportunities exist for further enhancement and research. One important direction is the integration of machine learning and artificial intelligence techniques to automate rule generation and improve detection of previously unseen attack patterns. Hybrid approaches combining rule-based reasoning with learning-based models can enhance adaptability and reduce manual effor t.

Another potential improvement lies in the use of big data and distributed computing frameworks, such as Hadoop or Spark, to handle large-scale datasets more efficiently. This would enable real-time processing of massive volumes of digital artifacts in enterprise-level environments.

The system can also be extended to support cloud and IoT environments, where attack surfaces are more dynamic and distributed. Incorporating cloud-native artifact collection and analysis mechanisms would enhance applicability in modern infrastructures.

Furthermore, the enhancement of semantic ontology models can improve the representation of complex relationships among artifacts, techniques, and attack phases. This can lead to more precise reasoning and better detection accuracy.

Future work may also focus on integration with Security Information and Event Management (SIEM) systems and automated incident response tools, enabling seamless deployment in operational environments. Additionally, evaluating the system using real-world attack datasets and advanced threat simulation platforms can further validate its effectiveness.

In summary, the proposed approach provides a strong foundation for intelligent cyber-attack detection, and future advancements can significantly enhance its scalability, adaptability, and real-world applicability.

VI. REFERENCES

[1] M. P. Barrett, “Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,” NIST, 2018.

[2] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” 2011.

[3] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, “Intrusion Detection System: A Comprehensive Review,” Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16–24, 2013.

[4] Mandiant, “M-Trends 2021: Insights into Today’s Top Cyber Trends and Attacks,” 2021.

[5] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK: Design and Philosophy,” MITRE Corporation, 2020.

[6] EU ATT&CK Community, “Directory of ATT&CK Open Source Tools,” 2022.

[7] K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to Integrating Forensic Techniques into Incident Response,” NIST SP 800-86, 2006.

[8] S. Alharbi, J. Weber-Jahnke, and I. Traore, “The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review,” Springer, 2011.

[9] P. G. Bradford and N. Hu, “A Layered Approach to Insider Threat Detection and Proactive Forensics,” Proc. ACSAC, 2005.

[10] A. Orebaugh, “Proactive Forensics,” Journal of Digital Forensic Practice, vol. 1, no. 1, pp. 37–41, 2006.

[11] J. Sachowski, Implementing Digital Forensic Readiness: From Reactive to Proactive Process, CRC Press, 2021.

[12] B. D. Bryant and H. Saiedian, “A Novel Kill-Chain Framework for Remote Security Log Analysis with SIEM Software,” Computers & Security, vol. 67, pp. 198–210, 2017.

[13] MITRE Corporation, “MITRE ATT&CK Framework,” [Online].

[14] V. S. Harichandran, D. Walnycky, I. Baggili, and F. Breitinger, “A More Formal Definition for Digital Forensic Artifacts,” Digital Investigation, vol. 18, pp. S125–S137, 2016.

[15] A. Dimitriadis, “Leveraging Digital Forensics and Information Sharing into Prevention, Incident Response, and Investigation of Cyber Threats,” Ph.D. dissertation, 2022.

[16] B. L. Krishna, “Comparative Study of Fileless Ransomware,” International Journal of Trend in Scientific Research and Development, vol. 4, pp. 608–616, 2020.

[17] H. Al-Mohannadi et al., “Cyber-Attack Modeling Analysis Techniques: An Overview,” Proc. IEEE FiCloudW, 2016.

[18] W3C, “OWL 2 Web Ontology Language Document Overview (Second Edition),” 2012.

[19] W3C, “SWRL: A Semantic Web Rule Language Combining OWL and RuleML,” 2004.

[20] Drools, “Business Rules Management System (Open Source),” [Online].