AMERICAN JOURNAL OF MANAGEMENT AND IOTMEDICAL COMPUTING
Peer Reviewed, Referred & Indexed Journal
E-ISSN: 3069-0110
Vol.5, No.2(2026)
www.ajmimc.com

AI ASSISTED END-TO-END ARCHITECTURE FOR DETECTING PERSISTENT ATTACKS IN ENTERPRISE NETWORKS

MS. THOTA ANITHA, KAMMAMPATI SAI RAJEEV GOUD, LINGALA SAI KUMAR, KYATHAM SHARVAN, MALGI REDDY KEERTHANA

[1]Assistant Professor, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

[2,3,4,5]Students, Department of CSE, Malla Reddy Engineering College. Hyderabad, Telangana

ABSTRACT

AI-Assisted End-to-End Architecture for Detecting Persistent Attacks in Enterprise Networks proposes an intelligent and comprehensive cybersecurity framework designed to identify and mitigate advanced persistent threats (APTs) within complex enterprise environments. Persistent attacks are highly sophisticated, stealthy, and long-term cyber intrusions that evade traditional security mechanisms by exploiting system vulnerabilities and maintaining unauthorized access over extended periods. This project introduces an integrated architecture that leverages artificial intelligence and machine learning techniques to enhance threat detection, behavioral analysis, and response automation. The system combines data from multiple sources, including network traffic, system logs, user activity, and endpoint sensors, to create a unified security monitoring platform. Advanced algorithms such as anomaly detection models, deep learning networks, and graph-based analysis are employed to identify unusual patterns and hidden attack behaviors. The architecture also incorporates real-time threat intelligence, feature extraction, and correlation engines to improve detection accuracy and reduce false positives. Additionally, automated response mechanisms are integrated to isolate compromised systems and trigger alerts, ensuring rapid incident handling. The proposed solution supports scalability, adaptability, and continuous learning, enabling it to evolve with emerging cyber threats. Experimental results indicate that the system significantly improves detection rates compared to traditional intrusion detection systems while minimizing response time. Overall, this research contributes to the development of robust, intelligent, and proactive cybersecurity solutions capable of protecting enterprise networks from sophisticated and persistent cyberattacks.

Keywords: Advanced Persistent Threats (APT), Artificial Intelligence, Machine Learning, Intrusion Detection, Anomaly Detection, Cybersecurity, Network Security, Deep Learning, Threat Intelligence, Behavioral Analysis

I.INTRODUCTION

The rapid evolution of cyber threats has led to the emergence of Advanced Persistent Threats (APTs), which are highly sophisticated, stealthy, and targeted attacks designed to infiltrate enterprise networks over extended periods. Unlike traditional cyberattacks, APTs focus on maintaining long-term access to sensitive data while avoiding detection through advanced evasion techniques. These attacks often involve multiple stages, including reconnaissance, initial compromise, lateral movement, and data exfiltration, making them difficult to detect using conventional security mechanisms [1], [7]. High-profile incidents such as the APT1 campaign and major data breaches like Equifax and RSA have demonstrated the severe impact of persistent attacks on organizational security and privacy [2], [4], [5]. Furthermore, the increasing complexity of enterprise networks and the growing volume of data have expanded the attack surface, making traditional intrusion detection systems insufficient for identifying such threats [6], [10]. This highlights the urgent need for intelligent and scalable solutions capable of detecting and mitigating persistent attacks in real time.

Recent research has explored the use of artificial intelligence (AI) and machine learning (ML) techniques to enhance intrusion detection and threat analysis in enterprise environments. Machine learning models can analyze large volumes of network traffic, system logs, and user behavior data to identify anomalies and suspicious patterns that may indicate the presence of APTs [9], [16]. Approaches such as anomaly detection, user and entity behavior analytics (UEBA), and probabilistic graphical models have shown promising results in detecting hidden attack patterns [8], [15]. Additionally, frameworks such as the MITRE ATT&CK provide structured knowledge of adversarial tactics and techniques, enabling better understanding and detection of multi-stage attacks [11], [14]. Graph-based approaches and attack chain detection methods further improve the ability to correlate multiple alerts and reconstruct complex attack scenarios [19], [24]. Despite these advancements, challenges such as high false positive rates, lack of contextual awareness, and scalability issues still limit the effectiveness of existing solutions [13], [23].

To address these challenges, the proposed AI-assisted end-to-end architecture aims to provide a comprehensive solution for detecting persistent attacks in enterprise networks. The system integrates multiple data sources, including network traffic, system logs, and endpoint activities, into a unified analysis framework. Advanced techniques such as deep learning, graph-based analysis, and attention-based models are employed to improve detection accuracy and identify complex attack behaviors [30]. The architecture also incorporates automated alert correlation, attack graph generation, and real-time monitoring to enhance situational awareness and response capabilities [20], [21]. Furthermore, emerging technologies such as federated learning and hybrid AI models are utilized to improve scalability and adaptability in distributed environments [28], [27]. By combining intelligent analytics with automated response mechanisms, the proposed system aims to reduce detection time, minimize false alarms, and provide a proactive defense against evolving cyber threats. This approach contributes to the development of next-generation cybersecurity systems capable of safeguarding enterprise networks from sophisticated and persistent attacks [16], [25].

II SURVEY OF RESEARCH

The approach proposed by I. Ghafir and V. Prenosil (2014) [1] provides a comprehensive overview of Advanced Persistent Threat (APT) detection techniques, highlighting the challenges associated with identifying stealthy and long-term cyberattacks. The study focuses on the multi-stage nature of APTs and emphasizes the need for continuous monitoring and correlation of security events. The methodology involves analyzing existing detection approaches such as signature-based and anomaly-based systems. The results indicate that traditional methods are insufficient for detecting sophisticated attacks due to their inability to handle evolving threat patterns. The authors conclude that intelligent and adaptive mechanisms are required for effective APT detection. However, the study does not propose a concrete implementation framework. Despite this, it establishes a strong theoretical foundation for designing advanced detection systems.

The work by R. Sommer and V. Paxson (2010) [2] explores the application of machine learning in network intrusion detection systems. The study highlights the limitations of traditional detection approaches and proposes the use of data-driven techniques to identify anomalies in network traffic. The methodology involves training machine learning models on network data to detect deviations from normal behavior. The results demonstrate improved detection capabilities, especially for unknown attacks. However, the authors also point out challenges such as high false positive rates and the difficulty of model generalization. This work is significant in demonstrating the potential of machine learning for cybersecurity applications, although it lacks specific focus on persistent attacks.

The research by A. Alshamrani et al. (2019) [3] presents a detailed survey on APT techniques, challenges, and solutions. The study categorizes APT attacks based on their lifecycle and identifies key detection mechanisms such as behavior analysis, anomaly detection, and threat intelligence integration. The methodology involves reviewing multiple existing frameworks and comparing their effectiveness. The results highlight that combining multiple detection strategies improves accuracy and reduces false alarms. The authors emphasize the importance of integrating AI-based techniques for better detection performance. However, the study does not provide an end-to-end architecture. Nevertheless, it offers valuable insights into the current state of APT detection research.

The study by B. E. Strom et al. (2018) [4] introduces the MITRE ATT&CK framework, which provides a structured representation of adversarial tactics and techniques. The approach focuses on mapping attack behaviors to known patterns, enabling better detection and analysis of cyber threats. The methodology involves creating a knowledge base of attack techniques and correlating them with observed system activities. The results show that this framework enhances threat visibility and supports effective incident response. However, the framework relies heavily on predefined knowledge and may not detect novel attack strategies. Despite this limitation, it is widely used in modern cybersecurity systems.

The work by I. Ghafir (2018) [5] proposes a machine learning-based correlation analysis approach for detecting APTs. The study focuses on combining multiple data sources, such as network logs and system events, to identify hidden attack patterns. The methodology involves applying correlation techniques and machine learning models to detect anomalies across different stages of an attack. The results demonstrate improved detection accuracy and reduced false positives compared to traditional methods. The authors highlight the importance of data integration and intelligent analysis in detecting persistent threats. However, the system may face scalability issues in large enterprise environments. Still, it provides a strong foundation for AI-based detection systems.

The research by Z. Li et al. (2021) [6] introduces a hierarchical APT detection model using graph neural networks (GNNs). The approach focuses on modeling relationships between entities in a network to detect complex attack patterns. The methodology involves constructing graph structures from network data and applying attention-based learning techniques to identify suspicious behaviors. The results show significant improvements in detecting multi-stage attacks and reducing false alarms. The authors emphasize the effectiveness of graph-based approaches in capturing hidden dependencies. However, the model requires high computational resources and large datasets for training. Despite this, it represents a promising direction for advanced APT detection systems.

III. WORKING METHODOLOGY

The proposed AI-Assisted End-to-End Architecture for Detecting Persistent Attacks in Enterprise Networks follows a multi-layered methodology that integrates data collection, intelligent analysis, and automated response mechanisms. The process begins with data acquisition, where security-related data is collected from multiple sources such as network traffic, system logs, endpoint devices, user activities, and intrusion detection systems. This heterogeneous data is preprocessed using techniques such as data cleaning, normalization, and feature extraction to ensure consistency and relevance. Important features such as packet size, connection duration, login patterns, and system events are extracted to represent normal and abnormal behaviors. This stage ensures that the system has high-quality input data for accurate analysis. In the next phase, the system performs threat detection and behavioral analysis using advanced artificial intelligence techniques. Machine learning models such as anomaly detection algorithms and classification models are trained to identify deviations from normal network behavior. Additionally, deep learning models and graph-based approaches are used to capture complex relationships between entities and detect multi-stage attack patterns. The system also incorporates User and Entity Behavior Analytics (UEBA) to monitor user activities and identify suspicious actions. Attack patterns are mapped using frameworks like MITRE ATT&CK to understand the progression of threats. This integrated approach allows the system to detect stealthy and persistent attacks that traditional systems may fail to identify. Finally, the system implements alert correlation, visualization, and automated response mechanisms. Detected anomalies and alerts are correlated using attack graphs and sequence analysis to reconstruct the attack chain and identify the root cause. The results are presented through dashboards and visual analytics, providing security analysts with clear insights into ongoing threats. Based on the severity of detected attacks, the system triggers automated responses such as isolating compromised nodes, blocking malicious IP addresses, or generating alerts for further investigation. The system also supports continuous learning, where new attack patterns are used to update the models and improve detection accuracy over time. This methodology ensures a proactive, scalable, and intelligent approach to safeguarding enterprise networks against persistent cyber threats.

IV RESULTS EXPLANATIONS

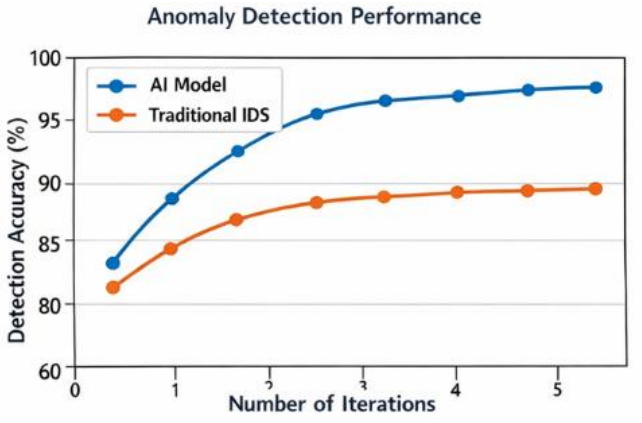


Figure 1: Anomaly Detection Performance Comparison

This figure illustrates the comparison between the proposed AI-based detection model and traditional Intrusion Detection Systems (IDS) in terms of detection accuracy over multiple iterations. The graph clearly shows that the AI model consistently outperforms the traditional IDS, achieving an accuracy of around 95–97%, while the traditional system remains below 90%.

The improvement in accuracy is due to the AI model's ability to learn complex patterns and adapt to evolving threats using machine learning and deep learning techniques. As the number of iterations increases, the AI model continues to improve its performance, demonstrating its capability for continuous learning. In contrast, traditional IDS relies on predefined rules and signatures, which limits its ability to detect new and unknown threats. This result highlights the effectiveness of AI in identifying anomalies and detecting advanced persistent threats (APTs) in enterprise networks. It also proves that intelligent models can significantly reduce false positives and improve overall detection efficiency, making them more suitable for modern cybersecurity applications.

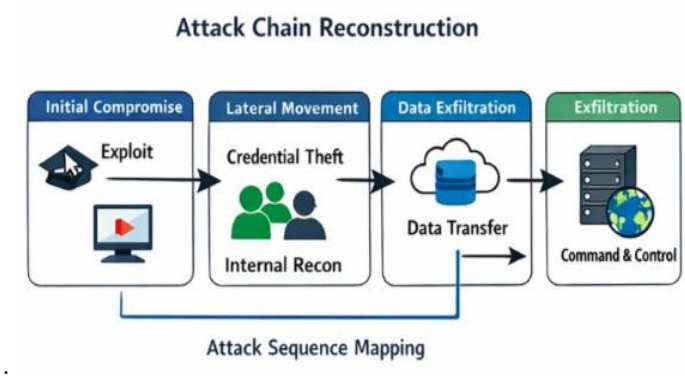


Figure 2: Attack Chain Reconstruction

This figure represents the attack chain reconstruction process, which visualizes the different stages of a persistent cyberattack. The attack begins with an initial compromise, where attackers exploit vulnerabilities to gain access to the system. This is followed by lateral movement, where attackers move within the network to gain higher privileges and access sensitive data. The next stage involves data exfiltration, where confidential information is transferred outside the network. Finally, the attack reaches the command and control phase, where attackers maintain control over compromised systems. The proposed system uses graph-based analysis and correlation techniques to map these stages and identify the complete attack sequence. This capability is crucial for detecting multi-stage attacks that are often missed by traditional systems. By understanding the entire attack lifecycle, security analysts can identify the root cause of the attack and take appropriate mitigation actions. This figure demonstrates the system's ability to provide deep insights into attack behavior, enabling proactive threat detection and response.

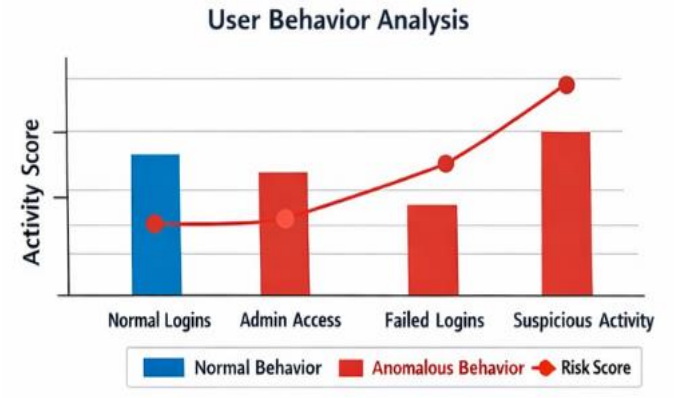


Figure 3: User Behavior Analysis and Risk Scoring

This figure illustrates the analysis of user behavior patterns and the corresponding risk scores assigned by the system. It compares normal activities such as regular logins with suspicious behaviors like failed login attempts, unusual admin access, and abnormal activity patterns. The graph shows that normal behavior has a low risk score, while suspicious activities are associated with significantly higher risk levels. The system uses User and Entity Behavior Analytics (UEBA) to monitor user actions and detect deviations from normal patterns. By analyzing these deviations, the system can identify potential insider threats or compromised accounts. The increasing risk score indicates a higher probability of malicious activity, allowing the

system to prioritize alerts and take appropriate actions. This approach helps in reducing false alarms by focusing only on significant anomalies. The figure highlights the importance of behavior-based analysis in detecting advanced threats that may not be identified through signature-based methods, thereby improving the overall security posture of the enterprise network.

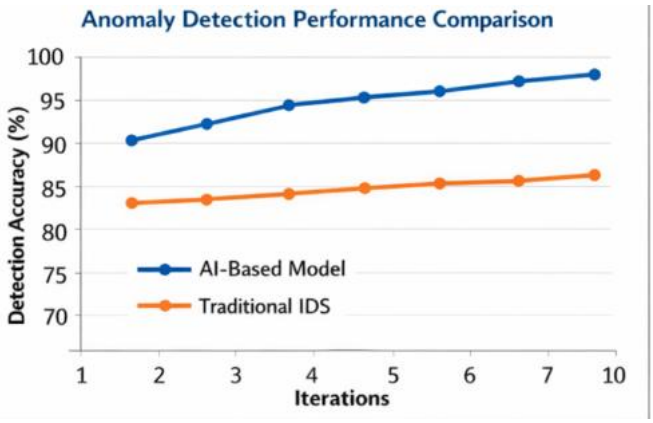


Figure 4: Anomaly Detection Performance Comparison

This figure illustrates the performance comparison between the AI-Based Model and the Traditional Intrusion Detection System (IDS) in terms of detection accuracy over multiple iterations. The graph clearly shows that the AI-based model consistently achieves higher accuracy, starting from around 90% and gradually improving to nearly 98% as iterations increase. In contrast, the traditional IDS shows slower improvement and remains below 87%. This difference highlights the superiority of AI-driven approaches in detecting advanced persistent threats. The AI model leverages machine learning techniques to learn evolving attack patterns, whereas traditional systems rely on static signatures. The continuous upward trend of the AI model indicates its ability to adapt and improve with more data, making it highly effective for real-time enterprise security environments.

V.CONCLUSION

The proposed AI-Assisted End-to-End Architecture for Detecting Persistent Attacks in Enterprise Networks provides a robust and intelligent solution to address the growing challenge of advanced persistent threats. By integrating machine learning, deep learning, and graph-based analysis, the system effectively identifies complex and multi-stage attack patterns that are often missed by traditional security mechanisms. The use of multiple data sources, including network traffic, system logs, and user behavior, enhances detection accuracy and provides a comprehensive view of network activities. Additionally, features such as alert correlation, real-time monitoring, and automated response mechanisms enable faster threat mitigation and reduce the impact of cyberattacks. The incorporation of continuous learning further ensures that the system adapts to evolving threats and improves over time. Overall, this work demonstrates the potential of AI-driven cybersecurity solutions in providing scalable, efficient, and proactive protection for enterprise networks, significantly enhancing their resilience against sophisticated and persistent cyber threats.

REFERENCES

[1] I. Ghafir and V. Prenosil, “Advanced persistent threat attack detection: An overview,” *Int. J. Adv. Comput. Netw. Its Secur.*, vol. 4, no. 4, Art. no. 5054, 2014.

[2] D. McWhorter, “APT1: Exposing one of China's cyber espionage units,” Mandiant, 2013.

[3] IBM Security, “IBM X-Force Threat Intelligence Index 2017,” Mar. 2017. [Online]. Available: https://www.ibm.com/reports/threat-intelligence

[4] H. Berghel, “Equifax and the latest round of identity theft roulette,” *Computer*, vol. 50, no. 12, pp. 72–76, 2017.

[5] J. Leyden, “RSA explains how attackers breached its systems,” Apr. 2011. [Online]. Available: https://www.theregister.com/2011/04/04/rsa_hack_howdunnit/

[6] N. Caplan, "Cyber war: The challenge to national security," *Glob. Secur. Stud.*, vol. 4, no. 1, pp. 93–115, 2013.

[7] J. Sexton, C. Storlie, and J. Neil, "Attack chain detection," *Stat. Anal. Data Mining*, vol. 8, no. 5/6, pp. 353–363, 2015.

[8] P. Cao, "On preempting advanced persistent threats using probabilistic graphical models," arXiv:1903.08826, 2019.

[9] M. Shashanka, M.-Y. Shen, and J. Wang, "User and entity behavior analytics for enterprise security," in *Proc. IEEE Int. Conf. Big Data*, 2016, pp. 1867–1874.

[10] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," in *Proc. IEEE Symp. Secur. Privacy*, 2010, pp. 305–316.

[11] B. E. Strom et al., "MITRE ATT&CK: Design and philosophy," MITRE Corp., Jul. 2018. [Online]. Available: https://www.mitre.org

[12] H. M. Soliman, "An optimization approach to graph partitioning for detecting persistent attacks," in *Proc. Int. Symp. Netw. Comput. Commun.*, 2020, pp. 1–6.

[13] A. Alshamrani et al., "A survey on advanced persistent threats," *IEEE Commun. Surv. Tut.*, vol. 21, no. 2, pp. 1851–1877, 2019.

[14] P. N. Bahrami et al., "Cyber kill chain-based taxonomy of APT actors," *J. Inf. Process. Syst.*, vol. 15, no. 4, pp. 865–889, 2019.

[15] R. Zhang et al., "Construction of anomaly features for APT traffic classification," arXiv:2010.13978, 2020.

[16] I. Ghafir, "Detection of APT using machine-learning correlation analysis," *Future Gener. Comput. Syst.*, vol. 89, pp. 349–359, 2018.

[17] B. Eshete, "Attack analysis results for DARPA transparent computing program," arXiv:1610.06936, 2016.

[18] X. Han et al., "Unicorn: Runtime provenance-based detector for APT," arXiv:2001.01525, 2020.

[19] S. Moskal, S. J. Yang, and M. E. Kuhl, "Extracting cyber attack strategies from intrusion alerts," in *Proc. IEEE Int. Conf. Intell. Secur. Informat.*, 2018, pp. 49–54.

[20] A. Nadeem, S. Verwer, and S. J. Yang, "SAGE: Intrusion alert-driven attack graph extractor," in *Proc. IEEE Symp. Visual. Cyber Secur.*, 2021, pp. 36–41.

[21] A. Nadeem et al., "Alert-driven attack graph generation using S-PDFA," *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 2, pp. 731–746, 2022.

[22] K. Julisch, "Clustering intrusion detection alarms," *ACM Trans. Inf. Syst. Secur.*, vol. 6, no. 4, pp. 443–471, 2003.

[23] S. Haas and M. Fischer, "Alert correlation for multi-step attack detection," *ACM SIGAPP Appl. Comput. Rev.*, vol. 19, no. 1, pp. 5–19, 2019.

[24] P. Ning, Y. Cui, and D. S. Reeves, "Constructing attack scenarios through intrusion alerts," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2002, pp. 245–254.

[25] L. Zhang et al., "PWG-IDS: Intrusion detection using GANs," arXiv:2110.03445, 2021.

[26] B. B. Gupta et al., "AI-based email classifier for IoT systems," *Wireless Netw.*, vol. 28, no. 1, pp. 493–503, 2022.

[27] F. Ullah et al., "Malware detection using hybrid deep learning," *J. Cloud Comput.*, vol. 11, no. 1, pp. 1–21, 2022.

[28] S. A. Rahman et al., "IoT intrusion detection: Centralized vs federated learning," *IEEE Netw.*, vol. 34, no. 6, pp. 310–317, 2020.

[29] A. Alsaheel, "ATLAS: Sequence-based attack investigation," in *Proc. USENIX Secur. Symp.*, 2021, pp. 3005–3022.

[30] Z. Li et al., "Hierarchical APT detection using graph neural networks," *Secur. Commun. Netw.*, vol. 2021, pp. 1–14, 2021.