Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/145/2025.21899

Artificial Intelligence-Driven Cybersecurity Visualization and Animation Technology: From Threat Perception to Decision Support

Zhiwei Guan[1,a,*]

[1]*Anhui University, Hefei, China*
a. chihwei.guan@gmail.com
**corresponding author*

Abstract: In the face of escalating complexity and scale of cyber attacks, traditional cybersecurity analysis methods are overwhelmed by the volume, dynamism, and complexity of data. Artificial Intelligence (AI), with its prowess in threat detection, behavioral analysis, and automated response, offers a beacon of hope. However, the "black box" nature of AI complicates trust in its decision-making. Concurrently, computer animation and data visualization emerge as powerful tools for intuitive and interactive data interpretation. This paper explores the synergy between AI and animation in cybersecurity, aiming to enhance analysis efficiency and decision transparency. Through a comprehensive review of AI applications in cybersecurity, the role of computer animation and visualization, and their integrated potential, we highlight the transformative impact of these technologies. The study also addresses technical challenges and future directions, emphasizing the practical significance across education, corporate, and national security contexts. Ultimately, the integration of AI and animation stands to revolutionize cybersecurity, making it more efficient, understandable, and user-friendly.

Keywords: Artificial Intelligence, Cybersecurity, Visualization, Animation, Decision Support

1. Introduction

In the rapidly evolving landscape of cybersecurity, the complexity and sophistication of cyber threats have surged, posing significant challenges to traditional security methodologies. These conventional approaches, often overwhelmed by the sheer volume and dynamic nature of data, necessitate a paradigm shift towards more efficient and transparent solutions. This research delves into the integration of Artificial Intelligence (AI) and computer animation technologies as a novel approach to enhance cybersecurity visualization, thereby addressing the critical need for improved threat perception and decision support.

The choice of this research topic is driven by the pressing need to bridge the gap between advanced AI capabilities and the human understanding of cyber threats. AI, with its ability to detect, classify, and respond to threats at unprecedented speeds, remains hindered by its "black box" nature, which complicates trust and understanding among security professionals. Conversely, computer animation and visualization technologies offer a compelling solution to this challenge by transforming complex data into intuitive, interactive formats that can be easily comprehended. For instance, consider the

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/145/2025.21899

case of network traffic visualization. Traditional methods of analyzing network traffic data often involve sifting through vast amounts of log files, a process that is both time-consuming and prone to human error. By employing computer animation, security personnel can visualize traffic patterns in real-time, with anomalies highlighted through dynamic displays. This not only accelerates the identification of potential threats but also enhances the overall understanding of attack vectors and their evolution over time. Moreover, the simulation of attack paths using animation technology provides a vivid representation of an attacker's journey through a network. This visual narrative aids analysts in grasping the intricacies of attack strategies, thereby enabling more effective countermeasures. Such simulations, when combined with AI-driven predictive analytics, can forecast potential attack scenarios, allowing for proactive defense strategies.

The significance of this research lies in its potential to revolutionize cybersecurity practices. By integrating AI with animation, we aim to create a more efficient, transparent, and user-friendly cybersecurity environment. This approach not only enhances the ability of security professionals to detect and respond to threats but also fosters a deeper understanding of the underlying complexities of cyber attacks. Ultimately, the integration of these technologies promises to pave the way for innovative solutions in the ongoing battle against cyber threats, ensuring a more secure digital future.

2. Literature reviews

2.1. The application of AI in cybersecurity

The application of artificial intelligence (AI) in cybersecurity is gradually becoming a core means to address complex threats. Firstly, in the area of threat detection and classification, machine learning-based anomaly detection technologies have made significant progress[1]. For instance, deep learning models such as LSTM are widely used in detecting anomalies in network traffic, effectively identifying known and unknown attack patterns[2]. In recent years, the introduction of graph neural networks (GNN) has further enhanced the threat analysis capabilities in complex network topologies, as GNN can more accurately locate potential sources of attacks by capturing the relationships between nodes[3]. Secondly, in the field of behavioral analysis and prediction, AI technologies can effectively identify internal threats and anomalous activities by analyzing user behavior patterns. Behavior modeling methods based on reinforcement learning can dynamically adjust detection strategies, while the introduction of time series analysis enables the system to predict potential attacks and deploy defensive measures in advance. Finally, in terms of automated response, AI-driven security orchestration and automated response (SOAR) systems are transforming traditional security operations models[4]. Rule-based automated response systems have been widely applied in practice, and the integration of dynamic response strategy generation technologies using generative AI, such as GPT, further enhances the system's flexibility and adaptability[5]. The application of these AI technologies not only improves the efficiency of detection and response in cybersecurity but also provides new solutions to address the increasingly complex threat environment.

2.2. Application of Computer Animation and Visualization in Cybersecurity: Intuitive Analysis

The application of computer animation and visualization technology in the field of cybersecurity provides intuitive and efficient means for understanding and analyzing complex data. Firstly, in the area of network traffic visualization, real-time traffic monitoring and dynamic display technologies assist security personnel in quickly identifying abnormal traffic patterns. Force-directed graph-based network topology visualization methods have been widely adopted, clearly illustrating the connections between network nodes[6]. Furthermore, using animation technology to display the changes in traffic anomalies enhances the comprehensibility of dynamic threats, enabling security

DOI: 10.54254/2755-2721/145/2025.21899

personnel to more intuitively track the evolution of abnormal behaviors. Secondly, in the simulation of attack path animations, animation technology is employed to simulate the intrusion paths of attackers, aiding analysts in understanding the behavioral logic of the attackers[7]. Path visualization methods based on attack graphs provide a theoretical foundation for this field[8], while immersive attack scenario displays that incorporate virtual reality (VR) technology allow analysts to observe the attack process as if they were present, enhancing the depth and efficiency of threat analysis. Lastly, in the timeline display of security incidents, timeline animations are used to illustrate the development process of security events, assisting security teams in clarifying the chronological order and causal relationships of events[9]. Timeline-based security log analysis tools have been widely applied in practice, and the introduction of interactive timelines further enhances user experience, supporting users in dynamically exploring event details to gain a more comprehensive understanding of the overall information regarding security incidents. The combination of these technologies not only enhances the intuitiveness and interactivity of cybersecurity analysis but also provides innovative solutions for addressing complex threats.

2.3. The Combination of AI and Animation: Interactive Tools

The combination of artificial intelligence (AI) and animation technology has opened new research directions in the field of cybersecurity, significantly enhancing the intuitiveness and interactivity of threat analysis. In ‘dynamic attack scenario generation’, AI technology generates diverse attack scenarios through models such as Generative Adversarial Networks (GANs) and presents them using animation technology, allowing security personnel to visually observe the attack process[10]. The integration of physics engines to create realistic attack animations further enhances the authenticity of the scenarios, providing an immersive experience for security training and education. In the development of ‘interactive security data visualization tools’, the combination of AI and animation technology supports real-time threat analysis, assisting security personnel in quickly identifying and responding to threats. WebGL-based interactive visualization tools have been widely applied in practice, and the introduction of natural language interaction (such as ChatGPT) has significantly improved user experience, enabling non-technical users to interact with the system through natural language commands, thereby lowering the usage threshold. In terms of ‘explainable AI and animation integration’, animation technology is utilized to visualize the decision-making process of AI models, enhancing the interpretability and transparency of the models. Explainable AI methods based on LIME and SHAP provide a theoretical foundation for this field, while using animation to demonstrate the reasoning paths of AI models in threat detection further increases user trust in model decisions[11]. The combination of these technologies not only promotes the intelligent development of cybersecurity analysis but also provides security personnel with more intuitive and efficient decision support tools, offering innovative solutions to address complex threat environments.

3. Technical challenges and future Directions

The application of artificial intelligence (AI) and animation technology in cybersecurity holds great promise, yet it still faces numerous technical challenges. In terms of data privacy and security, the training data may contain sensitive information, making the protection of this data a critical issue. Technologies such as differential privacy and federated learning offer solutions for data protection, while the integration of blockchain technology to ensure data integrity further enhances data security[12]. Regarding real-time performance and computational resource demands, efficient rendering and AI computation impose high requirements on computational resources[13]. Edge computing and AI model compression technologies can alleviate resource pressure to some extent, while utilizing quantum computing to accelerate the training of complex AI models presents new

DOI: 10.54254/2755-2721/145/2025.21899

possibilities for the future[14]. In the realm of multimodal data fusion and presentation, integrating network data, behavioral data, and environmental data is key to improving analytical effectiveness. Multimodal deep learning models provide technical support for data fusion, while the combination of augmented reality (AR) technology to achieve multimodal data presentation further enhances the comprehensibility and interactivity of the data[15]. These challenges and future directions not only drive continuous innovation in technology but also illuminate the path for the intelligent development of cybersecurity.

4. Practical Significance and Application Contexts.

The practical significance and application scenarios of artificial intelligence (AI) and animation technology in cybersecurity are profound, demonstrating immense potential across various contexts. In the field of cybersecurity education and training, immersive training systems developed using AI and animation technology can provide security personnel with a learning experience closely aligned with real-world scenarios. Virtual reality (VR)-based cybersecurity training platforms have achieved significant results in practice, and the incorporation of gamified design further enhances the enjoyment and engagement of the learning process, making training outcomes more pronounced[16]. In corporate environments, Security Operations Centers (SOC) can offer intuitive, interactive threat analysis tools by integrating AI and animation technology, assisting security teams in swiftly identifying and responding to threats. Commercial SOC visualization tools are widely utilized in enterprise security operations, and the introduction of AI-driven automated report generation features further enhances work efficiency while reducing the costs and errors associated with manual operations. In the realm of government and critical infrastructure protection, the combination of AI and animation technology supports real-time monitoring and response to large-scale cyber threats, providing robust assurance for national security. National-level cybersecurity monitoring systems have been deployed in multiple countries, and the integration of digital twin technology to simulate the security status of critical infrastructure offers innovative means for predicting and defending against potential attacks[17]. These application scenarios not only reflect the practical value of AI and animation technology but also provide new directions for the future development of cybersecurity.

5. Summary and prospect

The integration of AI and animation technology in cybersecurity offers innovative solutions to tackle complex threats by enhancing threat detection, analysis, and response. By combining AI's advanced capabilities in threat detection, classification, and automated response with the intuitive and interactive nature of animation, this integrated solution offers significant improvements in the efficiency, transparency, and interpretability of cybersecurity processes. Animation enhances the understanding of complex data and attack vectors, while AI provides the speed and accuracy necessary to combat evolving threats. Despite challenges such as data privacy concerns, resource demands, and the need for effective multimodal data fusion, emerging technologies like quantum computing, blockchain, and augmented reality (AR) offer promising solutions to overcome these obstacles. Together, AI and animation are set to transform cybersecurity, making it more accessible, engaging, and effective in safeguarding digital ecosystems.

References

[1] *Sommer, R., & Paxson, V. (2010, May). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE symposium on security and privacy (pp. 305-316). IEEE.*
[2] *Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural computation, 9(8), 1735-1780.*
[3] *Kipf, T. N., & Welling, M. (2016). Semi-supervised classification with graph convolutional networks. arXiv preprint arXiv:1609.02907.*

DOI: 10.54254/2755-2721/145/2025.21899

[4] Shrobe, H., Shrier, D. L., & Pentland, A. (Eds.). (2018). New Solutions for Cybersecurity. MIT Press.
[5] Brown, T., Mann, B., Ryder, N., Subbiah, M., Kaplan, J. D., Dhariwal, P., ... & Amodei, D. (2020). Language models are few-shot learners. Advances in neural information processing systems, 33, 1877-1901.
[6] Fruchterman, T. M., & Reingold, E. M. (1991). Graph drawing by force-directed placement. Software: Practice and experience, 21(11), 1129-1164.
[7] Noel, S., & Jajodia, S. (2004, October). Managing attack graph complexity through visual hierarchical aggregation. In Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security (pp. 109-118).
[8] Shiravi, H., Shiravi, A., & Ghorbani, A. A. (2011). A survey of visualization systems for network security. IEEE Transactions on visualization and computer graphics, 18(8), 1313-1329.
[9] Krstajic, M., Bertini, E., & Keim, D. (2011). Cloudlines: Compact display of event episodes in multiple time-series. IEEE transactions on visualization and computer graphics, 17(12), 2432-2439.
[10] Mao, X., Li, Q., Mao, X., & Li, Q. (2021). Generative adversarial networks (GANs). Generative Adversarial Networks for Image Generation, 1-7.
[11] Ribeiro, M. T., Singh, S., & Guestrin, C. (2016, August). " Why should i trust you?" Explaining the predictions of any classifier. In Proceedings of the 22nd ACM SIGKDD international conference on knowledge discovery and data mining (pp. 1135-1144).
[12] Dwork, C. (2008, April). Differential privacy: A survey of results. In International conference on theory and applications of models of computation (pp. 1-19). Berlin, Heidelberg: Springer Berlin Heidelberg.
[13] Satyanarayanan, M. (2017). The emergence of edge computing. Computer, 50(1), 30-39.
[14] Han, S., Mao, H., & Dally, W. J. (2015). Deep compression: Compressing deep neural networks with pruning, trained quantization and huffman coding. arXiv preprint arXiv:1510.00149.
[15] Baltrušaitis, T., Ahuja, C., & Morency, L. P. (2018). Multimodal machine learning: A survey and taxonomy. IEEE transactions on pattern analysis and machine intelligence, 41(2), 423-443.
[16] Slater, M., & Sanchez-Vives, M. V. (2016). Enhancing our lives with immersive virtual reality. Frontiers in Robotics and AI, 3, 74.
[17] Grieves, M. (2014). Digital twin: manufacturing excellence through virtual factory replication. White paper, 1(2014), 1-7.