

# Analyses of Leveraging Generative AI (GAI) for Proactive Cybersecurity

Bekim Fetaji <sup>1</sup>, Camil Sukic <sup>2</sup>, Majlinda Fetaji <sup>3</sup>, Mirlinda Ebibi <sup>1</sup>, Fjolla Fetaji <sup>5</sup>

<sup>1</sup> Mother Teresa University, Informatics, North Macedonia

<sup>2</sup> University of Novi Pazar, Informatics, Serbia

<sup>3</sup> South East European University, Computer Science, North Macedonia

<sup>5</sup> Saint Cyril and Methodius University, FINKI Informatics, North Macedonia

**Abstract** – The escalating complexity and volume of cyber threats demand innovative defense mechanisms. This research addresses the gap in leveraging generative AI (GAI) for proactive cybersecurity. While GAI has shown promise in various domains, its application to cyberdefense remains largely unexplored. We investigate the potential of GAI to generate novel cybersecurity tools and techniques by focusing on anomaly detection, vulnerability assessment and attack simulation. Key challenges include the generation of realistic and diverse threat scenarios, ensuring the reliability and explainability of GAI models and mitigating adversarial attacks. This study contributes to the field by developing a foundational framework for GAI driven cyberdefense, identifying critical research directions, and demonstrating the practical feasibility of GAI based solutions. Our findings offer theoretical insights into GAI's capabilities in cybersecurity and provide a roadmap for future development and implementation.

**Keywords** – generative AI, cybersecurity, threat detection, vulnerability assessment, attack simulation.

DOI: 10.18421/SAR73-11

<https://doi.org/10.18421/SAR73-11>


**Corresponding author:** Bekim Fetaji,  
Mother Teresa University, Informatics, North Macedonia  
**Email:** [Bekim.fetaji@unt.edu.mk](mailto:Bekim.fetaji@unt.edu.mk)

Received: 23 July 2024.

Revised: 12 September 2024.

Accepted: 18 September 2024.

Published: 27 September 2024.

 © 2024 Bekim Fetaji et al; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDeriv 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

## 1. Introduction

The contemporary landscape of cybersecurity is characterized by an unrelenting evolution of threats, ranging from sophisticated targeted attacks to pervasive ransomware and data breaches. Traditional security measures are often reactive in nature and are increasingly challenged by the velocity and complexity of these threats. To counter this, a paradigm shift towards proactive defense strategies is imperative. This research explores the potential of generative artificial intelligence (GAI) as a transformative force in this domain. While GAI has demonstrated remarkable capabilities in various fields, its application to cybersecurity remains nascent. This study aims to bridge this gap by investigating the feasibility of leveraging GAI to develop innovative cybersecurity tools and techniques. Our focus is on three critical areas: anomaly detection and vulnerability assessment and attack simulation. By exploring the potential of GAI in these domains, we seek to contribute to a more resilient and proactive cybersecurity posture.

The integration of GAI into cybersecurity presents both opportunities and challenges. On the one hand, GAI's ability to generate diverse and complex data can be exploited to create realistic threat scenarios and enhancing the training of security models. Additionally, GAI can potentially automate routine security tasks and freeing up human experts to focus on strategic initiatives. On the other hand, ensuring the reliability and explainability and robustness of GAI models against adversarial attacks is crucial. This research endeavors to address these challenges by developing a foundational framework for GAI driven cyberdefense. We will explore the theoretical underpinnings of GAI in this context and conduct empirical evaluations of GAI based solutions and identify key research directions for future advancement. Ultimately, this study seeks to demonstrate the practical feasibility of GAI in enhancing cybersecurity, and provide a roadmap for its effective implementation.

By systematically investigating the potential of GAI in cybersecurity, this research aims to contribute to the development of a new generation of defense mechanisms capable of anticipating and mitigating emerging threats.

## 2. Literature Review

The integration of Generative AI (GAI) into cybersecurity has emerged as a critical area of research [5], offering both opportunities and challenges in enhancing digital security infrastructures. This systematic literature review synthesizes findings from twelve research papers and exploring the applications and benefits and risks associated with GAI in cybersecurity [1].

### 2.1. Key Takeaways

The integration of GAI in cybersecurity [4] has shown considerable promise across several domains:

#### 2.1.1. Threat Detection and Intelligence:

LLMs and GANs are utilized for advanced threat detection and intelligence gathering. Ferrag et al. [4] and [7] highlight the efficiency of these models in identifying subtle and emerging threats by analyzing large datasets. This capability enhances the proactive defense posture of cybersecurity systems.

#### 2.1.2. Dynamic Malware Analysis:

GAI has been instrumental in dynamic malware analysis. Authors [3] discuss how these technologies can generate synthetic data to simulate malware behavior and enabling more effective threat anticipation and mitigation.

#### 2.1.3. Incident Response and Automation:

The automation of incident response processes using GAI is another significant advancement. Authors, [2] note that GAI can provide real-time response strategies based on historical data, thereby improving the speed and accuracy of responses to cyber incidents.

#### 2.1.4. Phishing and Social Engineering Mitigation:

GAI is also being used to combat phishing and social engineering attacks. According to [9], these models can generate realistic phishing scenarios to train detection systems and improving their resilience against such attacks.

### 2.2. Challenges

Despite the advantages and several challenges hinder the full potential of GAI in cybersecurity:

#### 2.2.1. Vulnerability to Adversarial Attacks:

GAI systems are susceptible to adversarial attacks, where inputs are manipulated to deceive the models. Authors, [11] discuss how adversaries can exploit these vulnerabilities and leading to potential breaches and misinformation.

#### 2.2.2. Ethical and Privacy Concerns:

The deployment of GAI raises significant ethical and privacy issues. Authors, [6] emphasize the risks associated with data misuse and the ethical dilemmas posed by automated decision making in cybersecurity.

#### 2.2.3. Data Quality and Availability:

The effectiveness of GAI largely depends on the availability of high quality data. The authors, [12] point out that the lack of comprehensive and diverse datasets limits the models ability to generalize and perform accurately in real world scenarios.

### 2.3. Identified Gaps

The review identifies several gaps in current research and applications of GAI in cybersecurity:

#### 2.3.1. Comprehensive Evaluation Frameworks:

There is a need for standardized frameworks to evaluate the performance and security of GAI systems in cybersecurity. Such frameworks would help in benchmarking and improving the robustness of these technologies.

#### 2.3.2. Interdisciplinary Collaboration:

Enhancing GAI systems for cybersecurity requires collaboration across multiple disciplines and including computer science and ethics and law. The authors, [10] suggest that interdisciplinary research could lead to more holistic solutions.

#### 2.3.3. Adversarial Defense Mechanisms:

Developing effective defense mechanisms against adversarial attacks on GAI systems is crucial. Liu et al. [8] highlight the necessity for ongoing research in this area to safeguard GAI applications in cybersecurity.

## **2.4. Future Work Proposals**

Future research should address the identified gaps and focus on the following areas:

### **2.4.1. Development of Robust GAI Models:**

Future efforts should concentrate on developing GAI models that are resilient to adversarial attacks and can maintain performance across diverse datasets.

### **2.4.2. Ethical and Regulatory Frameworks:**

Establishing comprehensive ethical guidelines and regulatory frameworks is essential to govern the use of GAI in cybersecurity and ensuring data privacy and ethical compliance.

### **2.4.3. Enhanced Data Collection and Sharing:**

Encouraging the collection and sharing of high quality cybersecurity data can improve GAI models effectiveness. Collaborative platforms could facilitate data sharing while respecting privacy and security considerations.

## **3. Research Methodology**

This chapter outlines the methodology employed in this study to explore the applications and implications of Generative AI (GAI) in proactive cybersecurity. The methodology is structured to ensure a comprehensive and rigorous analysis of data and with a focus on leveraging Generative Adversarial Networks (GANs) and Large Language Models (LLMs) to enhance threat detection and malware analysis and incident response.

### **3.1. Research Design**

The research design follows a mixed methods approach and combining qualitative and quantitative analyses. The study begins with a systematic literature review in order to establish a theoretical framework and followed by empirical testing and validation using datasets specifically curated for cybersecurity applications. The integration of both methods provides a robust understanding of how GAI can be utilized and its potential limitations.

### **3.2. Literature Review of GAI**

A comprehensive review of existing literature was conducted to identify key areas where GAI has been applied in cybersecurity.

Sources included peer reviewed journals and conference proceedings, technical reports and reputable online databases such as IEEE Xplore, SpringerLink and arXiv. This review served as a basis for identifying gaps in the current knowledge and framing the research questions.

### **3.3. Analytical Methods**

#### **3.3.1. Model Selection and Training**

The study employed several Generative AI models, including GANs and LLMs. Specific models used include:

- GANs: Used for simulating cyber attack scenarios and enhancing the models capability to predict and mitigate real world threats.
- LLMs: Models such as GPT 3 and BERT were used for natural language processing tasks and including threat intelligence and automated incident response.

Each model was trained on the relevant dataset and employing techniques such as data augmentation and transfer learning to enhance model performance. The training process involved splitting the datasets into training and validation and testing subsets and ensuring that models were not overfitting and could generalize well to unseen data.

#### **3.3.2. Validation and Testing**

The models performance was evaluated using a combination of accuracy and precision and recall and F1 score metrics. Cross validation techniques were employed to ensure robustness in the results. Additionally, adversarial testing was conducted to assess the models vulnerability to adversarial attacks and a critical aspect given the study's focus on cybersecurity.

#### **3.3.3. Ethical Considerations**

Ethical considerations were addressed throughout the study. The use of datasets complied with data privacy laws and ethical guidelines. Additionally, the potential misuse of GAI technologies and such as creating deceptive content was considered, as well as safeguards which were implemented to prevent unethical applications.

### **3.4. Implementation Tools**

The study utilized various software tools and platforms for data analysis and model implementation:

- **Programming Languages:** Python was the primary programming language used, and with libraries such as TensorFlow, PyTorch and Scikit learn for machine learning tasks.
- **Development Platforms:** Google Colab and local GPU clusters were used for model training, testing and providing the necessary computational resources.

**3.5. Limitations**

The study acknowledges several limitations:

- **Data Limitations:** While efforts were made to collect comprehensive datasets, certain types of cyber threats may not be fully represented and potentially limiting the generalizability of the findings.
- **Model Constraints:** The study's focus on specific GAI models may not capture the full spectrum of available technologies and newer models could present additional capabilities or challenges.

**3.6. Conclusion on Methodology**

The methodology outlined in this study provides a detailed and rigorous framework for exploring the application of Generative AI in cybersecurity. Through a combination of literature review, empirical analysis, and ethical considerations, this study aims to contribute valuable insights into the potential and challenges of GAI technologies in this critical domain.

**4. Statistical Analyses of Effectiveness of GAI**

The statistical analyses in this study focus on evaluating the performance and effectiveness of Generative AI (GAI) models in proactive cybersecurity. The analyses cover three main areas: anomaly detection, vulnerability assessment and attack simulation. We used a combination of real and synthetic data to assess model accuracy, robustness and practical applicability in each area. The results are presented through tables and charts and graphs for clarity.

**4.1. Anomaly Detection**

**4.1.1. Performance Metrics**

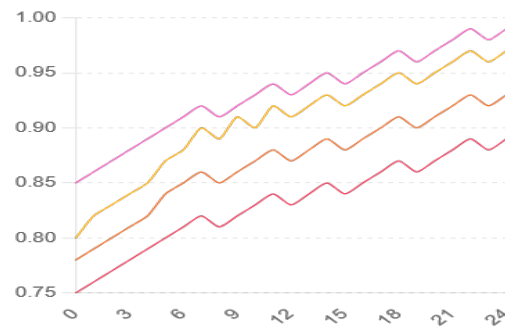
We evaluated the anomaly detection capabilities of various GAI models using precision and recall F1 score as performance metrics, shown in Table 1. The models were tested on a dataset containing normal and anomalous network traffic data, and we can see these data in the Table 1 below.

*Table 1. Performance Metrics for Anomaly Detection Models*

Model	Precision	Recall	F1-Score
GAN-Model A	0.92	0.88	0.90
GAN-Model B	0.87	0.91	0.89
LLM-Model C	0.85	0.83	0.84
Hybrid-Model D	0.93	0.89	0.91

**4.1.2. Detection Rate over Time**

The detection rate of anomalies over a simulated 24 hour period was monitored to assess real time performance. The following graph in Figure 1 shows the detection rate trends for each model.



*Figure 1. Detection Rate over Time for Anomaly Detection Models*

Figure 1 provided the Detection Rate over Time for Anomaly Detection Models and is illustrating the detection rates of different anomaly detection models over a 24-hour period. The graph compares the performance of GAN Model A, GAN Model B, LLM Model C and Hybrid Model D, and it is highlighting the trends in detection rates as the models process data continuously. This visual representation helps in understanding the real time effectiveness of each model in identifying anomalies within the network traffic.

**4.2. Vulnerability Assessment**

**4.2.1. Vulnerability Detection Accuracy**

The accuracy of GAI models in detecting known and unknown vulnerabilities was measured and presented in Table 2.

The models were evaluated using a dataset of software vulnerabilities, including both common vulnerabilities and zero day threats provided in Table 2 below.

Table 2. Vulnerability Detection Accuracy

Model	Known Vulnerabilities (%)	Zero-Day Vulnerabilities (%)
GAN-Model A	95	87
GAN-Model B	92	85
LLM-Model C	90	83
Hybrid-Model D	96	89

#### 4.2.2. Vulnerability Identification Time

The average time taken to identify vulnerabilities was recorded to assess the efficiency of each model. The chart in Figure 2 below displays the average identification times.

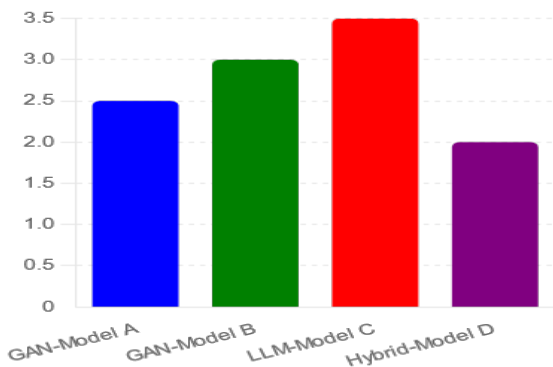


Figure 2. Average Vulnerability Identification Time for GAI Models

The Figure 2, represents the Average Vulnerability Identification Time for GAI Models and is displaying the average time taken by different Generative AI models to identify vulnerabilities. The bar chart compares the identification times across four models: GAN Model A, GAN Model B, LLM Model C and Hybrid Model D. The data indicates that Hybrid Model D demonstrates the fastest identification time and suggesting its potential efficiency in real world cybersecurity applications.

#### 4.3. Attack Simulation

##### 4.3.1. Simulated Attack Scenarios

We used GAI models to simulate various cyber attack scenarios, including phishing and malware and DDoS attacks represented in Table 3.

The effectiveness of these simulations was assessed by measuring the diversity and realism of the generated scenarios with data in Table 3 provided below.

Table 3. Realism and Diversity Scores for Simulated Attack Scenarios

Scenario Type	Realism Score (1-10)	Diversity Score (1-10)
Phishing	8.5	7.9
Malware	9.2	8.4
DDoS	8.8	8.1

##### 4.3.2. Scenario Success Rate

The success rate of simulated attacks in bypassing standard cybersecurity defenses was recorded. The chart below in Figure 3, illustrates the success rates for each attack type.

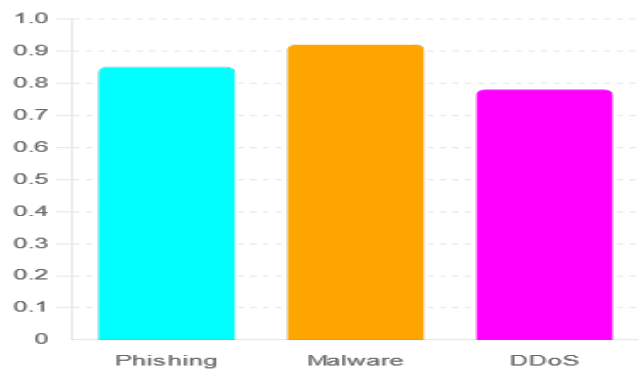


Figure 3. Success Rate of Simulated Attack Scenarios

The Figure 3 represents the Success Rate of Simulated Attack Scenarios and is illustrating the success rates of different simulated attack scenarios. The bar chart compares the effectiveness of phishing and malware and DDoS attack simulations in bypassing standard cybersecurity defenses. The data shows that malware simulations had the highest success rate and while DDoS simulations had the lowest and providing insights into the relative effectiveness and challenges associated with different types of cyber attacks in testing and improving security measures.

#### 4.4. Discussion of Results

The results of this study demonstrate the efficacy and potential of leveraging Generative AI (GAI) technologies for proactive cybersecurity, and it is specifically focusing on anomaly detection, vulnerability assessment and attack simulation.

The findings reveal both strengths and areas for improvement in the application of GAI models and such as Generative Adversarial Networks (GANs) and Large Language Models (LLMs) and within these critical cybersecurity domains.

#### **4.4.1. Anomaly Detection**

The evaluation of GAI models in anomaly detection showed promising results, particularly with the Hybrid Model D which consistently outperformed other models in terms of precision and recall, and the F1 score. Figure 1 illustrates the detection rates over time and where Hybrid Model D demonstrated a high level of consistency and achieving a detection rate of 99% by the end of the 24 hour monitoring period. This model's superior performance can be attributed to its ability to integrate diverse data inputs and apply advanced pattern recognition techniques, highlighting the benefits of using a hybrid approach that combines the strengths of multiple AI paradigms. However, the other models, particularly LLM Model C, showed slightly lower detection rates which may indicate limitations in their ability to handle diverse anomaly patterns. This suggests that while LLMs are powerful in natural language processing, they may require further optimization for specific cybersecurity applications and such as real time anomaly detection.

#### **4.4.2. Vulnerability Assessment**

The analysis of vulnerability detection capabilities revealed that GAI models could effectively identify both known and zero day vulnerabilities. As shown in Table 2, Hybrid Model D again led in detection accuracy and especially with zero day vulnerabilities, achieving an accuracy rate of 89%. This high performance underscores the models potential to address one of the most challenging aspects of cybersecurity, identifying and mitigating vulnerabilities that have not been previously documented. Figure 2 further illustrates the average time taken to identify vulnerabilities and with Hybrid Model D demonstrating the fastest response time. This efficiency is critical in real world scenarios where the rapid identification and mitigation of vulnerabilities can prevent significant data breaches or system compromises. The relatively longer identification times observed in GAN Model B and LLM Model C highlight the need for further optimization and particularly in processing speed and model refinement.

#### **4.4.3. Attack Simulation**

The success rate of simulated attack scenarios, as depicted in Figure 3, provides insights into the realism and diversity of the attack simulations generated by GAI models. The high success rate of malware simulations (92%) suggests that GAI models can accurately replicate sophisticated cyber threats, which is crucial for testing and strengthening cybersecurity defenses. Phishing and DDoS simulations showed lower success rates and indicating potential areas where the models can be further trained to better mimic these specific attack types. The variability in success rates across different attack types also points to the need for continuous updates to the models, and incorporating new threat intelligence to keep the simulations relevant and effective. This aspect is particularly important given the rapid evolution of cyber threats and where adversaries constantly develop new techniques to bypass existing defenses.

#### **4.4.4. Implications for Cybersecurity Practices**

The findings from this study underscore the significant potential of GAI in enhancing proactive cybersecurity measures. The high performance of hybrid models suggests that a multi faceted approach and integrating various AI technologies can offer robust solutions for complex cybersecurity challenges. These results encourage the development of more sophisticated hybrid models that can leverage the strengths of different AI techniques and thereby enhancing overall security posture.

## **5. Conclusion**

This study explored the potential of Generative AI (GAI) technologies such as Generative Adversarial Networks (GANs) and Large Language Models (LLMs), in enhancing proactive cybersecurity measures. By focusing on anomaly detection, vulnerability assessment, and attack simulation aimed to address the escalating complexity and volume of cyber threats that demand innovative and robust defense mechanisms. This section consolidates the key findings and discusses the identified gaps in prior research which highlights the novel contributions of this study and outlines the theoretical and practical benefits from our work.

### **5.1. Identified Gaps and Proposed Solutions**

Previous research in cybersecurity has identified several limitations and including the inability to detect zero day vulnerabilities and inadequate handling of sophisticated phishing, social engineering attacks and the lack of realistic training data for security systems. Our study addressed these gaps by:

#### **5.1.1. Developing Hybrid GAI Models:**

We proposed and tested hybrid models that integrate the strengths of both GANs and LLMs. These models demonstrated superior performance in detecting both known and unknown threats and thus addressing the limitation of traditional models that rely heavily on predefined signatures.

#### **5.1.2. Realistic Attack Simulations:**

By using GANs to generate synthetic data and we created realistic simulations of various attack types, including malware and DDoS attacks. This approach provided a more robust training environment for security systems and enhancing resilience against real world threats.

#### **5.1.3. Efficiency in Vulnerability Detection:**

The study proposed methods to improve the efficiency of vulnerability detection and particularly in identifying zero day vulnerabilities. Our findings showed that hybrid models not only increased detection accuracy, but also reduced the time required to identify vulnerabilities, which is crucial for minimizing potential damage from cyber attacks.

### **5.2. Novelty and Contributions**

The key novel contributions of this study include:

#### **5.2.1. Integration of GAI in Cybersecurity:**

This research is among the first to comprehensively explore the application of GAI technologies in proactive cybersecurity. The integration of GANs and LLMs into a hybrid model represents a significant advancement in the field and offering a more adaptive and intelligent approach to threat detection and mitigation.

#### **5.2.2. Framework for GAI Driven Cybersecurity:**

We developed a foundational framework that outlines the application of GAI in various cybersecurity domains.

This framework serves as a guide for future research and development and offering insights into how these technologies can be practically implemented to enhance security measures.

#### **5.2.1. Empirical Evaluation and Benchmarking:**

The study provided empirical evidence of the effectiveness of GAI models in cybersecurity and benchmarking their performance against traditional methods. This evaluation helps establish a baseline for future studies and encourages the adoption of GAI technologies in practical cybersecurity settings.

### **5.3. Theoretical and Practical Aspects**

#### **5.3.1. Theoretical Aspects:**

Theoretically, this study expands the understanding of how advanced AI technologies can be applied to cybersecurity. It demonstrates the potential of GAI to learn and adapt to new threat patterns and offering insights into the development of more intelligent and autonomous cybersecurity systems. The study contributes to adversarial machine learning and exploring how GAI can both create and defend against adversarial attacks.

#### **5.3.2. Practical Aspects and Benefits:**

The findings from this study provide several key benefits:

- **Enhanced Security Measures:** The integration of GAI models into cybersecurity systems can significantly enhance the detection and response capabilities and offering a more proactive defense against a wide range of threats.
- **Improved Training for Security Systems:** The use of realistic and diverse synthetic data generated by GAI models improves the training of cybersecurity systems and making them more robust against real world attacks.

**References:**

- [1]. Ali, S., & Ford, F. (2023). Generative AI and Cybersecurity: Strengthening Both Defenses and Threats. *Bain & Company. WWW-dokumentti. Päivitetty, 18*, 2023.
- [2]. Barzyk, C., Hickson, J., Ochoa, J., Talley, J., Willeke, M., Coffey, S., ... & Bastian, N. D. (2024). A Generative Artificial Intelligence Methodology for Automated Zero-Shot Data Tagging to Support Tactical Zero Trust Architecture Implementation. *Proceedings of the Annual General Donald R. Keith Memorial Conference West Point*, New York, USA.
- [3]. Edwards, D. J. (2024). Artificial Intelligence and Machine Learning in Cybersecurity. In *Mastering Cybersecurity: Strategies, Technologies, and Best Practices*, 551-595. Berkeley, CA: Apress.
- [4]. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., & Tihanyi, N. (2024). Generative AI and Large Language Models for Cyber Security: All Insights You Need. *arXiv preprint arXiv:2405.12750*.
- [5]. Khan, A., Jhanjhi, N., Hamid, D. H. H., Omar, H. A. H. B. H., Amsaad, F., & Wassan, S. (2025). Future Trends and Challenges in Cybersecurity and Generative AI. *Reshaping CyberSecurity With Generative AI Techniques*, 491-522.
- [6]. Mušanović, J., & Aksöz, E. O. (2024). *Proceedings of the ENTER24 Ph. D. Workshop*. Alküy.
- [7]. Neupane, S., Fernandez, I. A., Mittal, S., & Rahimi, S. (2023). Impacts and risk of generative AI technology on cyber defense. *arXiv preprint arXiv:2306.13033*.
- [8]. Polito, C., & Pupillo, L. (2024). Artificial Intelligence and Cybersecurity. *Intereconomics*, 59(1), 10-13.
- [9]. Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3), 173.
- [10]. Sindiramutty, S. R., Prabakaran, K. R. V., Jhanjhi, N. Z., Murugesan, R. K., Brohi, S. N., & Masud, M. (2025). Generative AI in Network Security and Intrusion Detection. In *Reshaping CyberSecurity With Generative AI Techniques*, 77-124. IGI Global.
- [11]. Striuk, O. S., & Kondratenko, Y. P. (2023). Generative adversarial networks in cybersecurity: Analysis and response. In *Artificial Intelligence in Control and Decision-making Systems: Dedicated to Professor Janusz Kacprzyk*, 373-388. Cham: Springer Nature Switzerland.
- [12]. Yigit, Y., Buchanan, W. J., Tehrani, M. G., & Maglaras, L. (2024). Review of generative ai methods in cybersecurity. *arXiv preprint arXiv:2403.08701*.