الذكاء الاصطناعي التوليدي للأمن السيبراني: مراجعة الأدبيات والتحديات

Generative Artificial Intelligence for Cyber Security: Literature Review and Challenges

Maqbol Ahmed [1]

Kazar Okba [2]

Saad Harous [3]

مقبول احمد – عقبة كزار – سعد هروس

https://doi.org/10.54582/TSJ.2.2.109

(1) College of IT & CS, University of Saba Region, Yemen.
E-mail: Maqbol3@usr.ac
(2) Department of Computer Science, College of Arts, Sciences& Information Technology, University of Kalba, Sharjah, UAE
(3) Department of Computer Science, College of Computing and Informatics, University of Sharjah, UAE

Abstract

The digital transformation era has witnessed substantial technological advancements, resulting in significant global changes. However, the increasing reliance on interconnected systems and data-driven processes emphasizes the criticality of cybersecurity. This paper explores the utilization of Generative Artificial Intelligence (Generative AI) within the domain of cybersecurity, underscoring its capacity to augment threat detection, facilitate anomaly identification, and optimize incident response. Through an extensive evaluation of existing scholarly work and methodologies, the investigation delineates principal applications such as intrusion detection, malware analysis, and the synthesis of artificial data for training objectives. The results indicate that Generative AI has the potential to markedly enhance the precision of cybersecurity systems while concurrently automating repetitive processes, thus improving overall operational efficacy. Nevertheless, obstacles persist, including susceptibility to adversarial attacks, ethical dilemmas, and the requirement for considerable computational resources. This research offers novel perspectives on how Generative AI may be employed to confront intricate cybersecurity challenges, highlighting the necessity of reconciling innovative applications with robust defensive strategies. This research presents pathways for future investigations into secure and ethical applications of Generative AI technologies in cybersecurity.

Keywords: Generative AI, Cyber Security, Artificial Intelligence

المستخلص:

شهد عصر التحول الرقمي تقدمًا تكنولوجيًا كبيرًا، مما أدى إلى تغييرات عالمية كبيرة. ومع ذلك، فإن الاعتماد المتزايد على الأنظمة المترابطة والعمليات التي تعتمد على البيانات يؤكد على أهمية الأمن السيبراني. يستكشف هذا البحث استخدام الذكاء الاصطناعي التوليدي (Generative AI) في مجال الأمن السيبراني، مع التأكيد على قدرته على زيادة اكتشاف التهديدات، وتسهيل تحديد الشذوذ، وتحسين الاستجابة للحوادث. من خلال تقييم شامل للأعمال والمنهجيات العلمية الحالية، يحدد التحقيق التطبيقات الرئيسية مثل اكتشاف الاختراق، وتحليل البرامج الضارة، وتوليف البيانات الاصطناعية لأهداف التدريب. تشير النتائج إلى أن الذكاء الاصطناعي التوليدي لديه القدرة على تعزيز دقة أنظمة الأمن السيبراني بشكل ملحوظ مع أتمتة العمليات المتكررة في نفس الوقت، وبالتالي تحسين الفعالية التشغيلية الشاملة. ومع ذلك، لا تزال العقبات قائمة، بما في ذلك قابلية التعرض للهجمات المعادية، والمعضلات الأخلاقية، والمتطلبات لموارد حسابية كبيرة. يقدم هذا البحث وجهات نظر جديدة حول كيفية توظيف الذكاء الاصطناعي التوليدي لمواجهة تحديات الأمن السيبراني المعقدة، مع تسليط الضوء على ضرورة التوفيق بين التطبيقات المبتكرة والاستراتيجيات الدفاعية القوية. يقدم هذا البحث مسارات للتحقيقات المستقبلية في التطبيقات الآمنة والأخلاقية لتقنيات الذكاء الاصطناعي التوليدي في مجال الأمن السيبراني.

الكلمات المفتاحية: الذكاء الاصطناعي التوليدي، الأمن السيبراني، الذكاء الاصطناعي

1. Introduction

The generation of virtual transformation has been ushered in through the fast development of virtual technologies, which profoundly affect various fields worldwide. Different sectors have experienced first-rate shifts and upgrades because of the seamless integration of revolutionary virtual solutions. Nevertheless, with the growing dependence of industries on interconnected systems and statistics-pushed methods, the significance of cybersecurity has risen to a paramount degree [1].

In the modern-day interconnected virtual panorama, cybersecurity has become a critical concern for corporations and people alike. Generative Artificial Intelligence (Generative AI) has emerged as a promising tool within the realm of cybersecurity, supplying progressive answers to deal with the dynamic and complicated nature of cyber-assaults. Generative AI is a subset of Artificial intelligence (AI) that specializes in developing algorithms and models capable of producing new, innovative, and sensible content [2].

The potential of Generative AI models produce novel information that closely mimics the stylistic and characteristic attributes of the datasets to which they have been previously subjected. This functionality has been made viable via advancements in deep learning, especially through the utilization of generative models together with generative artificial networks (GANs), deep belief networks (DBNs), and variational autoencoders (VAEs) [3-5].

The applications of Generative AI span diverse domains such as computer imagination and prescient, herbal language processing, and others. Generative AI techniques have been used for photosynthesis, top-notch resolution, and fashion transfer [6, 7]. Generative AI has been carried out in text technology, system translation, and talk systems [8, 9]. Generative AI also unearths programs in music technology, video synthesis, or even game improvement [10-12].

Generative AI possesses many models of competencies that contribute significantly to the realm of cybersecurity. An exceptional attribute of Generative AI is its aptitude for scrutinizing and ascertaining patterns within extensive quantities of data, thereby facilitating the identification of irregularities and potential breaches of security. Advanced machine learning models, such as deep neural networks, can be effectively trained on extensive datasets to discern

https://doi.org/10.54582/TSJ.2.2.109

patterns that serve as indicators of malevolent activities, thereby granting the opportunity for the timely detection and prevention of cyber-attacks [13]. The amalgamation of these remarkable capabilities and cutting-edge technologies significantly enhances Generative AI's effectiveness in combating cyber threats and safeguarding sensitive information from potential harm.

Moreover, it is possible to utilize Generative AI techniques, including generative models, to replicate and predict conceivable attack scenarios, thereby assisting in the formulation of proactive defense strategies. Through the creation of artificial data that closely resembles actual cyber threats, Generative AI models can aid cybersecurity experts in identifying vulnerabilities and assessing the durability of their systems [14]. This proactive approach empowers organizations to fortify security measures and maintain a competitive advantage over potential adversaries.

Additionally, Generative AI can play a critical role in cybersecurity by automating certain tactics and responsibilities, lowering the weight on human analysts, and enhancing reaction instances. Generative AI-powered structures can constantly display network site visitors, analyze log files, and detect anomalies in actual time, enabling fast incident response and mitigation [15]. By augmenting human abilities with AI-pushed automation, organizations can decorate their overall cybersecurity posture and better defend themselves in opposition to rising threats.

However, the adoption of Generative AI in cybersecurity raises several challenges. One of the primary worries is the potential for antagonistic attacks, wherein malicious actors make the most vulnerabilities in AI fashions to mislead or control their behavior [16]. Adversarial attacks may want to undermine the trustworthiness and effectiveness of Generative AI-powered cybersecurity systems, highlighting the need for robust defenses and ongoing research on this aspect [17].

Furthermore, the training of Generative AI models necessitates a considerable allocation of computational resources and a substantial quantity of high-caliber data [18]. In addition, without adequate control or guidance, Generative AI models have the potential to produce partial or biased output [19]. Thus, the persistent investigation and apprehension surrounding the ethical usage and conscientious implementation of Generative AI technology endure.

This work presents a comprehensive overview of research and literature on generative artificial intelligence (Generative AI) in cybersecurity. It aims to gather scholarly articles and other relevant literature examining the use of Generative AI in cybersecurity, including threat analysis, anomaly detection, and vulnerability assessment. Thus, it highlights multiple gaps in the existing literature, notably the imperative for a systematic appraisal of Generative AI methodologies specifically designed for applications in cybersecurity, the examination of ethical and computational dilemmas associated with these emerging technologies, and the evaluation of their efficacy in countering the dynamic landscape of cyber threats. The motivation for this study is derived from the escalating intricacy and prevalence of cyberattacks, which demand the development of innovative strategies to enhance defensive measures. This review provides insights and recommendations for future research directions to inform practitioners and researchers in leveraging generative AI for effective cybersecurity solutions.

The rest of this article is organized as follows. Section 2 discusses the applications of generative AI in cybersecurity, types of generative AI, their relationship to data privacy and security, and the advantages, limitations, and challenges of generative AI in cybersecurity. We have tried to categorize the papers based on paper type, topic focus and application, and have carefully analyzed generative AI papers in cybersecurity in Section 3. Trends and Future of Generative AI in Cyber Security are drawn in sections 4 and 5, respectively.

2. Overview of Generative AI in Cybersecurity

Generative AI has the potential to facilitate machines to generate unique content in different fields. It is important to find a middle ground between utilizing the creative capabilities of generative AI and dealing with the challenges to guarantee beneficial implementation.

The Eliza Chabot by Joseph Weizenbaum in the 1960s was an early example of generative AI which had limitations due to vocabulary, context, and reliance on patterns. Early chatbots were hard to customize and extend. Advances in neural networks and deep learning in 2010 revived the field by enabling technology to learn from existing texts, images, and audio. Ian Goodfellow's GANs in 2014 organized competing neural networks to generate and rate content variations, including realistic people, voices, music, and texts. This sparked

interest and concern about deepfakes created by generative AI impersonating voices and people in videos. Progress in other neural network techniques and architectures, such as VAEs, long short-term memory, transformers, diffusion models, and neural radiance fields, have expanded generative AI capabilities [20].

2.1. Definition and Principles of Generative AI

Generative AI is a recent development in AI generation. It is a subset of artificial intelligence that can create authentic songs, photos, or textual content. It researches from a dataset and use that knowledge to generate new content material that follows similar styles. Generative AI has many models such statistics synthesis, algorithm invention, records augmentation, and anomaly detection. It involves creating models and algorithms in AI to produce content that resembles examples in a dataset. These models learn the patterns in the training data and generate original content. Generative AI uses various techniques from machine learning, deep learning, and probabilistic modeling [21, 22].

The standards of generative AI can vary depending on the unique algorithm or model being used. However, there are a few common standards that can be regularly followed inside the discipline.

GANs are widely used in generative synthetic intelligence fashions that encompass a generator and a discriminator. The generator's most important intention is to create new content material that closely resembles the patterns within the schooling facts. On the other hand, the discriminator goals to distinguish between artificially generated content and true examples from the dataset. Through iterative opposed education, each generator and discriminator improve their capabilities, resulting in fairly realistic generated content [3]

Variational autoencoders (VAEs) are generally utilized in generative AI. (VAEs) have a significant impact on the generation of high-dimensional data by incorporating stochastic data representation and leveraging state-of-the-art deep learning methodologies. The primary benefits of such generators stem from their capacity to encode information while offering the potential for decoding and generalizing novel instances [5].

Reinforcement learning is a valuable training paradigm for improving generated models. It is designed to acquire knowledge through interaction. Unlike

supervised and unsupervised learning, it offers flexible objectives in terms of the reward function. RL methods can be applied to generation problems that can be reconceptualized as decision-making problems [23].

2.2. Applications of Generative AI in Cybersecurity

Generative AI is a burgeoning field that encompasses many packages, and one place wherein it has shown first-rate promise is inside the realm of cybersecurity. The utilization of AI in this domain has brought about a myriad of possibilities and advancements that had been previously unattainable. Some examples of generative AI packages are:

Intrusion Detection System (IDS): Generative antagonistic networks (GANs) have been used to generate greater correct artificial statistics, thereby improving the performance of IDS [24] and highlighting the application of GANs in cybersecurity, and their contribution to the improvement of intrusion detection structures. The development of deception techniques, which includes honeypots and honeytokens, has substantially benefited from the implementation of Generative AI. These strategies entail the introduction of artificial statistics that intently imitate authentic consumer behavior or community pastime, successfully tricking capability attackers.

Malware Detection and Analysis: Generative AI has established its effectiveness in malware detection and analysis. For example, it can generate artificial malware samples to learn their characteristics and behavior and developing countermeasures for system protection [25].

Adversarial assault generation: Generative AI can be leveraged to generate practical hostile attack scenarios for vulnerability assessment and protecting robustness. The authors [26] demonstrate the functionality of generative models to create opposed examples that can skip device getting to know-based protection solutions.

Data-Sharing: Generative AI techniques can create generative privacy-preserving synthetic records which could help corporations and online users securely proportion and examine data without the danger of revealing their raw proprietary facts [27]. The techniques leverage generative fashions to generate artificial information with statistical houses which are equal to the authentic information. This manner that analytic equipment may want to nevertheless

be used however without revealing touchy uncooked proprietary information.

2.3. Types of Generative AI and its Relationship to Data Privacy and Security

Many sorts of generative AI models are in operation nowadays, and many others are being developed and explored by researchers. Some of the most outstanding types of generative AI fashions encompass.

2.3.1. Generative Adversarial Networks (GANs)

GANs comprise two neural networks: the generator and discriminator, competing in a game-like fashion. The generator produces synthetic data from noise, while the discriminator differentiates real from fake data. GANs aim to create realistic data to fool the discriminator, which in turn enhances its ability to distinguish between real and generated data, resulting in high-quality content generation for various applications [28]. In security, GANs can create realistic synthetic data for training models and testing security systems, such as generating network traffic data for testing intrusion detection systems. However, they can also be misused to generate data resembling sensitive information, posing privacy risks if used by adversaries to infer or reconstruct private details [29].

2.3.2. Variational Autoencoders (VAEs)

Variational Autoencoders (VAEs) are a popular method for unsupervised learning of complex distributions. They are based on neural networks and can be trained using stochastic gradient descent. VAEs have demonstrated success in generating diverse data types such as handwritten digits, faces, house numbers, physical models of scenes, segmentation, and predicting the future from static images [30].

VAEs are utilized in anomaly detection and security to recognize normal data patterns and detect anomalies or security breaches. VAEs can identify unusual network activity and fraudulent transactions. Although VAEs are not primarily employed for privacy reasons, their application in anomaly detection may unintentionally reveal sensitive information if anomalous data is privacy-sensitive [29].

2.3.3. Autoregressive Models

Autoregressive models are statistical models representing time series data

https://doi.org/10.54582/TSJ.2.2.109

using linear combinations of previous values. The current value is predicted based on past values. These models are frequently utilized in time series analysis and forecasting [31]. Autoregressive models are not commonly utilized in security applications. They have the potential to create secure cryptographic keys and random number sequences for encryption. These models can be employed in text generation tasks with sensitive data, but without proper control, they may inadvertently disclose private information about individuals or organizations [29].

2.3.4. Recurrent Neural Networks (RNNs)

Recurrent Neural Networks (RNNs) are neural networks used to detect patterns in data sequences like handwriting, genomes, and stock market data. They can also be applied to images by breaking them into patches. RNNs are used in Language Modelling, Speech Recognition, Image Description Generation, and Video Tagging [32]. RNNs are used in security to analyze patterns in time-series data for tasks like detecting network intrusions and predicting cybersecurity threats. They can also be utilized for text generation similarly to autoregressive models, with a potential risk of unintentionally revealing sensitive information in the generated text [29].

2.3.5. Transformer-primarily Based Models

A Transformer-based model is a neural network architecture, that transforms Natural language processing tasks with top results. Unlike RNNs, Transformers process sequences in parallel, enhancing computational efficiency. The Transformer architecture is widely used and expanded into different domains like computer vision, speech recognition, and reinforcement learning [16]. Transformer-based models, such as GPT, are utilized in security applications to aid in natural language processing and understanding, assisting in identifying and stopping security breaches in text data. The extensive language models bring privacy concerns because they can create relevant text coherently, possibly revealing private or sensitive details unintentionally, which may result in data breaches or privacy infringements [29].

2.3.6. Reinforcement Learning for Generative Tasks

Reinforcement Learning (RL) is utilized in AI to train models for generative tasks. An agent learns to interact with an environment, aiming to maximize rewards. RL is employed in generating sequences like sentences, images, or music. The agent generates content based on valuable signals and improves

through feedback. RL is notably used in natural language processing to generate relevant sentences, dialogue responses, and stories [33]. Reinforcement learning has the capability to optimize security policies, like intrusion detection or access control mechanisms, in order to enhance overall security. Just like other generative AI models, reinforcement learning models may also unintentionally produce confidential information, particularly when employed in tasks involving natural language generation [29].

2.4. Advantages of Generative AI in Cybersecurity

Overall, Generative AI offers a wide range of advantages including enhancing creativity, improving productivity, enriching education and entertainment, providing personalized experiences, expanding data availability, automating content writing, reducing email response effort, improving technical query response, creating realistic representations, summarizing complex information, and simplifying content creation in a specific style. In this section, we can explain the benefits that generative AI presents in the field of cybersecurity in particular.

- Detect and prevent new and unknown threats: Generative AI can analyze large volumes of data and identify patterns that may go unnoticed by humans, enabling it to detect new and unknown threats, like zero-day attacks, before they can inflict substantial harm, thus helping in real-time detection and prevention [34, 35].
- Improved threat intelligence: Generative AI enhances Cybersecurity by utilizing threat intelligence and analyzing extensive data to identify patterns and proactively tackle potential threats, empowering security teams to remain ahead and promptly respond to potential attacks [22, 34, 36].
- Evaluate and examine vulnerabilities: Generative AI has the potential to significantly contribute to vulnerability scanning by conducting thorough code analysis and identifying and addressing security weaknesses [37].
- Automated and rapid incident response: Generative AI can enhance safety analytics and automate protection responses in endpoint detection and reaction gear and vulnerability scanners, thereby improving the detection of phishing and fraud campaigns. By streamlining incident reporting and prioritizing safety occasions, AI fashions can permit safety groups to reply more efficiently to cyberattacks and reduce the time to stumble on and remediate threats [38].
- Enhanced and early threat detection: The potential of anomaly detection,

behavioral analysis, and pattern recognition aligned with enterprise security policies is to proactively identify threats before damage occurs, and the enterprise defense system can generate new counter-responses from generative AI security models based on the attacker's changing actions, including identifying modified or disguised malware and previously unknown malware variants based on their behavior patterns [38].

- Elevating Supply Chain Security: Using the assistance of Generative AI, intricacies are recognized and alleviated, thereby generating plausible attack scenarios to be utilized for testing and the detection of issues. This process guarantees the establishment of a strong and resilient supply chain [36].
- In-depth analysis and summarization: Generative AI facilitates data analysis from diverse sources, allowing teams to perform traditionally time-consuming and monotonous tasks with efficiency and accuracy; it can also generate natural-language summaries of incidents and threat assessments, thereby enhancing team productivity [39].
- Answer Natural Language Questions in Real-Time: Artificial Intelligence models enable developers and security experts to inquire in a natural language without the need to learn a query language specific to a particular product, thus facilitating the asking of admin-oriented questions and queries [36].
- Automation of repetitive tasks: Automation of repetitive obligations in cybersecurity can be executed through using generative AI. This lets specialists pay attention to greater complex troubles, resulting in elevated efficiency, productiveness, and job delight. Generative AI is likewise able to identify styles and anomalies in massive datasets, leading to advanced accuracy and pace in risk detection and response for better cybersecurity consequences [35].
- Analyze large amounts of data quickly and accurately: Generative AI utilizes machine learning algorithms to analyze extensive data efficiently and accurately, identifying potential cyber-attacks through pattern and anomaly detection [35].
- Improving cost management: AI answers for price control can be high-priced upfront, but they could deliver long-term advantages. According to the 2023 IBM Cost of a Data Breach document, the common price of a statistics breach is $4.45 million. Organizations with the use of safety AI had decreased data breach fees than those without AI-based cybersecurity equipment [40].
- Generate synthetic data: Generative AI has the potential to create synthetic data as a supplement to real data, serving purposes such as training machine learning models and testing security systems, where the synthetic data closely

resembles real data and does not contain any sensitive information [41].

2.5. Limitations and Challenges of Generative AI in Cybersecurity

Although the ability of generative AI within the area of cybersecurity is promising, it's far more important to be well-known and deal with various obstacles and demanding situations. The following are a few key limitations and demanding situations that should be taken under consideration.

- Lack of training data: Obtaining enough schooling facts is crucial for Generative AI. However, acquiring such data in cybersecurity, particularly for rising threats, may be tough [34].
- Adversarial attacks: Adversarial attacks have the strength to manipulate generative AI models and create misleading consequences. For instance, an attacker can create a counterfeit sample designed to trick a generative AI model into mistakenly classifying it as proper [34, 42].
- Explainability: The complexity of generative AI models makes it challenging to understand how they make decisions, which hampers cybersecurity analysts' understanding of their reasoning [43].
- Ethical considerations: Current discussions are prompting ethical inquiries about privacy and data governance. Biased algorithms in Cybersecurity pose ethical concerns, especially about social justice and fairness. Various factors can lead to bias, including training data, algorithm structure, and result interpretation [36, 39].
- Cost and complexity: Generative AI fashions are steeply priced and complex to educate and enforce, requiring specialized hardware and software program infrastructure. This may be hard for smaller agencies or people with limited resources trying to adopt generative AI for cybersecurity [34].
- False positives: Generative AI in cybersecurity may lead to false positives, wasting resources and diverting interest from actual threats. To address this, the machine ought to study various consultant records, whilst also incorporating human oversight and feedback mechanisms [38].
- Preventing misuse and abuse: AI-powered hackers create advanced cyber threats, including realistic phishing emails, malware distribution, and convincing deep faux motion pictures [44].
- Advancement in mimicking human speech patterns: Artificial intelligence has made tremendous progress in imitating human speech patterns, making it

challenging to differentiate between people and machines. Consequently, it's miles essential for us to stay alert and proactively deal with the evolving panorama of cybersecurity threats [45].

- Data Volume: Collecting data from multiple sources leads to a significant volume of data. The processing of billions of events becomes more complex. The challenge is further amplified by the multitude of external data sources, such as threat intelligence [46].
- Deepfakes: Generative Artificial Intelligence can produce highly advanced deepfake videos, audio recordings, or images by manipulating visual and auditory elements, thus leading to deception and misleading viewers. The technology is often leveraged to impersonate public figures or individuals to cause harm to their reputations. Moreover, it can facilitate phishing, scams, and dissemination of inaccurate information [47].
- Contextual Understanding: Generative AI models' limited contextual understanding may result in response inaccuracies or misunderstandings due to their incomplete comprehension of nuanced meaning or intent behind specific inputs [48].
- Identification of Content Source: An important drawback to consider when implementing or using a generative AI app is its consistent inability to identify the source of the generated content, which poses challenges in verifying accuracy, credibility, and legality, potentially leading to issues related to misinformation, bias, or ethical concerns [49].
- Evolving Threats: Adversarial generative AI methods possess the capacity to develop advanced assaults that exploit vulnerabilities and evade conventional security measures, employing artificial intelligence to devise malicious strategies that can infiltrate systems and networks, constituting a substantial cybersecurity risk, as they exploit weaknesses in security protocols, bypassing traditional defenses and rendering organizations and individuals at risk of breaches and data compromises [50].
- Legal implications of generative AI content: The primary legal concern regarding content created by generative AI is the issue of intellectual property rights, which is further complicated by data privacy concerns, ownership and liability implications, and challenges in enforcing laws due to difficulties in identifying the origin of AI-generated content and jurisdictional complexities [51].
- Implications on digital trust: The loss of safety controls in AI structures may lead to losses or damages. This can cause manipulation of financial markets and

public opinion. It additionally poses security threats to biometric structures. Therefore, a comprehensive technique is needed related to law, content material verification algorithms, digital watermarking, and more suitable cybersecurity measures [51].

- Integrating AI and security effectively: it is a challenging task for organizations. It requires a deep understanding of existing systems, processes, and security measures. Adaptation of these elements is necessary to accommodate AI-driven solutions [52].
- Avoiding bias and discrimination: Generative AI models may display bias and discrimination due to the data used for training. This is especially important in cybersecurity, as it can result in models that struggle to identify certain threats or misclassify data [44].
- Generation of Misleading Information: Generative AI models may unintentionally produce deceptive or inaccurate content, particularly when working with partial or biased training data, thereby posing potential risks in cybersecurity situations [48].
- Inadequate Understanding of Security Concepts: AI models may struggle to accurately interpret and respond to security-related queries or scenarios due to their inadequate understanding of complex security concepts [48].
- Data Privacy Concerns: Generative AI models require large volumes of data for training, which may include sensitive or personal information. Ensuring data privacy and protection is crucial in Generative AI applications.
- Scalability: The utilization of Generative AI methods can demand considerable computational resources for both training and implementation. The process of expanding Generative AI systems to effectively handle extensive volumes of cybersecurity data may present certain challenges [45].
- Threat overload and alert fatigue: As the quantity of indicators continues to increase, it becomes tough to distinguish between essential problems that require on-the-spot attention and lower-priority concerns that may be dealt with later. Security teams can also face risk overload and alert fatigue because of the overwhelming extent of alerts, resulting in ignored threats and an inability to efficiently respond to capacity breaches [52].
- Lack of trained experts: The lack of trained specialists within the cybersecurity subject has resulted in an international scarcity of 3 million properly knowledgeable specialists. This scarcity poses demanding situations for companies in coping with various threats. The excessive demand for professional practitioners makes it tough to draw and hold top talent, resulting in a lack of

institutional know-how and understanding in defense in opposition to cyber threats. Continuous AI training and empowerment are important for effective implementation in corporations. However, obstacles inclusive of financial constraints, societal modifications, lack of management dedication, and team motivation make reaching empowerment tough [52].

- Linear scaling of security operations: The increasing complexity of security needs in organizations' cloud-based assets due to digitization and expansion results in a significant rise in telemetry. However, the workload of managing and defending these systems only scales linearly, burdening security teams with manual and repetitive tasks that hinder their ability to focus on strategic responsibilities [52].

3. Analysis of Generative AI Papers in Cybersecurity

This literature overview affords a complete assessment of the works and empirical studies that have delved into the evolution and usage of generative AI in cyber security. We have tried categorizing the papers based on paper type, topic focus and application, and have carefully analyzed generative AI papers in cybersecurity. The first category of these papers is surveys and reviews that present an exploration of the various aspects surrounding Generative Adversarial Networks (GANs) within the field of cybersecurity.

Category 1: **Surveys and reviews that explore multiple facets of Generative Adversarial Networks** (**GANs**).

GAN can surpass other models in tasks like encryption, decryption, attack data simulation, and model enhancement. The paper [18] explains GAN theories, models, and applications in security. GAN has great potential in security. The paper discusses current GAN challenges and believes GAN can solve the problem of missing attack samples.

The survey [53] covers recent research on GANs, including image steganography, neural cryptography, and malware generation for defense improvement. It discusses GAN types, variations, and their use in addressing security issues like surveillance, detection systems, and vulnerability analysis. GANs successfully create undetectable attacks, reveal defense system weaknesses, and facilitate robust security measures in computer-based products and IoT devices.

Analyzes cutting-edge GAN methodologies for privacy and security was

discussed in a survey [54]. It covers domains like image and video generation, malware, and fraud detection. The survey evaluates the advantages and disadvantages of these approaches. Existing methodologies address different objectives by formulating problems based on GAN variations. Formulations consider metrics like attack success rate and data utility. The survey identifies unresolved challenges and suggests research directions for application scenarios, model design, and data use.

The authors in [7] examined Generative Adversarial Networks (GANs) and their types. They aimed to compare these networks and explore their applications across various fields. Different GAN models can be used for similar tasks, requiring further investigation for optimal selection. The authors also discussed the challenges GAN techniques pose in cyber security, including generating adversarial input and facilitating DDoS attacks.

A review [3] provided a comprehensive overview of Generative Adversarial Networks (GANs) and their advantages over other generative models, as well as the challenges in training, tuning, and evaluating GANs. It also discussed key GAN architectures like Deep Convolutional Generative Adversarial Network (DCGAN) and Wasserstein GAN, focusing on how their design addresses issues with the basic GAN model. The main emphasis is on GANs' role in cybersecurity, particularly in enhancing security and adversarial systems by improving generalization and generating realistic adversarial data. These approaches define the current landscape of cybersecurity research utilizing GANs.

The review of GANs in cybersecurity, emphasizing their effectiveness in improving accuracy rates and developing real-time applications for analyzing malicious activities and identifying new malware variants is discussed in [55]. GANs are used for offensive tasks like generating adversarial attacks and defensive tasks like discovering undetectable attacks and generating secure stego-images. Various GAN extensions, including WGANs/GANs, Bidirectional Generative Adversarial Networks (BiGANs), and Cycle-Consistent Adversarial Networks (Cycle-GANs), are employed for specific cybersecurity tasks such as generating high-quality passwords, learning complex data distributions, and converting normal data to malicious data and vice-versa for intrusion detection dataset training.

The review [56] discussed a range of Generative Adversarial Networks

(GANs) and diverse categories in the realm of identifying anomalies, along with a selection of pivotal datasets crafted by researchers to tackle real-world concerns related to detecting anomalies.

The importance of using GANs to create synthetic attack data for cybersecurity is discussed in [57]. GANs are beneficial for training deep learning models due to limited datasets. More research is required to assess if models trained on synthetic data can effectively handle real cyber threats. A balanced approach using both natural and synthetic data is crucial for reliability and ethical considerations.

Category 2: The papers concentrated on generative adversarial networks (GANs) in intrusion detection and anomaly detection.

The research [17] aimed to evaluate the effectiveness of adversarial training with GAN on generic classification models and their generated models. It reveals the vulnerability of Machine learning-based network intrusion detection system (NIDS) to adversarial attacks and builds upon earlier research by evaluating their datasets. The proposed methodologies are shown to be effective through experimentation, with the discriminator accurately distinguishing between real and fake data from IoT datasets.

The paper [58] introduced Generative Adversarial Artificial Immune Network (GAAINet) for intrusion detection in e Industrial Internet of Things (IIoT) systems. Safeguarding IIoT is crucial for organizational and national Critical Information Infrastructure. The paper explains GANs and Artificial Immune Networks. The training process involves two phases: discriminator training in unsupervised learning and generator training to deceive the discriminator. The discriminator needs continuous updating with a feedback mechanism to correct incorrect predictions.

In this study [59], a GAN-based intrusion detection system (G-IDS) was proposed, where GAN generates synthetic samples and IDS is trained on both synthetic and original samples. Experimental analysis showed G-IDS outperforms independent IDS in accuracy, despite having a small original dataset. However, the centralized, computationally expensive, and time-consuming nature of the G-IDS framework requires further investigation.

A novel AI-based NIDS was introduced in the study [60] to address the

data imbalance problem and enhance the classification performance of previous systems. By utilizing a state-of-the-art generative model and implementing autoencoder-driven detection models, the proposed system demonstrated superior performance compared to machine learning and deep learning approaches, achieving accuracies of up to 93.2% and 87% on benchmark data sets. Experiments on IoT and real data sets validated the system's effectiveness in detecting network threats in distributed and real-world environments.

A novel method called Time series Anomaly detection with GAN (TAnoGan) is proposed in [61] for detecting anomalies in time series with limited data points. TAnoGan utilizes a generator and inverse mapping to reconstruct sequences in latent space and estimate anomaly scores. Experimental results on 46 real-world time series datasets demonstrate the superiority of TAnoGan over traditional and neural network models, although challenges such as determining an optimal window length and model instability remain in GAN-based anomaly detection in time series.

The authors explored the problem of creating network flows that can avoid detection by BlackBox IDSs. To address this challenge, they have developed a new generative adversarial network (GAN) framework, called SGAN-IDS [62], which combines self-attention and GANs to enhance the resilience of ML models against attack detection. evaluation using the CICIDS2017 dataset demonstrates that SGAN-IDS significantly reduces the average detection rate of five ML-based IDSs from 97.46% to 81.93%, indicating its effectiveness and wide applicability.

In this study [63], they proposed a framework called deep adversarial insider threat detection (DAITD) that utilizes Generative Adversarial Networks (GANs) for data augmentation. The framework combines an LSTM-Autoencoder for user behavior representation, a GAN generator for modeling true anomalous behavior distribution, and a GAN discriminator for distinguishing real and generated samples. Experimental results demonstrate that the DAITD framework outperforms other existing algorithms for insider threat detection.

Category 3: These papers provide a comprehensive review and overview of deep learning in cybersecurity

The paper [64] analyzed cybersecurity using artificial neural networks and deep learning. It reviewed recent studies on neural networks and emphasized

https://doi.org/10.54582/TSJ.2.2.109

their use in cybersecurity. The importance of deep learning modeling and learning algorithms for security was discussed. Challenges, research opportunities, and future directions in cybersecurity were highlighted.

Extensively analyzed cybersecurity with a focus on artificial neural networks and deep learning [65]. The study analyzed existing research on neural networks in various domains and provided an overview of how these techniques can address cybersecurity challenges. A robust security model must include appropriate deep-learning models based on data characteristics. Advanced learning algorithms need training to utilize security data before enabling intelligent decision-making.

The authors in [66] discussed various uses of deep learning in cybersecurity and addressed security concerns such as exploitation. Deep learning is shown to be important in cybersecurity and can exceed current methods. Further research is needed to improve security for neural networks against attacks.

A comprehensive overview of recent research on using Deep Learning for computer security was discussed in the survey [67]. It covers eight security problems addressed with Deep Learning, such as program analysis, defending against ROP attacks, achieving CFI, and classifying malware. The analysis shows that the literature on Deep Learning for computer security is still in the early stages of development.

The paper [68] demonstrated the effectiveness of generative deep learning methods, such as Adversarial autoencoders (AAE) and Bidirectional GAN (BiGAN), in accurately classifying attacks on IoT devices with a limited set of attacks. The use of the IoT-23 dataset, which was specifically generated from IoT devices, further enhances the results, showing that GAN-based models are more successful in identifying and classifying attacks. Additionally, the model was able to recognize new information injected into the randomized test set as an anomaly, showcasing its adaptability.

A reinforcement learning system was suggested [69] to protect network users from malicious network traffic by training two reinforcement learning agents, namely the network attack generation agent and network defense agent, in the context of deep neural networks. This system aims not only to surpass conventional machine learning algorithms like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) but also to iden-

tify adversarial examples, a major hurdle for existing machine learning-based intrusion detection systems.

Category 4: These papers addressed multiple topics related to Generative AI and its risks to cybersecurity

This category of papers addressed multiple topics related to generative artificial intelligence and its risks to cybersecurity, privacy, social, legal, and ethical implications, As well as the challenges and advantages of generative models and their applications in cybersecurity. Several papers have focused specifically on the challenges, positives, and societal ramifications tied to the implementation of ChatGPT.

The manuscript [22] analyzed obstacles, constraints, and prospects of Generative AI in cybersecurity using ChatGPT. It showed how ChatGPT can be made vulnerable to ethical breaches through reverse psychology and jailbreaking. It demonstrated cyber-attacks possible with Generative AI, experimented with cyber defense mechanisms, and analyzed societal, legal, and ethical concerns. Various unresolved challenges and research dilemmas in cybersecurity and the effectiveness of Generative AI tools were outlined.

An in-depth analysis of the challenges and opportunities of utilizing generative artificial intelligence in business, specifically focusing on ChatGPT, was provided in the article [70]. Identified risks are categorized into seven primary groups, which include lack of AI market regulation, poor quality control, the spread of disinformation and deep fake content, algorithmic bias, job displacement from automation, privacy violations, ethical decline, and socio-economic inequalities. It emphasized the importance of regulating the AI market to ensure fairness, competition, protection of intellectual property and privacy, and prevention of potential geopolitical risks.

The paper [71] presented an analysis of risks and events faced by ChatGPT, suggested a framework for examining cybersecurity in cyberspace, delved into adversarial models and systems, proposed an evolutionary link between attackers and defenders using ChatGPT, and concluded with specific recommendations.

The concerns in cyber security regarding Generative AI and ChatGPT were addressed in [72]. Organizations can reduce risks by applying securi-

ty measures. Recommendations emphasized responsible usage of ChatGPT through collaboration among researchers, developers, and policymakers. Leaders like Chief Executive Officers (CEOs), Chief Information Officers (CIOs), and Chief Security Officers (CSOs) should consider adopting and creating policies to handle security challenges and risks.

The importance of ChatGPT in cybersecurity according to [73] by defining the responsibilities of the Chief Information Security Officer (CISO), developing a cybersecurity framework, and raising awareness. It helps with decisions on firewalls and incident management, effectiveness varies with organization size and technology. ChatGPT aids in automating tasks like patch management, vulnerability management, and data analysis in Cybersecurity operations. However, evaluating Antivirus solutions is restricted due to a lack of recent data. It avoids aiding hackers, supports ethical hacking, and can transform human-computer interactions with its advanced NLP capabilities. CISOs can benefit from improved Cybersecurity operations, management, and implementation.

A comprehensive review of AI-generated content (AIGC) focusing on security, was provided by a survey [74], which discusses principles, technologies, architecture, modes, characteristics, and applications. It identified security threats, privacy issues, and ethical concerns in GPT and AI content, and discussed regulation solutions, challenges, and limitations. It also explored future directions for explainable, effective, accountable, and secured AI content.

This article [75] delved into the impact of the ChatGPT model on cybersecurity, focusing on its practical uses and a case study on false data injection attacks. It also explored ChatGPT's potential to aid security analysts in creating security solutions. However, the current ChatGPT version needs human review and future versions might be used for malicious activities. Addressing privacy, transparency, misleading info, and trust issues is crucial in designing this tool.

According to [76], Generative AI models, including ChatGPT, Midjourney, and DeepBrain, are significant technological advancements that can produce new content in various forms. These models are viewed as crucial for achieving artificial general intelligence and have diverse applications in fields like business, education, healthcare, and content creation. Despite its potential

benefits, generative AI also presents challenges in ethics, technology, regulations, policy, and economy due to the lack of human-centered AI. The ongoing progress in generative AI will impact businesses and industries, emphasizing the need to adapt and collaborate with this technology as the new standard.

The review in [77], explained that cybersecurity faces global concerns due to deepfake algorithms and Massive Language Models (MLMs) like ChatGPT. These technologies create fake content without code, posing a threat. Deepfake algorithms are used in videos, images, and movies utilizing natural language processing and machine learning. Generative adversarial networks (GAN) help create deepfake images with a generator and discriminator. This technology allows cybercriminals to commit hard-to-detect crimes like vishing and email compromise.

The research [78] aimed to explore the changing cybersecurity landscape and the impact of Generative AI. It highlighted the necessity of unified efforts to enhance digital ecosystems through a collaborative AI governance framework. A global cybersecurity entity is suggested for knowledge exchange, norm development, and coordinated responses to cyber threats.

A comprehensive analysis presented in [79] of the security and privacy challenges associated with generative data, as well as the corresponding solutions, including the process of Artificial intelligence-generated content (AIGC) and the fundamental properties of information security, successful protection measures, and potential future directions in this field.

The legal and regulatory implications of Generative AI and LLMs in the European Union were discussed in [80], including aspects of liability, privacy, intellectual property, and cybersecurity, and evaluated the existing and proposed EU legislation, such as the Artificial Intelligence Act (AIA) draft, in addressing the challenges posed by Generative AI and LLMs. It concluded that EU law is ill-equipped to handle these emerging technologies and suggested policy updates and specific regulations for Generative AI.

The study [81] involving 2383 participants and 24502 guesses explored the implications of AI media. The analysis found that AI tools are advanced, with room for improvement and both positive and negative examples. Deepfakes gain attention for potential misinformation, while GPT-3 boosts the popularity

https://doi.org/10.54582/TSJ.2.2.109

of AI-generated text. Despite prevention tools, human intervention remains crucial to combat misinformation in AI media, leading to ethical and societal implications. Researchers stress prioritizing future discussions and preventive measures.

Using synthetic data and surveys, workers' exposure to generative AI and its risks were evaluated in [82]. The study presented the first evidence-based analysis of AI risks in the Australian economy, including privacy, cybersecurity, ethical concerns, bias, economic impacts, and labor displacements. The findings showed a significant level of exposure to generative AI, affecting tasks and work time.

The hypothesis suggested in the study [83] is the increase in generative AI software has caused a rise in social engineering attacks and disinformation, enabled by AI's anonymity. Case studies showed AI's perception and unrestricted use have led to disinformation attacks. To address this, the study recommended improving education, government oversight, and ethical standards in AI projects to reduce its use in spreading disinformation and misinformation.

The paper [84] addressed the ethical considerations underlying AI-driven chatbots, focusing on biases, misinformation, and factual accuracy. It highlighted the importance of inclusivity, user-centric design, data privacy, and responsible research conduct. Collaborative efforts are needed to establish ethical frameworks prioritizing fairness, inclusivity, transparency, and factual accuracy in developing AI-driven chatbots.

Cybersecurity risks from Generative AI were studied and analyzed in [85]. Various Generative Models are used for AI's purposes. Five Generative AIs, including Text-Based Generative AI like Chat GPT, were examined. Security risks and countermeasures were discussed based on the analysis. Real cases show Generative AI being used for attacks, indicating the need for strong cybersecurity measures. Security measures and regulations should be developed by experts and governance in each field. Education and regulations for corporate members are necessary, along with fostering ethical awareness among individuals.

Category 5: **These papers demonstrate the potential for applying Generative AI techniques to enhance cybersecurity**.

The paper [21] examined AI in cyber threat-hunting in 6G IoT networks. A new model that combines GAN and Transformer for this purpose was proposed. Empirical analysis showed the model can detect attacks with 95% accuracy. Challenges like scalability, privacy, and energy efficiency need attention. Despite obstacles, using AI for cyber threat-hunting in 6G IoT networks is promising for future research.

A GAN model was developed in [86] to create adversarial samples of attack classes from the training dataset to improve classifier performance by addressing dataset imbalances. The UGR'16 dataset was used for this project. The neural network classifier progressively received larger inputs to observe feature distribution and accuracy. A GAN model was implemented to generate samples with various attack labels. Samples were produced based on data from UGR16. The model's accuracy was tested with an imbalanced dataset and improved with increased attack samples.

The authors [87] suggested modifications to the GAN schema, such as a proactive neural-network-driven player and a Turing Discriminator with human input. Different players in the GAN setup led to 12 distinct architectures with specific features for Industry 4.0 systems. Choosing the right GAN architecture can handle tasks like training against sophisticated attacks, using smart adversarial components. Multiplying basic GAN components creates complex GANs to solve new problems.

Three GAN-based approaches were proposed and compared for generating fake Modbus frames, with different efficiencies [88]. The single-GAN approach had 55.47% efficiency. The one-GAN-per-byte approach showed 84.08% efficiency. Two approaches achieved 100% efficiency using single-GAN and multiple GAN models for selected bytes. Frames were partially generated by GANs and expert knowledge of Modbus protocol. These approaches aimed to test machine learning capabilities in modeling communication protocols and assess control system vulnerability to cyber-attacks. Fake frames did not cause system collapse but led to suboptimal performance and potential economic losses.

The study [89] introduced a proposed framework that utilizes a generative

adversarial network for effective detection and classification of malware, including zero-day malware. By training the discriminator using malware images generated by the generator, the framework achieved high accuracy and stability in detecting analogous zero-day malware attacks, eliminating the need for inefficient malware signature analysis.

The proposed Bot-GAN framework in this study [90] continuously generates synthetic samples to augment labeled data, resulting in improved precision, accuracy, and performance indicators while reducing the false positive rate of the original model, thus offering a versatile approach to enhance botnet detection models, with future research focusing on its applicability across various detection models.

A study [91] aimed at the ChatIDS approach for elucidating alerts from an intrusion detection system to individuals lacking expertise in the subject matter. ChatIDS accomplished this objective by transmitting anonymous alerts to ChatGPT, a sophisticated language model, which in turn provides intuitive explanations and proposes effective countermeasures against cyberattacks. The conducted experiments have indicated that ChatIDS can be readily implemented, although further attention must be directed towards prompt engineering to ensure the provision of intuitive explanations upon the initial encounter.

The potential for cybercriminals to use Generative AI to carry out ransomware attacks, even with limited IT skills, was demonstrated in [92]. Moreover, the article highlighted the advantages that highly skilled criminals could derive from employing Generative AI, such as for drafting phishing e-mails. Consequently, the widespread availability of generative AI could result in an escalation of both the quantity and quality of ransomware attacks, necessitating the regulation of AI and the implementation of proactive measures to combat cyber risks.

The article [93] explored creating adversarial examples for ML-based PDF malware classifiers. This is challenging due to the complex structure of PDFs and the need for generated PDFs to show malicious behavior. A variant of generative adversarial networks is proposed to generate evasive PDF malware while maintaining original malicious behavior. The model uses the target classifier as a second discriminator and features unique features from malicious PDF files. The technique is evaluated against three PDF malware classifiers and test-

ed with AntiVirus engines from VirusTotal.

A generative artificial intelligence model that demonstrated the ability to produce anonymized traffic data traces resembling authentic ones was proposed in [94]. The proposal is based on employing a Conditional Variational Autoencoder (CVAE) and a preprocessing procedure, they validate their solution through an extensive empirical study using publicly-available datasets, demonstrating its effectiveness in both classification performance and data quality compared to existing models.

3.1. Discussion

The realm of cybersecurity presently exhibits a variety of perspectives and discoveries concerning the function and consequences of generative AI. The above papers which are organized by topic will be carefully examined. Our objective is to furnish an exhaustive evaluation encompassing both converging and diverging perspectives, elucidate crucial facts, and formulate pertinent deductions.

• GANs have shown promise in generating new defense techniques for cyber intrusion, malware detection, secure image steganography [53], detecting various types of cyber-attacks, including DDoS attacks, insider attacks, phishing attacks, adversarial attacks, and deep fakes [7]. as well as, GANs can outperform other models in tasks such as information encryption and decryption, simulation of attack data, password cracking, and enhancing model robustness in the security field [28, 56]. GANs have provided state-of-the-art performance in many areas of application and are considered one of the most successful deep generative models, especially in cybersecurity [3]. To improve defense mechanisms, GANs are used to create attacks or malware that provides knowledge about previously unknown attacks [3, 53, 55]. Also, to ensure the robustness and reliability of cybersecurity models, a balanced approach is required, incorporating both natural and synthetic data [57].
• Nevertheless, according to [53] GANs represent a recently emerged technology. Consequently, these papers [28, 54, 56] recommend continued research and development in the application of GANs for cybersecurity across various domains. In addition, emphasis should be placed on devising new defense techniques based on GANs and evaluating potential attacks [7], more research and experimentation with GANs to discover undetectable attacks and new mal-

ware variants [55]. Moreover, exploring the potential of GANs in improving generalization to adversarial attacks and enhancing security system defenses, creating adversarial systems that can learn authorized features and generate fake data capable of deceiving security systems [3].

• Generative AI-based models or systems for intrusion detection have proven efficient and effective, the model in [58] predicts enhancing the discriminator's intrusion detection ability, possibly exceeding conventional training approaches that depend only on existing datasets. However, it lacks mention of real-world implementation or validation, scalability of GAAINet, consideration of resource constraints in Industrial IoT systems, and comparison of GAAINet with other methods. The study [53] demonstrates that the G-IDS framework performs better than a standalone IDS in various aspects such as attack detection, stability during training, and accuracy in prediction even with a small dataset. Nevertheless, the centralized, computationally expensive, and time-consuming aspects of the G-IDS framework are not discussed. Moreover, it highlighted the necessity of a dynamic, efficient, and lightweight decentralized algorithm for framework dissemination to edge devices within the IoT domain. The system in [60] attained high accuracies, reaching 93.2% on NSL-KDD dataset and 87% on UNSW-NB15 dataset, showing notable enhancement in detecting minor classes. While Mitigation of adversarial attacks bypassing AI-based NIDS remains an unresolved issue. Furthermore, the framework has not been utilized in federated learning systems and ensemble AI systems for improving network threat detection in practical distributed environments. According to [17], Experiments in an IoT dataset showed successful network threat detection in a distributed environment. However, current GANs struggle with balancing generator and discriminator, lack full dataset understanding, and need further exploration in signature-based classifications. The study [61] shows that TAnoGan performs better than traditional and neural network models in anomaly detection. It is effective in small datasets by handling limited data points and achieving superior performance compared to other models. The optimal window length determination, model instability addressing, and comparative studies with larger architectures and a broader set of baseline models in big datasets are all part of future work. The paper shows that SGAN-IDS lowers the average detection rate of five ML-based IDSs by 15.93% from 97.46% to 81.93% [62]. Nevertheless, it lacks a comprehensive discussion on the challenges and weaknesses of zero-day attacks, their detection, and miti-

gation. Moreover, it does not thoroughly examine the potential limitations or drawbacks of the suggested framework. The study [63] found that the DAITD framework performed better than other algorithms for detecting insider threats. However, the Limitations of the proposed data augmentation method using the DAITD framework are not addressed.

• The importance of deep learning in cybersecurity has been emphasized for its superiority over traditional approaches. An effective security system needs specific deep-learning models designed for the data characteristics [64–66]. The study [67] shows Deep Learning is still in the early stages of computer security challenges. Results in [68] proved AAE and BiGAN can accurately classify attacks on limited IoT devices. The paper [69] suggested a reinforcement learning system for adversarial samples in deep learning. No comparison was made with existing DL methods in handling such samples.

• Several researchers have pointed out the security vulnerabilities associated with the use of generative AI. These vulnerabilities consist of various types of attacks on ChatGPT such as Jailbreaks, reverse psychology, and prompt injection. ChatGPT has the potential to be utilized for False Data Injection attacks on crucial infrastructure and can generate offensive cybersecurity content, making it prone to manipulation. The code from ChatGPT may cause security issues [75]. Deepfake can create fake images that avoid analysis [77]. Generative AI content raises legal and accuracy concerns [80]. Distinguishing between AI and human content is difficult [81]. Generative AI is used to spread misinformation [83]. Ethical issues come from biases in AI training data [84].

• Some argue that generative AI boosts cybersecurity by improving security measures. Generative AI tools aid in defensive techniques like cyber defense automation and malware detection [22]. ChatGPT plays a vital role in cybersecurity by defining CISO responsibilities, guiding decisions, and assisting in operations [73, 75]. It also serves as a defensive tool by aiding in vulnerability detection and suggesting solutions for attack detection [75].

• On the other side, a correlation is found between attackers and defenders in using ChatGPT to enhance skills [71]. Robust AI models have potential for both good and bad purposes [75, 81].

• Various stakeholders like governments, international organizations, industries, researchers, developers, and policymakers should collaborate to responsibly and ethically address the cybersecurity risks of generative AI [22, 70, 72, 73, 75, 77, 78, 82, 84]. This collaboration must establish an AI governance

risk management framework with regulations for deploying rigorously tested generative AI models for public use [78, 95]. Extensive legislation is needed to tackle obstacles and protect the benefits of generative AI [77, 80, 83]. Establishing a global platform or international body dedicated to cybersecurity is essential for knowledge sharing and coordinated responses to cyber incidents worldwide [75, 78]. Lastly, continuous education, training, and awareness-raising are vital to helping individuals acquire new digital skills for the evolving labor market influenced by generative AI systems [7, 70, 72, 73, 76, 77, 82, 83, 95].

• Generative Artificial Intelligence has shown considerable potential in enhancing cybersecurity measures across various domains. Numerous research studies have highlighted the effectiveness of Generative AI approaches such as Generative Adversarial Networks (GANs) in addressing critical issues in network intrusion detection [86]. These methodologies have consistently performed well in detecting and predicting zero-day malware instances [89], as well as improving the functionality of botnet detection systems [90]. Demonstrating an impressive accuracy rate of 95%, Generative AI has proven its ability to identify IoT attacks [21] and provide meaningful recommendations for enhancing network security based on alerts from Intrusion Detection Systems (IDS) [91], and the generation of traffic data to fortify Network Intrusion Detection Systems (NIDS) [94]. Additionally, Generative AI architectures have shown promise in conducting training to boost immunity against diverse attacks and developing sophisticated GANs to tackle emerging challenges [88].

• It is imperative to point out the defects and obstacles that necessitate attention. Generative AI availability increases ransomware attacks in quantity and quality [92]. Numerous studies remain unfinished and unimplemented in practical settings, exhibiting various deficiencies. The studies neglected to analyze adversarial methods for generating synthetic data, which is essential for ensuring the effectiveness of the proposed methodologies [86, 94]. Additionally, the lack of empirical evidence and experimental results hinders support for the proposed frameworks, leading to oversight of practical implementation and evaluation [21, 87, 91]. The consequences of counterfeit frames on security, dependability, and stability were ignored, neglecting the real-world impacts of the proposed solution [88]. Moreover, lack of attention to adversarial attacks [89, 90], ethical issues [89, 91], decentralized training [21], computational power, network constraints [21, 91], scalability challenges [21, 91, 94], and the need for defense mechanisms and mitigation strategies is evident [21, 93].

Table 1: Shows the results and recommendations reached by previous studies.

Results	Recommendations
• GANs are highly effective in cybersecurity. They demonstrate better performance in generating defense techniques, detecting various cyber-attacks, and outperforming other models in tasks like encryption and enhancing model robustness. • Generative AI-based intrusion or anomaly detection models are highly effective, outperforming traditional systems in accuracy, stability, and performance, even with limited datasets. • Deep learning is essential in cybersecurity, surpassing traditional methods with specialized models for data characteristics and demonstrating effective attack classification on IoT devices and potential in addressing adversarial samples. • Generative AI enhances cybersecurity by automating defenses, improving malware detection, defining CISO responsibilities, guiding decision-making, and assisting in vulnerability and attack detection. • Empirical research indicates elevated accuracy rates for generative models in the identification of minor attack classes and within distributed network environments. • The proliferation of generative artificial intelligence has precipitated a notable escalation in ransomware incidents, underscoring the imperative to rectify its inherent deficiencies and challenges. • Generative AI raises legal and accuracy concerns, complicates the distinction between AI and human content, and is used to spread misinformation. • Ethical issues arise from biases in AI training data. Numerous studies concerning generative artificial intelligence remain unfinished and devoid of pragmatic applicability, neglecting to consider adversarial methodologies, empirical substantiation, tangible societal implications, and scalability within intrusion detection frameworks.	• To ensure the robustness and reliability of cybersecurity models, a balanced approach is required, incorporating both natural and synthetic data. • Continue research and development in the application of GANs for cybersecurity across various domains. • Emphasis should be placed on devising new defense techniques based on GANs and evaluating potential attacks, more research and experimentation with GANs to discover undetectable attacks and new malware variants. • Emphasis on exploring the potential of GANs in improving generalization to adversarial attacks and enhancing security system defenses, creating adversarial systems that can learn authorized features and generate fake data capable of deceiving security systems. • Various stakeholders like governments, international organizations, industries, researchers, developers, and policymakers should collaborate to responsibly and ethically address the cybersecurity risks of generative AI. • Collaboration among stakeholders is essential to responsibly address the cybersecurity risks of generative AI by establishing a governance framework and regulations for the safe deployment of rigorously tested models. • Extensive legislation is needed to tackle obstacles and protect the benefits of generative AI. • Establishing a global platform or international body dedicated to cybersecurity is essential for knowledge sharing and coordinated responses to cyber incidents worldwide. • Continuous education, training, and awareness-raising are vital to helping individuals acquire new digital skills for the evolving labor market influenced by generative AI systems.

4. Trends of Cybersecurity in the Era of Generative AI

The advent of Generative AI has yielded substantial transformations within the realm of cybersecurity. With the increasing prevalence of Generative AI technologies, it is imperative to comprehend the nascent patterns that are molding the cybersecurity domain. In this exposition, we shall delve into several pivotal trends that are revolutionizing cybersecurity during the era of Generative AI.

• Prioritizing AI cloud security: The integration of Generative AI models with cloud computing is inevitable in various sectors due to the need for computational power, specialized hardware, and extensive datasets. This raises important security concerns that organizations must prioritize. Generative AI models require strong computational infrastructure during the training phase, which is often beyond the capabilities of local hardware. Thus, cloud environments with graphics processing unit (GPU) support are crucial for efficient training. Organizations must understand and effectively utilize security measures provided by cloud providers for Generative AI models and large datasets hosted in the cloud [96].

• Rebuilding business applications with Generative AI: The growing presence of Generative AI in business applications requires robust cybersecurity measures. Security approaches must be rethought to adapt to Generative AI-driven environments. Research and investment in educational initiatives are necessary to develop security frameworks and produce capable cybersecurity professionals. Failure to address these aspects could expose businesses to vulnerabilities that compromise data and disrupt workflows, impacting operations significantly [96].

• The proliferation of AI-powered security tools: Generative AI technology has a profound impact on business applications and cybersecurity. It transforms the cybersecurity toolbox and gives rise to specialized tools with various applications. It enhances application security through real-time code analysis, improves data privacy and large language model security, and enables proactive threat detection and response. However, using Generative AI tools in highly regulated industries adds complexity to compliance and raises ethical and regu-

latory challenges. Ongoing research and multidisciplinary efforts are necessary to address AI bias detection and fairness and balance benefits and risks [96].

• Increasingly Cyber Attacks Using Generative AI: The use of Generative AI in cyber-attacks is increasing, which presents a complex problem. While Generative AI strengthens cybersecurity, it also helps malicious actors. Tools like FraudGPT and WormGPT exemplify this situation. FraudGPT generates malicious code for malware and fraudulent activities. WormGPT facilitates sophisticated phishing attacks. It is easily accessible to novice cybercriminals and generates convincing fake emails. These Generative AI-driven threats require real-time evolution of defense mechanisms [96].

• Expanding attack surfaces: As technology evolves, the attack surface expands, increasing security risks. This includes various devices like thermostats, sensors, monitors, and vehicles. Specialized endpoint security solutions are needed for these devices with limited processing capabilities. A multi-layered security strategy is necessary to secure devices, data pipelines, algorithms, and user interfaces [96].

• Generative AI brings safety opportunities and threats: Generative AI and machine-gaining knowledge convey both opportunities and threats to safety. Companies face sophisticated cyber-assaults like deep fakes and evolving malware. AI-pushed Cybersecurity can revolutionize the enterprise via computerized configurations, advanced get entry to controls, and superior threat detection [97].

• Cyber Resilience: Cyber resilience is wonderful from cyber safety. While protection specializes in prevention, resilience makes a specialty of short recovery and minimizing damage. In 2024, organizations will prioritize resilience in the face of a hit breach [98].

• The growing function of the Chief Information Security Officer (CISO): C-suite executives could have a greater role in choice-making related to cyber risk. Boards will attention more to cybersecurity and may set up devoted committees or interactions with outside stakeholders [98].

• Upgraded Phishing Attacks: Phishing attacks are becoming more advanced, with the potential for growing sophistication. Generative AI tools like ChatGPT

empower attackers to develop more intelligent methods. Deepfake attacks will also become more widespread. Business awareness and education are crucial in responding to these attacks, despite the expanding role of AI [98].

• Cyber Security Regulation: The regulation of cyber security is growing due to awareness of country-wide protection dangers and monetary increase risks related to cyber threats. This has led to the improvement of recent cybersecurity guidelines influenced with the aid of the ability social and political repercussions of facts breaches. For instance, the UK has introduced the Product Security and Telecommunications Act, which calls for organizations to conform to minimal safety requirements for networked merchandise by April 2024 [98].

• Generative AI impacts both components of warfare: Both professionals and attackers are impacted through generative AI. Professionals face sophisticated AI-powered assaults, whilst also making the most of AI in detecting anomalies, authentication, and incident reaction [98].

• Enhancing Network Security: AI has revolutionized network security by analyzing network traffic data in real-time to identify vulnerabilities and respond to threats, enabling proactive cybersecurity [2].

• AI-Powered User Authentication and Access Control: AI is crucial for user authentication and access control, as it analyzes behavior and patterns to detect risks and prevent unauthorized access, enhancing data and system security [2].

• Predicting Breach Risk with AI: AI tools simplify the process of assessing vulnerabilities and predicting attacks by identifying the most vulnerable components and continuously monitoring access points [2].

• Identification and prevention of malicious software programs: AI-powered cybersecurity structures continuously replace their fashions with state-of-the-art data on threats and vulnerabilities, letting them protect against new threats and save you from future attacks. AI can analyze good-sized facts to pick out malware styles and strange conduct, improving cybersecurity and decreasing the hazard of unfavorable attacks [2].

• Behavioral analysis and vulnerability evaluation with AI: AI uses behavioral evaluation and vulnerability assessment to pick out cyber-attacks employing studying consumer conduct and network visitors. It can respond in actual time to unusual conduct and prevent capacity harm. Additionally, system master-

ing permits AI to evolve to evolving threats, making it a valuable device for detecting and responding to cyber-assaults. AI in cybersecurity can automate vulnerability assessment and prioritize threats based totally on their ability to impact. This lets companies proactively address safety dangers and decrease the probability of a hit cyber-attack [2].

5. Future of Generative AI in Cyber Security

Let us acknowledge the significant impact of generative artificial intelligence and its role in shaping the imminent realm of cybersecurity. As the technology of Generative AI is consistently applied with various characteristics and functionalities, we will probably witness the formulation of even more intricate and efficient security solutions. Future developments of Generative AI in the field of cybersecurity are anticipated to concentrate on several key areas.

• Comprehensive AI assistant for cybersecurity specialists: AI researchers and red teamers are developing generative AI tools for cybersecurity specialists, which can lead to the emergence of a cybersecurity assistant based on a large language model (LLM) or a Machine Learning (ML) model. These tools automate red teaming tasks and guide in a pen-testing environment [99].

• Neural networks in scam visuals: Scammers use neural networks to deceive targets in cybercrime, but these AI tools can also be used to create more convincing fraudulent content. Cyber literacy and reliable antivirus software are necessary for protection against scam emails and suspicious websites [99].

• Enterprise transformation: Enterprise transformation requires the adoption of personalized LLMs, more desirable security awareness, and stricter AI regulations. Concerns approximately privacy and security have brought about an increase in Private Large Language Models (PLLMs) and the need for specialized protection awareness schooling and policies to save data leakage [99].

• AI-related regulatory initiatives: There will be a global increase in AI-related regulatory initiatives, with a focus on African and Asian nations. The competition between legal bans and non-binding guidelines will make it challenging to establish a unified solution [99].

• Role of private stakeholders: Private stakeholders in the corporate sector will

play a significant role in shaping AI rules and practices. Policymakers seek input from businesses, academia, and civil society to inform AI governance.

• Watermarks for AI-generated content: Service providers will need to identify and flag synthetic content due to policies and regulations. Detection technologies will be developed, and watermarks will be used to facilitate easier identification and provenance of synthetic media [99].

• The Rise of "Shadow AI": The vast use of generative AI in the place of job creates cybersecurity-demanding situations in the shape of 'Shadow AI.' Organizations want to adopt Managed AI coverage, educate teams on safe AI practices, establish clean utilization rules, and update protection protocols as AI generation advances to mitigate risks to records privacy and cybersecurity [97].

• Advanced AI to Unleash Social Engineering Attacks: Advanced AI can enable attackers to create successful social engineering campaigns by leveraging personal data on social media platforms like LinkedIn and Reddit, making it easier for lower-level attackers to execute targeted strategies [97].

• Evolving AI Security Posture Testing and Deterrence: AI cybersecurity will advance by prioritizing AI red teaming and bug bounties, detecting and addressing unique AI vulnerabilities like model manipulation and prompt injection attacks. Diverse teams will continue to conduct comprehensive assessments and detailed testing scenarios to secure AI systems against sophisticated threats [97].

• Increased automation: Generative AI can automate tasks and improve response speed, reducing the need for human intervention in cybersecurity [35].

• Integration with other technologies: Combining generative AI with machine learning and natural language processing can enhance threat detection and response in cybersecurity [35].

• Increased adoption: The increasing complexity of cybersecurity threats is expected to drive the wider adoption of generative AI as a crucial tool in combating cybercrime [35].

6. Conclusion

This literature review has conducted an extensive examination of the

function of Generative Artificial Intelligence (Generative AI) within cybersecurity, emphasizing its prospective applications, advantages, challenges, and constraints. The findings indicate that Generative AI possesses the capacity to substantially augment cybersecurity protocols through enhanced threat detection, anomaly recognition, and proactive defensive methodologies. By utilizing sophisticated machine learning methodologies, such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), organizations are enabled to gain deeper insights into and mitigate nascent cyber threats, consequently strengthening their defenses against adversarial attacks.

The ramifications of this study are twofold. Theoretically, it enriches the current body of knowledge by situating Generative AI as an essential instrument for advancing cybersecurity practices, underscoring its ability to generate synthetic data that can augment training datasets and bolster model resilience. Practically, the conclusions derived from an array of studies accentuate the imperative for organizations to implement Generative AI solutions to fortify their cybersecurity frameworks and more effectively address vulnerabilities.

Future research trajectories should concentrate on several pivotal domains: initially, investigating the ethical ramifications and biases intrinsic to Generative AI models, especially about data privacy and security. Furthermore, empirical investigations should be undertaken to assess the efficacy of Generative AI applications in practical contexts, including the long-term consequences on threat detection and response times. Scholars should also explore the formulation of more resilient defenses against adversarial attacks on Generative AI systems to ensure their dependability in cybersecurity utilization. This review lays a groundwork for further inquiry into Generative AI within cybersecurity, promoting both theoretical progress and practical applications that can contribute to a more secure digital environment.

7. References

1. Kumar, S., et al., Artificial Intelligence. Journal of Computers, Mechanical and Management, 2023. **2**(3): p. 31-42.

2. Technologies, R. AI in Cyber Security. 2024 3 Mars 2024]; Available from: https://redblink.com/artificial-intelligence-in-cybersecurity.

3. Yinka-Banjo, C. and O.-A. Ugot, A review of generative adversarial networks and its application in cybersecurity. Artificial Intelligence Review, 2020. **53**: p. 1721-1736.

4. Ahmed, S.F., et al., Deep learning modelling techniques: current progress, applications, advantages, and challenges. Artificial Intelligence Review, 2023. **56**(11): p. 13521-13617.

5. Molnár, S. and L. Tamás, Variational autoencoders for 3D data processing. Artificial Intelligence Review, 2024. **57**(2): p. 1-53.

6. Dasgupta, D., Z. Akhtar, and S. Sen, Machine learning in cybersecurity: a comprehensive survey. The Journal of Defense Modeling and Simulation, 2022. **19**(1): p. 57-106.

7. Tasneem, S., et al. Generative Adversarial Networks (GAN) for Cyber Security: Challenges and Opportunities. in Proceedings of the 2022 IEEE Symposium Series on Computational Intelligence, Singapore. 2022.

8. Lansky, J., et al., Deep learning-based intrusion detection systems: a systematic review. IEEE Access, 2021. **9**: p. 101574-101599.

9. Papernot, N., et al. Practical black-box attacks against machine learning. in Proceedings of the 2017 ACM on Asia conference on computer and communications security. 2017.

10. Engel, J., et al. Neural audio synthesis of musical notes with wavenet autoencoders. in International Conference on Machine Learning. 2017. PMLR.

11. Dong, H.-W., et al. Musegan: Multi-track sequential generative adversarial networks for symbolic music generation and accompaniment. in Proceedings of the AAAI Conference on Artificial Intelligence. 2018.

12. Dosovitskiy, A., et al., Learning to generate chairs, tables and cars with convolu-

tional networks. IEEE transactions on pattern analysis and machine intelligence, 2016. **39**(4): p. 692-705.

13. Isola, P., et al. Image-to-image translation with conditional adversarial networks. in Proceedings of the IEEE conference on computer vision and pattern recognition. 2017.

14. Zhu, J.-Y., et al. Unpaired image-to-image translation using cycle-consistent adversarial networks. in Proceedings of the IEEE international conference on computer vision. 2017.

15. Radford, A., et al., Language models are unsupervised multitask learners. OpenAI blog, 2019. **1**(8): p. 9.

16. Vaswani, A., et al., Attention is All you Need Advances in Neural Information Processing Systems. vol. 30. Curran Associates. 2017, Inc.

17. Liu, Z., et al., Anomaly-Based Intrusion on IoT Networks Using AIGAN-a Generative Adversarial Network. IEEE Access, 2023.

18. Bandi, A., P.V.S.R. Adapa, and Y.E.V.P.K. Kuchi, The power of generative ai: A review of requirements, models, input–output formats, evaluation metrics, and challenges. Future Internet, 2023. **15**(8): p. 260.

19. Hadid, A., T. Chakraborty, and D. Busby, When Geoscience Meets Generative AI and Large Language Models: Foundations, Trends, and Future Challenges. arXiv preprint arXiv:2402.03349, 2024.

20. Lawton, G. What is generative AI? Everything you need to know. 2024; Available from:https://www.techtarget.com/searchenterpriseai/definition/generative-AI.

21. Amine Ferrag, M., M. Debbah, and M. Al-Hawawreh, Generative AI for Cyber Threat-Hunting in 6G-enabled IoT Networks. arXiv e-prints, 2023: p. arXiv: 2303.11751.

22. Gupta, M., et al., From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy. IEEE Access, 2023.

23. Cao, Y., et al., Reinforcement learning for generative ai: A survey. arXiv preprint arXiv:2308.14328, 2023.

24. Dunmore, A., et al., A comprehensive survey of generative adversarial networks (gans) in cybersecurity intrusion detection. IEEE Access, 2023.

25. Raff, E., et al. Malware detection by eating a whole exe. in Workshops at the thirty-second AAAI conference on artificial intelligence. 2018.

26. Grosse, K., et al., On the (statistical) detection of adversarial examples. arXiv preprint arXiv:1702.06280, 2017.

27. Beaulieu-Jones, B.K., et al., Privacy-preserving generative deep neural networks support clinical data sharing. Circulation: Cardiovascular Quality and Outcomes, 2019. **12**(7): p. e005122.

28. Cheng, J., et al., Generative adversarial networks: A literature review. KSII Transactions on Internet and Information Systems (TIIS), 2020. **14**(12): p. 4625-4647.

29. Porter, A. 2024 1 April 2024]; Available from: https://bigid.com/blog/unveiling-6-types-of-generative-ai/.

30. Doersch, C., Tutorial on variational autoencoders. arXiv preprint arXiv:1606.05908, 2016.

31. Hamilton, J.D., Time series analysis. 2020: Princeton university press.

32. Schmidt, R.M., Recurrent neural networks (rnns): A gentle introduction and overview. arXiv 2019. arXiv preprint arXiv:1912.05911, 2019.

33. Uc-Cetina, V., et al., Survey on reinforcement learning for language processing. Artificial Intelligence Review, 2023. **56**(2): p. 1543-1575.

34. Solution, b.I. Generative AI for Cybersecurity: Enhancing Threat Detection and Response with AI. 2024 25 Mars 2024]; Available from: https://bayshoreintel.com/generative-ai-for-cybersecurity-enhancing-threat-detection-and-response-with-ai.

35. Culbreath, D. SWOT Analysis for Generative AI and its use in Cyber. 2024; Available from: https://www.linkedin.com/pulse/swot-analysis-generative-ai-its-use-cyber-darren-culbreath/.

36. Mathew, A. A Broader View of Generative AI in Cybersecurity. 2024 4 April 2024]; Available from: https://medium.com/@annamathew03/a-broader-view-of-generative-ai-in-cybersecurity-fd86ce5d4644.

37. Esmailzadeh, Y., Potential Risks of ChatGPT: Implications for Counterterrorism and International Security. International Journal of Multicultural and Multireligious Understanding (IJMMU) Vol, 2023. **10**.

38. Mamgai, A. Generative AI With Cybersecurity: Friend or Foe of Digital Transformation? 2024; Available from: https://www.isaca.org/resources/news-and-trends/industry-news/2023/generative-ai-with-cybersecurity-friend-or-foe-of-digital-transformation.

39. Stanham, L. Generative AI (GenAI) in Cybersecurity. 2024 5 April 2024]; Available from: https://www.crowdstrike.com/cybersecurity-101/secops/generative-ai/.

40. Team, P.C. The impact of AI: Cybersecurity challenges and opportunities. 2024 10 April 2024]; Available from: https://www.pluralsight.com/resources/blog/security/ai-impact-cybersecurity.

41. Rathore, S. Role Of Generative AI In Cybersecurity. 2024 11 April 2024]; Available from:https://hashstudioz.com/blog/generative-ai-in-cybersecurity/.

42. Abdullahi, A. Generative AI Models: A Complete Guide. 2024 11 April 2024]; Available from: https://www.eweek.com/artificial-intelligence/generative-ai-model/.

43. Hui, X. Exploring Challenges & Opportunities: Generative AI in Cyber Security. 2024 22 Maris 2024]; Available from: https://www.exabytes.my/blog/generative-ai-cyber-security/.

44. Zhang, C.Y. Cybersecurity and Generative AI. 2024 20 February 2024]; Available from: https://www.linkedin.com/pulse/cybersecurity-generative-ai-dr-christina-yan-zhang/.

45. Stankovich, M. Unlocking the Potential of Generative AI in Cybersecurity: A Roadmap to Opportunities and Challenges. 2024 15 February 2024]; Available from: https://dai-global-digital.com/unlocking-the-potential-of-generative-ai-in-cybersecurity-a-roadmap-to-opportunities-and-challenges.

46. HANCOCK, D. The Intersection of Generative AI and Cybersecurity. 2024 30 Maris 2024]; Available from: https://www.reliaquest.com/blog/intersection-generative-ai-cybersecurity/?utm_medium=email&utm_source=third-party&utm_campaign=fy24q4-hackernewsarticle_automation&utm_content=hackernews.

47. Technologies, S. What is Generative AI in Cybersecurity? 2024 20 December 2023]; Available from: https://www.sangfor.com/blog/cybersecurity/what-is-generative-ai-cybersecurity.

48. Choudhury, A. and H. Shamszare, Investigating the impact of user trust on the adoption and use of ChatGPT: Survey analysis. Journal of Medical Internet Research,

2023. **25**: p. e47184.

49. Dwivedi, Y.K., et al., "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. International Journal of Information Management, 2023. **71**: p. 102642.

50. Gupta, D. The Road Ahead: Adapting to the Generative AI Cybersecurity Landscape. 2024 11 April 2024]; Available from: https://guptadeepak.com/the-road-ahead-adapting-to-the-generative-ai-cybersecurity-landscape/.

51. Yoong, G.S. Intersection of generative AI, cybersecurity and digital trust. 2024 8 January 2024]; Available from: https://www.techtarget.com/searchsecurity/post/Intersection-of-generative-AI-cybersecurity-and-digital-trust.

52. David, H. Generative AI in cybersecurity: Top 5 cyber security pains it will help to solve. 2024 3 January 2024]; Available from: https://legacy.mindflow.io/generative-ai-in-cybersecurity/.

53. Dutta, I.K., et al. Generative adversarial networks in security: A survey. in 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). 2020. IEEE.

54. Cai, Z., et al., Generative adversarial networks: A survey toward private and secure applications. ACM Computing Surveys (CSUR), 2021. **54**(6): p. 1-38.

55. Arora, A. and Shantanu, A review on application of GANs in cybersecurity domain. IETE Technical Review, 2022. **39**(2): p. 433-441.

56. Rayavarapu, S.M., et al. Generative Adversarial Networks for Anomaly Detection in Cyber Security: A Review. in 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC). 2023. IEEE.

57. Agrawal, G., A. Kaur, and S. Myneni, A Review of Generative Models in Generating Synthetic Attack Data for Cybersecurity. Electronics, 2024. **13**(2): p. 322.

58. Sithungu, S.P. and E.M. Ehlers, Gaainet: A generative adversarial artificial immune network model for intrusion detection in industrial iot systems. Journal of Advances in Information Technology, 2022. **13**(5).

59. Shahriar, M.H., et al. G-ids: Generative adversarial networks assisted intrusion detection system. in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). 2020. IEEE.

60. Park, C., et al., An enhanced AI-based network intrusion detection system using generative adversarial networks. IEEE Internet of Things Journal, 2022. **10**(3): p. 2330-2345.

61. Bashar, M.A. and R. Nayak. TAnoGAN: Time series anomaly detection with generative adversarial networks. in 2020 IEEE Symposium Series on Computational Intelligence (SSCI). 2020. IEEE.

62. Aldhaheri, S. and A. Alhuzali, SGAN-IDS: Self-Attention-Based Generative Adversarial Network against Intrusion Detection Systems. Sensors, 2023. **23**(18): p. 7796.

63. Yuan, F., et al. Data augmentation for insider threat detection with GAN. in 2020 IEEE 32nd International Conference on Tools with Artificial Intelligence (ICTAI). 2020. IEEE.

64. Sarker, I.H., Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective. SN Computer Science, 2021. **2**(3): p. 154.

65. Ghillani, D., Deep learning and artificial intelligence framework to improve the cyber security. Authorea Preprints, 2022.

66. Sharma, B. and R. Mangrulkar, Deep learning applications in cyber security: a comprehensive review, challenges and prospects. International Journal of Engineering Applied Sciences and Technology, 2019. **4**(8): p. 148-159.

67. Choi, Y.-H., et al., Using deep learning to solve computer security challenges: a survey. Cybersecurity, 2020. **3**: p. 1-32.

68. Abdalgawad, N., et al., Generative deep learning to detect cyberattacks for the IoT-23 dataset. IEEE Access, 2021. **10**: p. 6430-6441.

69. Xia, S., M. Qiu, and H. Jiang. An adversarial reinforcement learning based system for cyber security. in 2019 IEEE International Conference on Smart Cloud (SmartCloud). 2019. IEEE.

70. Wach, K., et al., The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. Entrepreneurial Business and Economics Review, 2023. **11**(2): p. 7-30.

71. Hu, C. and J. Chen. A dimensional perspective analysis on the cybersecurity risks and opportunities of chatgpt-like information systems. in 2023 International Conference on Networking and Network Applications (NaNA). 2023. IEEE.

72. Pasupuleti, R., R. Vadapalli, and C. Mader. Cyber Security Issues and Challenges Related to Generative AI and ChatGPT. in 2023 Tenth International Conference on Social Networks Analysis, Management and Security (SNAMS). 2023. IEEE.

73. Prasad, S.G., V.C. Sharmila, and M. Badrinarayanan. Role of artificial intelligence based chat generative pre-trained transformer (chatgpt) in cyber security. in 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC). 2023. IEEE.

74. Wang, Y., et al., A survey on ChatGPT: AI–generated contents, challenges, and solutions. arXiv 2023. arXiv preprint arXiv:2305.18339.

75. Al-Hawawreh, M., A. Aljuhani, and Y. Jararweh, Chatgpt for cybersecurity: practical applications, challenges, and future directions. Cluster Computing, 2023. **26**(6): p. 3421-3436.

76. Fui-Hoon Nah, F., et al., Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. 2023, Taylor & Francis. p. 277-304.

77. Dash, B. and P. Sharma, Are ChatGPT and deepfake algorithms endangering the cybersecurity industry? A review. International Journal of Engineering and Applied Sciences, 2023. **10**(1): p. 21-39.

78. Dhoni, P. and R. Kumar, Synergizing generative ai and cybersecurity: Roles of generative ai entities, companies, agencies, and government in enhancing cybersecurity. Authorea Preprints, 2023.

79. Wang, T., et al., Security and privacy on generative data in aigc: A survey. arXiv preprint arXiv:2309.09435, 2023.

80. Novelli, C., et al., Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. arXiv preprint arXiv:2401.07348, 2024.

81. Partadiredja, R.A., C.E. Serrano, and D. Ljubenkov. AI or human: the socio-ethical implications of AI-generated media content. in 2020 13th CMI Conference on Cybersecurity and Privacy (CMI)-Digital Transformation-Potentials and Challenges (51275). 2020. IEEE.

82. Walkowiak, E. and T. MacDonald, Generative AI and the Workforce: What Are the Risks? Available at SSRN, 2023.

83. Aurand, A., Generative Artificial Intelligence and Its Relationship with Disinformation. 2023.

84. Chugh, H., Cybersecurity in the Age of Generative AI: Usable Security & Statistical Analysis of ThreatGPT. International Journal for Research in Applied Science and Engineering Technology, 2024. **12**(1): p. 9.

85. Subin Oh, T.S., Cybersecurity Issues in Generative AI. 2023, IEEE. p. 97–100.

86. Yilmaz, I. and R. Masum, Expansion of cyber attack data from unbalanced datasets using generative techniques. arXiv preprint arXiv:1912.04549, 2019.

87. Terziyan, V., S. Gryshko, and M. Golovianko, Taxonomy of generative adversarial networks for digital immunity of Industry 4.0 systems. Procedia Computer Science, 2021. **180**: p. 676-685.

88. Zarzycki, K., et al., GAN Neural Networks Architectures for Testing Process Control Industrial Network Against Cyber-Attacks. IEEE Access, 2023.

89. Won, D.-O., Y.-N. Jang, and S.-W. Lee, PlausMal-GAN: Plausible malware training based on generative adversarial networks for analogous zero-day malware detection. IEEE Transactions on Emerging Topics in Computing, 2022. **11**(1): p. 82-94.

90. Yin, C., et al. An enhancing framework for botnet detection using generative adversarial networks. in 2018 International Conference on Artificial Intelligence and Big Data (ICAIBD). 2018. IEEE.

91. Jüttner, V., M. Grimmer, and E. Buchmann, Chatids: Explainable cybersecurity using generative ai. arXiv preprint arXiv:2306.14504, 2023.

92. Teichmann, F., Ransomware attacks in the context of generative artificial intelligence—an experimental study. International Cybersecurity Law Review, 2023. **4**(4): p. 399-414.

93. Bae, H., et al., Learn2Evade: Learning-based generative model for evading PDF malware classifiers. IEEE Transactions on Artificial Intelligence, 2021. **2**(4): p. 299-313.

94. Giuseppe, A., et al., Synthetic and Privacy-Preserving Traffic Trace Generation using Generative AI Models for Training Network Intrusion Detection Systems. Available at SSRN 4643250, 2023.

95. Oh, S. and T. Shon. Cybersecurity Issues in Generative AI. in 2023 International Conference on Platform Technology and Service (PlatCon). 2023. IEEE.

96. Huang, K. Top 5 Cybersecurity Trends in the Era of Generative AI. 2024 11

April 2024]; Available from: https://cloudsecurityalliance.org/blog/2023/10/06/top-5-cybersecurity-trends-in-the-era-of-generative-ai.

97. Masters, J. 7 AI Trends and Predictions for Cybersecurity in 2024. 2024 11 April 2024]; Available from: https://www.msspalert.com/news/ai-trends-2024-what-the-experts-are-saying.

98. Agrawal, V. Top 10 Generative AI Cybersecurity Trends You Should Know. 2024 9 April 2024]; Available from: https://www.novelvista.com/blogs/ai-and-ml/top-10-generative-ai-cybersecurity-trends.

99. VLADISLAV TUSHKANOV, V.S., ANDREY OCHEPOVSKY, YULIYA SHLYCHKOVA. Story of the year: the impact of AI on cybersecurity. 2024 6 April 2024]; Available from: https://securelist.com/story-of-the-year-2023-ai-impact-on-cybersecurity/111341/.