T5-survey examines privacy and security challenges inherent to Generative Artificial Intelligence (GAI) paper highlights current security strategies and proposes sustainable solutions . paper highlights user, developer, institutional, and policymaker involvement . paper highlights current security strategies and proposes sustainable solutions . in addition, it highlights user, developer, institutional, and policymaker involvement .

BART- Privacy and Security Concerns in Generative AI: A Comprehensive Survey. Generative Artificial Intelligence (GAI) has sparked a transformative wave across various domains, including machine learning, healthcare, business, and entertainment. This comprehensive survey offers a meticulous examination of the privacy and security challenges inherent to GAI. It provides five pivotal perspectives essential for a comprehensive understanding of these intricacies. The paper encompasses discussions on GAI architectures, diverse generative model types, practical applications, and recent advancements within the field. In addition, it highlights current security strategies and proposes sustainable solutions, emphasizing user, developer, institutional, and policymaker involvement.

GEMINI- Generative AI (GAI) poses privacy and security challenges due to its ability to create realistic data. This survey examines these challenges comprehensively, covering GAI architectures, model types, applications, and policies. It highlights data privacy, bias, and security risks associated with GAI and proposes solutions involving users, developers, institutions, and policymakers. The survey emphasizes the need for responsible development and use of GAI to mitigate privacy and security concerns.

GPT-4 In recent years, the growing field of Generative Artificial Intelligence (GAI) has seen a transformative wave across various domains such as machine learning, healthcare, business, and entertainment, primarily due to its advanced capability to generate lifelike data. This comprehensive survey meticulously examines the privacy and security challenges inherent to GAI, providing essential insights into the complexities of the field. The paper offers five pivotal perspectives that are crucial for a thorough understanding of these issues, encompassing discussions on GAI architectures, diverse generative model types, practical applications, and recent advancements within the field.

Previous research highlights significant advances in GAI, yet this survey uniquely focuses on the security strategies currently in place and proposes sustainable solutions to mitigate risks. It emphasizes the importance of involving various stakeholders including users, developers, institutions, and policymakers, suggesting a collaborative approach to tackle the privacy and security challenges effectively. The survey not only reviews existing models and applications but also critically assesses the vulnerabilities that these technologies bring to the forefront.

Numerous studies have addressed this topic with varying approaches; however, this survey stands out by systematically categorizing the types of security threats and offering a structured analysis of potential defenses. By integrating the latest research findings with expert opinions, the paper provides a comprehensive resource for anyone looking to understand the intricacies of GAI from a security and privacy standpoint. It calls for ongoing research and adaptive strategies to ensure that as GAI technologies evolve, they do so with robust safeguards against potential abuses and threats, thereby securing the benefits of GAI for future advancements across all sectors.

GPT-3 Generative Artificial Intelligence (GAI) has revolutionized multiple sectors with its lifelike data generation capabilities. This survey delves into the critical privacy and security issues surrounding GAI, offering five key perspectives for a thorough comprehension. It explores GAI architectures, various generative model types, practical applications, and recent advancements, shedding light on the complexities within the field. The paper not only discusses existing security measures but also suggests sustainable solutions, stressing the importance of engagement from users, developers, institutions, and policymakers. This comprehensive analysis serves as a vital resource for understanding and addressing the challenges posed by GAI, providing insights that are crucial for navigating the evolving landscape of artificial intelligence.