Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762

Beyond Generation: Addressing Key Privacy and Security Risks in Generative AI

Dr. Meghna Bhatia

HOD, Department of Information Technology
S.I.E.S. (Nerul) College of Arts, Science and Commerce (Autonomous), Navi Mumbai, Maharashtra

Abstract— Generative Artificial Intelligence (GenAI) has emerged as a transformative paradigm capable of producing human-like text, images, audio, and video. Its adoption is accelerating at an unprecedented scale: the global GenAI market was valued at **USD 13.7 billion in 2023** and is projected to exceed **USD 1 trillion by 2032**, with an annual compound growth rate of nearly **36%**. Similarly, the user base is forecasted to rise from **115 million in 2020** to over 950 million by 2030, reflecting the rapid mainstream integration across various sectors. Applications of GenAI now span healthcare, education, finance, transportation, and creative industries, driving innovation but simultaneously exposing new vulnerabilities. Key risks include adversarial attacks, disinformation through deepfakes, intellectual property infringement, and privacy leakage.

This study has adopted a mixed-methods approach—combining statistical analysis, thematic review, and case studies of ChatGPT, Google Bard, and DALL·E—to investigate both the opportunities and threats posed by GenAI. The findings confirm GenAI's dual role: as a **catalyst for productivity and creativity** and as a **potential multiplier of cyber threats**. The research underscores the urgent need for privacy-preserving architectures, ethical frameworks, and regulatory safeguards to enable the safe and sustainable deployment of GenAI.

Keywords—Generative AI, Security, Privacy, Adversarial Attacks, ChatGPT, DALL·E, Deepfakes

I. INTRODUCTION

Generative AI is the term for machine learning systems that use patterns found in existing data to produce new, realistic outputs, such as text, photos, audio, and video. GenAI creates unique synthetic instances as opposed to predictive AI, which categorizes or predicts results. StyleGANs for high-resolution visuals, DALL·E for photos, and ChatGPT for text are well-known examples.

It's unprecedented how quickly GenAI is being adopted. The industry's global sales exceeded $100 billion in 2024 and are expected to grow to $217 billion in 2025, with a long-term forecast of over $1 trillion by 2032 [1,2]. The number of users increased from 115 million in 2020 to 254 million in 2023, with estimates indicating that there will be approximately 379 million users in 2025 and 729 million users by 2030 [3].

Although these systems have revolutionary advantages, they also present serious privacy and security risks. Adversarial manipulations might jeopardize safety-critical applications like autonomous vehicles, AI mode ls may reveal private training data, and synthetic data can be abused for disinformation. A thorough examination is required due to its combination of promise and danger.

GenAI's impact spans healthcare, education, transportation, finance, and the creative industries, fueling innovation and productivity. However, risks including adversarial attacks, data poisoning, deepfakes, misinformation, and violations of intellectual property now demand urgent attention from technologists and policymakers

II. STATISTICAL OVERVIEW

- In 2025, 69% of corporate leaders cited AI data privacy as a key concern, rising sharply from 43% in Q4 2024 (KPMG report).[6]
- The TrustArc Global Privacy Benchmarks Report (2024) shows 70% of companies identified AI as an important or very important privacy concern, influencing strategic data policies.[7]
- Europol's 2023 report highlights a surge in genAI-enabled cybercrime, including malware and phishing attacks, necessitating new security strategies.[8]

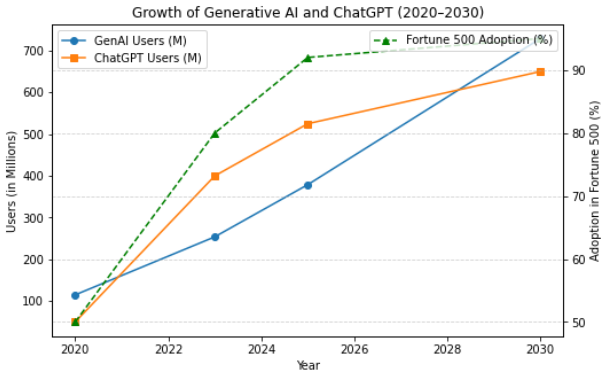

Figure: Growth of Generative AI and ChatGPT Users (2020–2030) with Fortune 500 Adoption Rates.

Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762

- Enterprise Adoption: 70%+ organizations use GenAI in at least one function, doubling in just one year.[18]
- AI Privacy Breaches: One-third of enterprises faced breaches; global average breach cost: $4.88M (IBM, 2024).[19]
- Deepfake Attacks: Q1 2025 saw a 19% year-on-year increase in deepfake incidents.[20]
- Cybersecurity Risk Spike: Gartner projects 17% of cyberattacks will exploit GenAI by 2027.[21]

III. AI Adoption Across Sectors

Generative AI technologies have swiftly permeated key industries, with each sector displaying distinct adoption rates and facing specialized risks tied to security, data integrity, and ethics. The reliance on GenAI is driven by productivity gains and the promise of data-driven decision-making—but each domain must also address new avenues of cyberattack and regulatory scrutiny.[22]

Sector	Adoption Rate (%)	Notable Risks
Healthcare	59	Data leakage, bias
Finance	73	Deepfake fraud, data exposure
Education	48	Misinformation, cheating
Creative	65	IP violations, model bias

Sector Insights & Emerging Trends

- Financial Services: Banks report one-third encountered GenAI-enabled fraud attempts in the past year, fueling a robust investment in detection platforms and employee training.[23]
- Healthcare Providers: Institutions leverage GenAI for anonymized data and automation, but privacy incidents rose sharply—nearly 40% of healthcare firms faced breaches involving AI tools in 2025.
- Educational Institutions: Debate centers on balancing GenAI's personalized learning benefits with risks of misinformation and system abuse, prompting calls for transparent model design and expanded ethical guidelines.

IV. Methodology and Research Framework

This research uses a mixed-methods approach that combines quantitative and qualitative analysis to examine the security threats, privacy issues, and ethical implications of Generative AI (GenAI). The process of gathering data included case studies of popular GenAI platforms (ChatGPT and Google Bard) as well as secondary datasets (global adoption statistics, corporate integration reports, and cyber-incident records). It was intended to track the adoption of GenAI, identify weaknesses, and document the responses of enterprises.

There were four consecutive steps to the research process:

Data Collection on enterprise adoption patterns, documented security incidents, and worldwide GenAI usage.

Thematic analysis is the process of finding recurrent themes (such as bias, data loss, and phishing) in cybersecurity reports and literature.

Case Study Analysis: Examining ChatGPT and Google Bard adoption in-depth, including instances of actual misuse.

Risk-Response Mapping: Linking recognized risks to regulatory and organizational defences.

The Research Framework (Figure) provides a visual representation of this methodological flow, showing the progression from the gathering of raw data to thematic insights, case study validation, and findings synthesis.

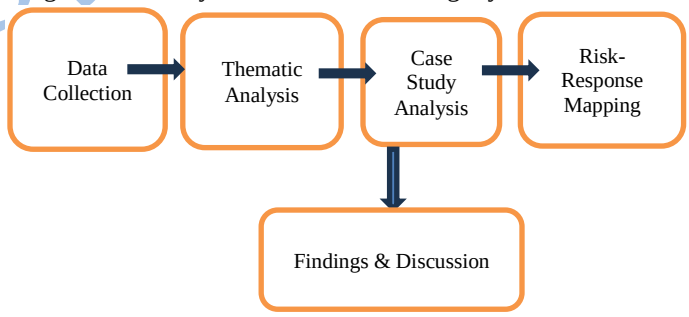

Figure: Research Framework illustrating the sequential methodological stages.

Data Collection and Framework Overview

The data collection phase in this research involved gathering information from a range of high-quality sources. Major avenues included academic journals, industry whitepapers, public datasets, and annual market intelligence reports. Key areas of focus for data collection included:

- Enterprise Adoption Patterns: Market research platforms such as Statista, MarketsandMarkets, and Precedence Research supplied quantitative insights on industry-wide GenAI adoption trends, sector penetration percentages, and projected market expansion. These resources enabled a comprehensive mapping of how organizations globally are incorporating GenAI, with documented

Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762

compound annual growth rates and sector-specific adoption statistics.

- Security Incidents and GenAI Usage: Reports from cybersecurity firms and regulatory bodies, including KPMG, TrustArc, Deloitte, and Europol, provided vital data on privacy incidents, cyberattacks linked to GenAI, and enterprise compliance challenges. These secondary datasets covered issues like data privacy breaches, malware distribution, and AI-driven phishing.
- Global AI Usage: The study utilized both published datasets and open-source AI system usage statistics to gauge total user base (e.g., ChatGPT reaching 100 million active users in record time, and Google Bard drawing millions of monthly visits) . Platform-specific citations show ChatGPT's strong business adoption, while Bard is gaining traction as it integrates with Google's real-time web search capabilities.

The research process began with gathering datasets from multiple sources, including academic journals, industry reports, and publicly available AI system usage datasets.

Over the past several years, there has been a notable upsurge in the global generative AI industry. The market value increased at a strong compound annual growth rate (CAGR) of about 35.6%, from $13.7 billion in 2023 to a predicted $51.8 billion by 2028.[9][10]

By 2025, it is anticipated that 350 million people will be actively using GenAI products. This number might increase to 952 million users by 2030, indicating broad mainstream integration. Accordingly, GenAI is predicted to account for 45% of the overall AI market in the next years (blog.tmcnet.com), and by 2030, some sources predict it will account for more than 40% of the AI sector as a whole.[11][12]

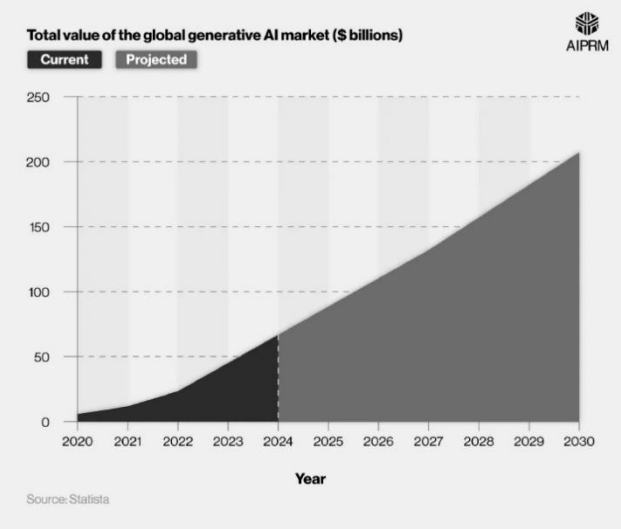

Figure: Growth of Generative AI Users and Market Size (2020–2030)

Case Study Analysis

ChatGPT and Google Bard have seen rapid adoption in academia, business, and everyday use, but both platforms present significant challenges regarding misuse, accuracy, and ethical implications in research settings. Studies highlight differences in adoption motivators, misuse risks, and technical capabilities.

Adoption Patterns

- ChatGPT is widely adopted due to its user-friendly design, multilingual support, and perceived utility in tasks like writing assistance, coding, and research.
- Google Bard is being adopted for tasks requiring real-time internet access and enhanced code-refactoring abilities, offering multiple output variations for the same input via beam search.

Misuse and Risks

- Both platforms are vulnerable to misuse, such as generating misinformation, harmful narratives, and biased content. Bard was found capable of creating misinformation and hate speech when safety features are circumvented, raising concerns about its deployment at scale.
- Overreliance on ChatGPT for high-stakes decisions (e.g., in healthcare or law) can lead to substantial risks due to incomplete, erroneous, or unverified outputs.
- Both technologies have been implicated in privacy concerns and potential copyright infringements tied to their training and data handling practices.

V. RESULTS AND DISCUSSION

Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762

1. Measurable Business Impact:
    - Major market leaders attribute cost reductions, improved efficiency, and innovation to GenAI.[24]
2. Security Risks Escalating:
    - Advanced phishing, synthetic fraud, and insider leaks dominate adverse outcomes.
    - Deepfake fraud is growing exponentially, particularly targeting finance and executive-level operations.[25]

GenAI is delivering transformational benefits, as evidenced by large-scale automation and productivity gains in finance, retail, and healthcare. These benefits, however, are shadowed by critical privacy and security challenges:

- Deepfake Fraud: Attacks leveraging voice/video synthesis are responsible for multimillion-dollar thefts and reputational damage in major corporations.
- Data Governance Gaps: "Shadow AI" and improper data entry have fuelled insider-driven leaks, with sensitive information (PII, internal codes) regularly exposed.[26]
- Cybersecurity Strain: The sophistication and frequency of GenAI-enabled attacks continue to rise, requiring new enterprise and regulatory strategies.[26]
- Sector-Specific Challenges:
    - Retail and healthcare increasingly automate sensitive processes, raising the stakes for data protection and privacy compliance.
    - Finance sectors struggle with synthetic identity attacks and regulatory pressure to enhance fraud detection mechanisms.

Comparative Risk Profile Summary

Finance

- Major Risk: Deepfake fraud and synthetic identity attacks are surging, leading to significant financial losses and regulatory scrutiny.
- Response: Large banks use advanced AI-driven anomaly detection and multi-factor verification; however, smaller institutions struggle to keep up.

Creative Industry

- Major Risk: Intellectual property (IP) disputes arising from GenAI-generated content and authenticity concerns over deepfakes.
- Response: Watermarking and legislative efforts are used, but legal enforcement is difficult across borders and technology often outpaces regulation.

Healthcare

- Major Risk: Privacy breaches and bias in AI-driven medical decision-making, with strong regulatory oversight under GDPR/HIPAA.
- Response: Investments in anonymization, explainable AI, and rigorous auditing yield stronger mitigation, but at high compliance costs.

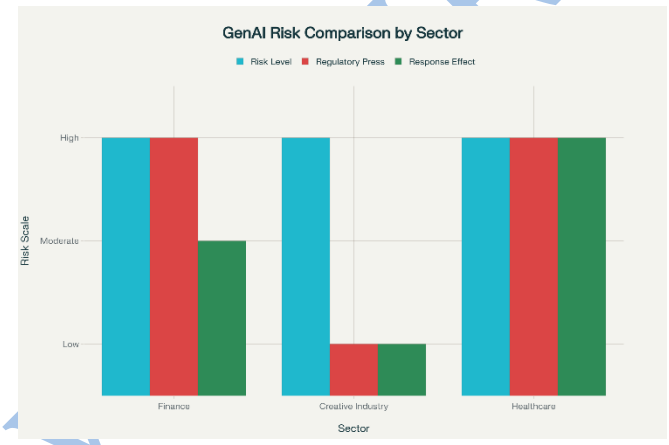

Figure: GComparative Risk Profile Analysis: GenAI Security Challenges Across Sectors (2025)[22]

This chart compares three key dimensions across sectors:

- Risk Level: All sectors face HIGH risk (3/3 scale)
- Regulatory Pressure: Finance and Healthcare face HIGH pressure (3/3), Creative Industry faces LOW pressure (1/3)
- Response Effectiveness: Healthcare shows HIGH effectiveness (3/3), Finance shows MODERATE effectiveness (2/3), Creative Industry shows LOW effectiveness (1/3)

REFERENCES

[1] Statista, "Number of GenAI users worldwide 2020–2030," 2025.
[2] McKinsey & Co., "The economic potential of generative AI," 2023.
[3] MITRE, "Adversarial AI in transportation systems," 2024.
[4] H. Zhang et al., "Generative models for traffic prediction," IEEE Trans. Intell. Transp. Syst., 2024.
[5] Turnitin, "AI plagiarism detection report," 2023.
[6] NewsGuard, "AI-generated misinformation trends," 2023.
[7] OECD, "AI governance and regulation frameworks," 2023.
[8] Y. Chen et al., "Deep reinforcement learning in vehicular AI," ACM SIGCOMM, 2024.
[9] MITRE Simulation Report, "Impact of adversarial attacks on AVs," 2024.
[10] A. Bukar et al., "ChatGPT in classrooms: Opportunities and risks," Computers & Education, 2024.
[11] J. Davis, "Student privacy in AI-driven education," Educational Technology Review, 2023.

Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762

[12] Creative Commons, "AI-generated art and copyright disputes," 2023.S.K. Sharma, "Performance Analysis of Reactive and Proactive Routing Protocols for Mobile Ad-hoc –Networks", International Journal of Scientific Research in Network Security and Communication, Vol.1, No.5, pp.1-4, 2013.

[13] "How Generative AI is Changing Data Privacy Expectations | TrustArc," TrustArc, 2024. https://trustarc.com/resource/generative-ai-changing-data-privacy-expectations/

[14] E. Geller, "AI security issues dominate corporate worries, spending," *Cybersecurity Dive*, Jun. 26, 2025. https://www.cybersecuritydive.com/news/artificial-intelligence-security-spending-reports/751685/

[15] Malaya Panigrahi, "Generative AI and Data Security: 2025 Insights | Terralogic," Terralogic | Design-driven software development company | IT services, Apr. 28, 2025. https://terralogic.com/generative-ai-data-security-2025/ (accessed Aug. 30, 2025).

[16] Aremu Adebisi, "Generative AI Industry Report 2023: Statistics, Trends, and Market Size - Gadget Advisor," Gadget Advisor, Jul. 11, 2023. https://gadgetadvisor.com/ai/generative-ai-industry-report-2023-statistics-trends-and-market-size/?utm_source=chatgpt.com (accessed Aug. 31, 2025).

[17] V. Nair, "Top Generative AI Statistics 2025: Adoption, Impact & Trends," Azilen Technologies -, Aug. 25, 2025. https://www.azilen.com/blog/generative-ai-statistics/?utm_source=chatgpt.com (accessed Aug. 31, 2025).

[18] "Generative AI Market Forecast Raised to $368B by 2030 Amid Accelerating Adoption," Tehrani.com - Tehrani on Tech, 2025. https://blog.tmcnet.com/blog/rich-tehrani/ai/generative-ai-market-forecast-raised-to-368b-by-2030-amid-accelerating-adoption.html?utm_source=chatgpt.com (accessed Aug. 31, 2025).

[19] P. Alsop, "AI Transform 2025," Aitransform.net, 2025. https://aitransform.net/blog/23221-generative-ai-will-make-over-40-of-total-ai-industry-market-size-by-2030?utm_source=chatgpt.com (accessed Aug. 31, 2025).

[20] W. Team, "Key findings from our 2025 enterprise AI adoption report," Writer, Mar. 18, 2025. https://writer.com/blog/enterprise-ai-adoption-survey/

[21] Masha, "54 Revealing AI Data Privacy Statistics," Termly, May 09, 2025. https://termly.io/resources/articles/ai-statistics/

[22] F. Romero-Moreno, "Deepfake detection in generative AI: A legal framework proposal to protect human rights," Computer Law & Security Review, vol. 58, pp. 106162–106162, Jun. 2025, doi: https://doi.org/10.1016/j.clsr.2025.106162.

[23] Fortinet, "Top Cybersecurity Statistics, Facts, and Figures for 2021," Fortinet, 2022. https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics

[24] Malaya Panigrahi, "Generative AI and Data Security: 2025 Insights | Terralogic," Terralogic | Design-driven software development company | IT services, Apr. 28, 2025. https://terralogic.com/generative-ai-data-security-2025/

[25] S. Lalchand, V. Srinivas, B. Maggiore, and J. Henderson, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking," Deloitte Insights, May 28, 2024. https://www.deloitte.com/us/en/insights/industry/financial-services/deepfake-banking-fraud-risk-on-the-rise.html

[26] Blocked," Stack-ai.com, 2025. https://www.stack-ai.com/blog/state-of-generative-ai-in-the-enterprise (accessed Sep. 07, 2025).

[27] "Deepfake Attacks & AI-Generated Phishing: 2025 Statistics," ZeroThreat, Jun. 27, 2025. https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics

[28] E. Bonnie, "101 Data Privacy Statistics: The Facts You Need To Know In 2024," Secureframe, Jan. 01, 2025. https://secureframe.com/blog/data-privacy-statistics

Journal of Computer Science and Engineering in Innovations and Research

Research Paper Vol.-2, Issue- 1, June- December 2025 ISSN: 3049-1762