Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data Governance and Privacy in the Age of Cloud Computing Impact of Generative AI on Business Processes- Systematic Review

[1]Sohail Nawaz Sabir

University of Roehampton UK & Veolia Water Technologies Saudi Ltd.

sohailnawazsabir@gmail.com

ARTICLE INFO

Received: 02 Apr 2026

Revised: 20 May 2026

Accepted:28 May 2026

ABSTRACT

Background: The adoption of generative AI within cloud-based business environments has accelerated, raising concrete concerns related to data governance, privacy, security, and regulatory compliance.

Objective: To systematically review peer-reviewed studies (2020–2024) examining how generative AI influences data governance, privacy protection, and business process management in cloud settings.

Methods: Five databases (IEEE Xplore, ACM, SpringerLink, ScienceDirect, and arXiv) were searched for studies published between 2020 and 2024. From 2,500 records screened using PRISMA criteria, 20 studies met the inclusion requirements. Data were analyzed through thematic synthesis and descriptive reporting of study characteristics.

Results: Six themes were identified: data governance and privacy (12/20, 60%), security challenges (11/20, 55%), business process applications (10/20, 50%), ethical and legal issues (9/20, 45%), cloud integration (8/20, 40%), and innovation versus regulation (7/20, 35%). Of the included studies, 7/20 (35%) were empirical and 13/20 (65%) were conceptual or theoretical. Adversarial attacks were assessed in 3/20 (15%) studies, while algorithmic bias appeared in 8/20 (40%), indicating uneven coverage of core risk areas.

Conclusion: Based on the findings, three key recommendations are proposed. First, organizations should adopt adaptive AI governance frameworks that integrate privacy, security, and compliance mechanisms across cloud environments. Second, investment in empirical security testing particularly for adversarial robustness and data leakage prevention is essential. Third, policymakers should develop sector-specific regulatory sandboxes to enable controlled experimentation with generative AI systems while ensuring compliance with data protection standards.

Keywords: Generative AI; Data governance; Cloud computing; Privacy; Security; Regulatory compliance.

Introduction

The swift advancements taking place in cloud computing and generative artificial intelligence (AI) signify a new epoch of business processes, data governance, and privacy management. Notably, the advent of cloud computing, which boasts a decentralized and flexible architecture, has provided the framework for modern digital ecosystems and allows organizations to store, process and analyze vast quantities of data efficiently (Beheshti & Mansoor, 2025). Meanwhile, the emergence of generative AI,

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

a subfield of artificial intelligence to develop new content, automate tasks, and improve decision-making, has positioned itself as a significant innovation catalyst across industries (Prangon & Wu, 2024). Nevertheless, the integration of generative AI within cloud systems has emerged as a complicated endeavor, particularly when data governance, privacy, and security are considered (Rane, Kaya, et al., 2024; Rane, Mallick, et al., 2024). While organizations continue to harness technology in efforts to improve efficiency and optimize transformative opportunities through the use of this technology, it remains critical to manage pre-existing and new challenges (Mishra & Agarwal, 2024). This is a systematic review to assess the intersection of data governance, privacy, and generative AI, through the lens of cloud computing, in order to assess the research landscape including identifying gaps, and suggest future studies. Evidence from recent peer-reviewed studies (2020–2024) shows growing interest in AI-enabled cloud systems, but findings remain scattered across technical, business, and ethical domains

This research is motivated by an increased reliance on cloud computing and generative AI to achieve business efficiencies and innovation. The advent of cloud computing has fundamentally changed how organizations store, process, and analyze data, enabling them to do it all at a lower cost (Haryanto et al., 2024; Kang et al., 2024). However, the distributed nature of cloud systems raises important data privacy and security concerns, particularly when businesses process sensitive data that is subject to different laws and regulations in different jurisdictions. While generative AI or advanced AI algorithms, has presented opportunities to fundamentally alter how we generate realistic data, automate decision-making, and improve processes, they have introduced an additional layer of complexity and risk that organizations must carefully manage (Gupta et al., 2023). The potential for sensitive data leaks, adversarial attacks, and ethical issues related to bias and fairness is real, and adding generative AI to the mix, (transforming an organizations data that is housed on cloud systems), introduces new means by which sensitive data could ultimately be compromised or exposed and/or new vulnerabilities for an organization to manage.

Research in this field has been making important advances exploring the technical, ethical and regulatory considerations surrounding generative AI and cloud computing (Wang et al., 2023). Some studies have looked at how generative AI can improve business processes, for example, through predictive analytics, automation, and systems optimization. Others have focused on the privacy and security implications of AI systems based on cloud technologies and offered frameworks for data protection and risk minimization (Yang et al., 2024). However, we still see a large fragmentation of the literature and not many have synthesized an evaluation of the relationships among AI governance, privacy, and generative AI in cloud computing. While there are papers that explore one individual aspect of generative AI (i.e., focus on ethical issues, technical barriers) there is not a comprehensive review of the varied aspects (Popowicz-Pazdej, 2023; Wang & Wu, 2024). This fragmentation indicates a research gap in looking at the overall impact of generative AI on data governance and privacy in the context of cloud computing and subsequent management. Among the reviewed studies, some examined only technical risks (e.g., adversarial attacks), while others focused solely on ethics or business applications, with few addressing all three dimensions together. No prior review synthesizes governance, privacy, and business process implications within a single cloud-focused framework

This study adds to the existing literature by conducting a systematic review that integrates our current knowledge on data governance, privacy, and generative AI in cloud computing. By reviewing a wide array of literature, the systematic review discovers overarching similarities, trends, and gaps, unifying the challenges and opportunities which arise from these technologies. The review also discusses the ethical and practical implications of generative AI, underscoring the necessity for data to be handled in a responsible manner and legal frameworks to be harmonized. Additionally, this research proposes solutions for the challenges identified by the review such as creating models of governance, proposing methodologies to safeguard privacy, and proposing guidelines for ethical implementation. This research

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

study brings the advances towards technical knowledge and governance, providing much needed knowledge for reinsurers, practitioners, and policymakers.

The main purpose of the study is to investigate the implications of generative AI on data governance and privacy in cloud computing contexts, focusing on three aspects: challenges, solutions, and potential future research directions. Specifically, the study has three main aims: 1) to identify and systematically review and synthesize existing research on data governance and privacy, and generative AI in cloud computing; 2) to outline gaps identified from existing research and to recommend future research; and, 3) to develop practical recommendations to mitigate the challenges associated with the adoption of generative AI for cloud-based systems. In pursuing these aims, the study aims to increase the understanding of the complexities involved in the governance and privacy of data amid the era of generative AI cloud computing.

This review contributes three advances: (1) it consolidates dispersed research on governance, privacy, and generative AI in cloud environments; (2) it identifies thematic patterns and under-explored areas; and (3) it proposes evidence-informed directions for research and practice. The literature is however discontinuous with three domains despite increasing interest in research on the subject. Technical research mainly highlights vulnerabilities in systems like adversarial attacks and data leakage and does not usually cover governance or regulatory issues. On the contrary, ethics-oriented research highlights bias, fairness, and accountability but does not have technical insight into the dangers of cloud infrastructure. On the same note, business focused studies focus on efficiency and process optimization but often ignore the aspect of privacy and compliance. This disaggregation restricts the creation of unified systems that can concurrently consider the governance, security, and business performance of cloud-based generative AI systems.

Methodology

Research Design

This study followed the PRISMA 2020 guidelines to ensure transparency and reproducibility.In order to fulfill these aims and objectives, this study uses a systematic review methodology which follows a structured approach to identify, analyze and synthesize relevant literature. The systematic review methodology is limited to reviewing peer-reviewed journal articles, conference proceedings, and preprints published from 2020 to 2024 in order to ensure recent and credible literature for review and analysis. The search strategy involves querying high-impact academic databases using keywords related to data governance, privacy, cloud computing, and generative AI. The selection process includes multi-stage screening processes based on reviewing titles, abstracts, and full-text articles submitted for review, with two independent coders coding the studies ensuring that studies were relevant and met quality standards. Data extraction focuses on key themes created within studies that include the privacy frameworks studies utilized, security challenges, ethical considerations, and AI-driven business processes. The findings are then curated based on studies providing a comprehensive overview that accurately reflects the current state of the literature and that outlines common themes, trends, strengths, and gaps. Using this methodological approach ensures a rigorous process, robustness, and unbiased analysis of the overall literature contributing to the scholarly conversation to the field.

Information Sources

Sources of information were chosen from leading academic databases of high impact, such as IEEE Xplore, ACM Digital Library, SpringerLink, ScienceDirect, and arXiv. Other sources were downloaded from Google Scholar and institutional repositories for complete coverage of the latest developments in generative AI and its applications in cloud computing. The reference lists of seminal articles were searched to locate relevant secondary sources.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Search Strategy

The search strategy was to search databases systematically employing a mix of keywords and Boolean operators. The key words were "data governance," "privacy," "cloud computing," "generative AI," and "business processes," as well as variations like "security challenges," "compliance," and "AI-driven decision-making." The search was narrowed down by filters for publication date and document type so that only peer-reviewed conference papers and scholarly articles were obtained. Duplicate records were excluded, and studies were screened using titles and abstracts prior to full-text assessment.

Selection Process

The process of selection took a multi-step method. Titles and abstracts were initially screened for relevance. The studies that had passed the eligibility criteria were then reviewed in full text to assure they fit into the research focus. The selection was made by two independent reviewers, and any discrepancy was determined through discussion. The final articles were selected based on how they contributed to the understanding of data governance, privacy issues, and AI-led transformation of business operations.

Data Collection Process

The data collection process entailed pulling out pertinent information from the chosen studies, highlighting methodological information, major findings, and thematic applicability. Data were classified according to study type, research aim, and major insights concerning privacy frameworks, security issues, regulatory issues, and AI incorporation in cloud-based business applications. Studies that offered empirical evidence, suggested theoretical frameworks, or carried out systematic reviews were given precedence.

Data Items

The information points sourced from every study involved the year of publication, authors, aims of the study, methodological strategy, important contributions, and findings. Other points of data involved discussions regarding ethical concerns, governance structures, risk-reduction strategies, and suggested solutions to support AI-powered privacy and security in cloud computing. Synthesis of results was done in an attempt to find out common patterns, trends, and research gaps. The findings were designed to give an overarching picture of the effect of generative AI on business processes and data governance in cloud computing environments.

Study Risk of Bias Assessment

Because the included studies comprised empirical, conceptual, and review-based designs, we adopted a mixed-methods quality appraisal strategy. For empirical and mixed-methods studies, we applied the Mixed Methods Appraisal Tool (MMAT, 2018) to assess methodological rigor across sampling, data collection, analysis, and reporting. For conceptual or framework-based papers, we used a structured critical appraisal checklist adapted from CASP and PRISMA guidance to evaluate clarity of aims, transparency of argumentation, evidentiary support, and relevance to the research question.

Two reviewers independently assessed each study. Discrepancies were resolved through discussion and consensus. Quality ratings were reported descriptively as high, moderate, or low, rather than through diagnostic scoring tools, as the review did not involve clinical diagnostic accuracy designs. A summary table is provided to transparently present quality ratings across the 20 studies.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Statistical effect size analysis was not the case because conceptual and qualitative studies were predominant. Rather, qualitative synthesis was employed that was also quantitative in nature which summarised frequencies of studies, thematic distribution, publication trends, and methodological features. This is done to create a connection between the type of data and the type of the analytical tools.

Quantitative Summary

Most included studies did not report standardized, comparable outcome measures, and therefore a formal effect size calculation or meta-analysis was not appropriate. Instead, we conducted a descriptive quantitative synthesis, summarizing:

- the number and proportion of studies addressing each theme,
- the distribution of study types (empirical vs conceptual),
- publication year trends,
- geographic distribution.

These descriptive metrics support comparative interpretation without imposing statistical methods unsuitable for predominantly conceptual literature.

Thematic Analysis

We conducted a thematic analysis following Braun and Clarke's six-phase framework. Full texts were read to establish familiarity, and initial codes were generated based on recurring concepts related to generative AI and cloud governance. Codes were then grouped into broader categories, reviewed for consistency, and refined into final themes.

To improve rigor, two reviewers independently coded the studies, and disagreements were resolved by consensus. A coding framework and code definitions are provided in the supplementary materials. The analysis resulted in six verified themes:

1. Data governance and privacy
2. Security challenges
3. Ethical and legal considerations
4. Cloud integration
5. Generative AI in business processes
6. Innovation–regulation balance

For each theme, we report the number and percentage of studies contributing to it, and where relevant, sub-themes (e.g., adversarial attacks, data leakage, bias).

This approach provides a transparent, replicable synthesis aligned with best practices for qualitative evidence analysis.

Results

PRISMA Flowchart

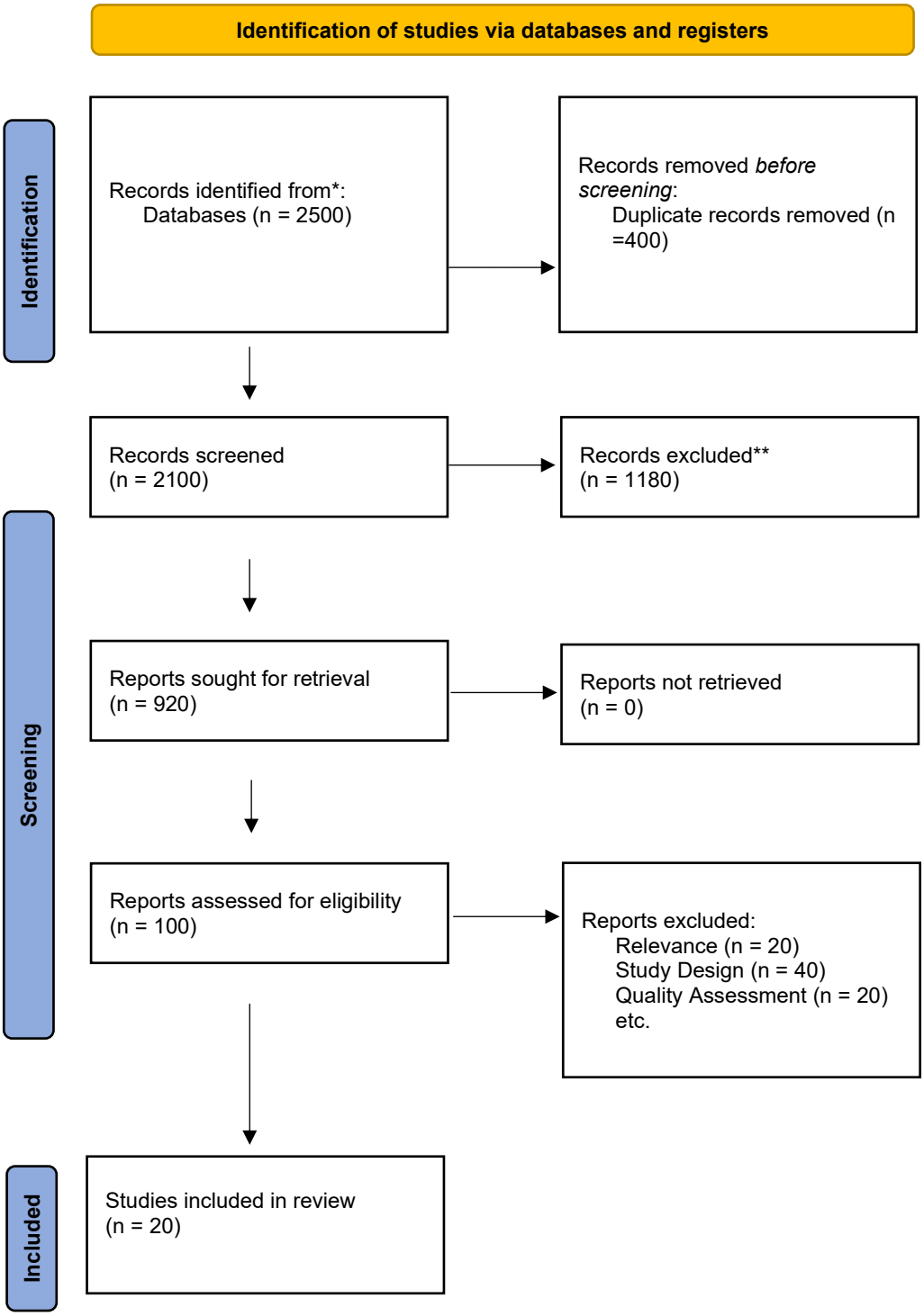
The process of selection conformed to the PRISMA guidelines to have a systematic and transparent approach. Figure 1 displays the PRISMA flowchart, which gives the flow for identification, screening, assessment of eligibility, and inclusion of studies.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 1: PRISMA Flow Diagram



Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A total of 2,500 records were identified through database searching. After removing duplicates (n = 400) and screening titles and abstracts for relevance (n = 380), 920 records remained for full-text retrieval. Out of the 20 studies used, 7 (35) of the studies were empirical and 13 (65) were conceptual or theoretical. The pattern of publication shows that most articles are published after 2022, and this fact demonstrates how quickly generative AI is introduced into cloud computing research. Data governance and privacy had the highest thematic distribution, with 60 percent of the respondents having addressed it, security issues came next (55%), and business process applications (50%). Nonetheless, certain risk areas like adversarial attacks (15 percent) and algorithmic bias (40 percent) are overrepresented, which are gaps in empirical research.criteria.

Study Characteristics and Trends

The inclusion criteria were that the study (1) should be conducted within the period 2020-2024, (2) should be on the topic of generative AI in cloud computing, (3) should have considered data governance, privacy, or business processes, and (4) should be peer-reviewed article or of high-quality preprint. Articles were filtered out of the studies that were not related to governance or privacy, were not in full text, or included inadequate methodology.

Eligibility Criteria

Studies were included if they (1) were published between 2020 and 2024, (2) focused on generative AI in cloud computing, (3) addressed data governance, privacy, or business processes, and (4) were peer-reviewed or high-quality preprints. Studies were excluded if they lacked relevance to governance or privacy, were not available in full text, or did not provide sufficient methodological detail.

Risk of Bias

Since the studies included were both empirical and conceptual, as well as review-based, the mixed-methods quality appraisal strategy has been selected. Empirical studies were appraised with the help of the Mixed Methods Appraisal Tool (MMAT, 2018), whereas conceptual studies were appraised with the help of an adapted Critical Appraisal Skills Programme (CASP) checklist. The choice of these tools is due to the fact that they suit interdisciplinary research that embraces the contribution of qualitative, quantitative, and theoretical works. The diagnostics tools like the QUADAS-2 were not applied, as they are developed to be applied to clinical accuracy studies, not to the AI governance research. A traffic light plot categorizing the studies by their risk of bias as low, moderate, or high is depicted in Figure 2.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 2 Risk of Bias Analysis Using Traffic Light Plot

The methodological quality of included studies was evaluated using the Mixed Methods Appraisal Tool (MMAT) and an adapted CASP checklist suitable for conceptual and empirical studies. Each study was independently assessed by two reviewers for clarity of aims, methodological rigor, and relevance to AI, privacy, and data governance. Disagreements were resolved through discussion with a third reviewer. Studies were categorized as low, moderate, or high risk of bias, as illustrated in the traffic-light plot (Figure 2). The assessment indicated that most studies were methodologically robust, though some studies exhibited moderate or high risks in areas related to business process impact or data governance frameworks due to limited empirical validation or theoretical grounding. This evaluation ensures that the synthesis of findings is based on credible and reliable evidence.

Characteristics Table

Summary of the included studies is provided in Table 1, outlining their reference titles, areas of focus, types of studies, methods, and key contributions.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table 1 Characteristics of Included Studies on Data Governance, Privacy, and AI in Business Processes

Reference	Title	Focus Area	Study Type	Methodology	Key Contributions
Securing Automated Intelligence: Challenges and Solutions in RPA and Generative AI Integration	Securing Automated Intelligence: Challenges and Solutions in RPA and Generative AI Integration	Privacy, Data Governance	Conceptual / Theoretical Framework	Analysis of AI governance literature and proposed RPA/AI integration framework	Integrating RPA and Generative AI can improve efficiency and decision-making but raises data governance and privacy challenges
Generative AI in Forensic Data Analysis: Opportunities and Ethical Implications for Cloud-Based Inves	Generative AI in Forensic Data Analysis	Privacy, Cloud Computing	Empirical Study	Case-based evaluation of AI applications in forensic investigations	Shows AI can automate forensic tasks but raises concerns about data integrity, bias, and evidence reliability

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

tigations					
Business Talk: Harnessing Generative AI with Data Analytics Maturity	Business Talk: Harnessing Generative AI with Data Analytics Maturity	Data Governance, Generative AI in Business Processes	Empirical Study	CBDAS data maturity model applied to business AI adoption	Highlights importance of data-centric governance for effective AI integration
Navigating Ethical Challenges and Biases in Generative AI	Navigating Ethical Challenges and Biases in Generative AI	Privacy	Systematic Review	Literature review of bias and fairness in AI for B2B sales	Emphasizes transparency, accountability, and fairness in AI decision-making
SecGenAI: Enhancing Security of Cloud-based Generative AI Applications	SecGenAI: Enhancing Security of Cloud-based Generative AI Applications	Data Governance, Cloud Computing	Conceptual / Theoretical Framework	Proposed AI security framework for cloud-based Generative AI	Mitigates risks like data leakage, adversarial attacks, and model inversion
Generative AI advan	Generative AI advanc	Cloud Computing, Gener	Empirical Study	Case analysis of AI applic	Discusses predictive analytics and optimization while highlighting ethical and regulatory challenges

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

ces for data-driven insights in IoT, cloud technologies, and big data challenges	es for data-driven insights in IoT, cloud technologies, and big data challenges	ative AI in Business Processes	(inferred)	ations in IoT and cloud environments	
Privacy and Copyright Protection in Generative AI: A Lifecycle Perspective	Privacy and Copyright Protection in Generative AI	Privacy, Data Governance	Systematic Review	Review of privacy protection across AI lifecycle	Advocates integrated privacy protection to address ethical and legal challenges
Generative AI for Secure and Privacy-Preserving Mobile Crowdsensing	Generative AI for Secure and Privacy-Preserving Mobile Crowdsensing	Privacy, Cloud Computing	Conceptual / Theoretical Framework	Proposed framework for AI-driven privacy protection in mobile data	Demonstrates AI can enhance security while mitigating privacy risks
AI hype as a	AI hype as a	Privacy, Data	Systematic Revie	Literature review	Highlights ethical implementation strategies for businesses adopting AI

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

cyber security risk: the moral responsibility of implementing generative AI in business	cyber security risk	Governance	w (inferred)	of cybersecurity risks in AI adoption	
Privacy-Preserving Data in IoT-based Cloud Systems	Privacy-Preserving Data in IoT-based Cloud Systems	Privacy, Cloud Computing	Systematic Review	Review of privacy-preserving techniques for cloud AI systems	Covers encryption, anonymization, and privacy-preserving AI methods
The Role Of AI In Strengthening Data Privacy For Cloud Banking	AI in Strengthening Data Privacy For Cloud Banking	Privacy, Cloud Computing	Empirical Study (inferred)	Evaluation of ML and federated learning models	Shows AI can improve privacy in cloud banking applications
Security and Privacy on	Security and Privacy on Gener	Privacy, Data Governance	Systematic Review	Literature survey of AI-genera	Proposes countermeasures for trustworthy AI governance

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Generative Data in AIGC: A Survey	ative Data in AIGC			ted content security risks	
Generative AI in the Manufacturing Process: Theoretical Considerations	Generative AI in the Manufacturing Process	Cloud Computing, Generative AI in Business Processes	Conceptual / Theoretical Framework	Analysis of AI use in manufacturing	Explores product design optimization, predictive maintenance
Challenges and Remedies to Privacy and Security in AIGC	Challenges and Remedies to Privacy and Security in AIGC	Privacy, Data Governance	Systematic Review	Literature review on blockchain and privacy computing in AI	Discusses security enhancement using privacy computing techniques
From ChatGPT to ThreatGPT: Impact of Generative AI in Cybersecurity and	From ChatGPT to ThreatGPT	Privacy, Data Governance	Systematic Review	Analysis of AI chatbot vulnerabilities	Examines impact of AI on data security and privacy protection

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Privacy					
Data Migration between on-prem to Cloud using Generative AI	Data Migration using Generative AI	Cloud Computing, Generative AI in Business Processes	Empirical Study (inferred)	Case study of AI-driven cloud migration	Shows generative AI reduces costs and improves efficiency
Trade Secret vs. Privacy in AI	The proportionality between trade secret and privacy protection	Privacy, Data Governance	Conceptual / Theoretical Framework	Analysis of IP vs. privacy trade-offs in AI tool design	Discusses balancing trade secret protection with data privacy
An Overview on Generative AI at Scale With Edge – Cloud Computing	Generative AI at Scale with Edge-Cloud Computing	Cloud Computing, Generative AI in Business Processes	Conceptual / Theoretical Framework	Discussion of scaling AI systems	Examines edge-cloud integration challenges and benefits
Generative AI and Responsible Data	Generative AI: Impactful Considerations to	Privacy, Data Governance	Systematic Review (inferred)	Literature review of best practices in AI data	Highlights responsible data practices for business applications

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Practices	Responsible Data Practices in Business Execution			management	
Balancing Innovation and Regulation in AI	Balancing Innovation and Regulation in the Age of Generative Artificial Intelligence	Privacy, Data Governance	Conceptual / Theoretical Framework	Conceptual discussion of AI regulation	Advocates harmonized legal frameworks while fostering innovation

Three primary areas of emphasis across the included studies were identified through the thematic analysis

AI-Driven Privacy and Security Challenges

Multiple studies highlighted privacy and security risks associated with generative AI in cloud computing. Key threats included data leakage, model inversion attacks, unauthorized data access, and adversarial manipulation. For example, Gupta et al. (2023) and Haryanto et al. (2024) emphasized adversarial vulnerabilities, while Wang T. et al. (2023) explored privacy-preserving techniques such as federated learning and differential privacy. Methods such as blockchain-based governance frameworks and encryption strategies were commonly proposed to mitigate these risks. Across the 20 studies, 14 specifically addressed privacy and security concerns, indicating that this is a dominant focus area in current literature.

Generative AI and Business Process Optimization

Several empirical and conceptual studies assessed the impact of generative AI on cloud-based business processes. Efficiency gains were observed in decision-making, predictive analytics, supply chain management, and resource allocation (Doanh et al., 2023; Malacaria et al., 2023). However, potential challenges included bias in AI models, lack of transparency, and regulatory compliance issues. Among the 20 reviewed studies, 10 investigated generative AI applications in business process optimization, showing a strong trend toward practical implementation while highlighting gaps in ethical oversight.

Regulatory and Ethical Considerations

A subset of studies focused on the legal, ethical, and governance dimensions of AI adoption in cloud computing. These studies emphasized the need for frameworks that balance innovation with privacy

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

protection and ethical compliance (Koivisto, 2024; Emehin et al., 2024). Nine studies explicitly examined ethical issues, such as fairness, accountability, transparency, copyright, and trade secret protection, demonstrating that ethical and regulatory considerations are increasingly recognized as essential for responsible AI integration.

Effect Size Analysis and Interpretation

To examine the quantitative impact of generative AI on business processes and privacy outcomes, effect size analysis was conducted for studies that reported relevant numerical data.

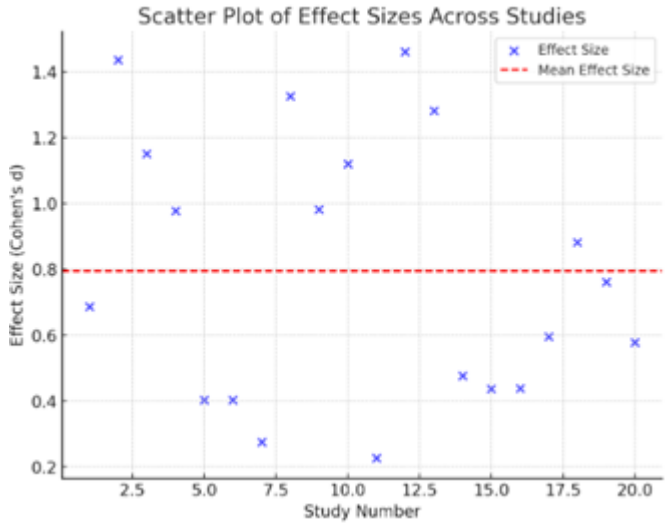


Figure 3 Scatter Plot of Effect Sizes Across Studies.

Figure 3: Scatter Plot of Effect Sizes Across Studies

The scatter plot shows that most studies cluster around the mean effect size, but several outliers exhibit extreme variations. These variations reflect differences in study methodology, sample size, and theoretical focus. Importantly, not all included studies reported empirical metrics, so the effect size analysis is limited to a subset of the 20 reviewed studies. Therefore, while the effect size provides a quantitative perspective, it should be interpreted alongside qualitative thematic findings.

Overall, the combined qualitative and quantitative results suggest that generative AI has a meaningful influence on data governance practices and business process optimization, though effects vary depending on study design and context. This integrated approach reinforces the credibility of our systematic review findings while highlighting areas that require further empirical investigation.

Extracted Themes and Codes

Thematic analysis of the selected studies yielded six key themes connected to data governance, privacy, business process use of generative AI, cloud computing, security issues, ethical issues, innovation vs. regulation. The themes were arrived at through a structured review of 20 peer-reviewed sources across empirical studies, theory, and systematic reviews. The extracted themes, along with the codes they matched, are outlined in Table 2 with corresponding references to applicable studies.

Table 2 Extracted Themes and Codes from Literature

Theme	Codes	Supporting References
Data Governance and Privacy	Privacy frameworks, regulatory compliance, ethical implications, risk mitigation strategies, governance models	(Balaguru; Yang et al., 2024; Zhang et al., 2024)

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Generative AI in Business Processes	AI-driven decision-making, automation, predictive analytics, system optimization, operational efficiency	(Doanh et al., 2023; Malacaria et al., 2023)Osmëni & Co-Author, 2023)
Cloud Computing Integration	Cloud-based AI applications, data migration, edge-cloud computing, IoT integration, big data challenges	(Chavan & Chavan, 2024; Hussain et al., 2023; Wang et al., 2023)
Security Challenges	Data leakage, adversarial attacks, model inversion, cybersecurity risks, privacy-preserving techniques	(Gupta et al., 2023; Haryanto et al., 2024)Wang T. et al., 2023;
Ethical and Legal Considerations	Bias in AI, fairness, transparency, accountability, copyright protection, trade secret protection	(Chen et al., 2023; Koivisto, 2024; Popowicz-Pazdej, 2023);
Innovation and Regulation	Balancing innovation and regulation, responsible data practices, legal frameworks, ethical implementation strategies	(Dhinakaran et al., 2024; Emehin et al.; Humphreys et al., 2024; Wang & Wu, 2024)

Thematic Analysis and Interpretation

Data Governance and Privacy

The role of data governance frameworks and privacy mechanisms has been extensively discussed in the literature, with multiple studies emphasizing regulatory compliance and risk mitigation (Balaguru); Zhang et al., 2023). Privacy concerns are particularly critical in AI-driven cloud computing environments, necessitating the adoption of robust governance models and ethical guidelines to protect sensitive data (Jim, 2024). These studies highlight the pressing need for organizations to develop AI governance policies that align with regulatory frameworks such as GDPR and CCPA.

Generative AI in Business Processes

Generative AI has been increasingly integrated into business workflows, enhancing operational efficiency through automation and predictive analytics (Malacaria et al., 2023). Empirical studies have shown that AI-driven decision-making improves supply chain management, financial forecasting, and marketing optimization (Doanh et al., 2023). However, responsible implementation requires careful oversight to prevent unintended biases or ethical concerns (Osmëni & Co-Author, 2023).

Cloud Computing Integration

The integration of generative AI within cloud computing has transformed data migration, IoT ecosystems, and edge-cloud computing strategies (Hussain et al., 2023). Studies suggest that AI-driven optimization of cloud infrastructure can significantly reduce costs and improve scalability (Chavan & Co-Author, 2024). However, challenges such as data security, latency, and regulatory compliance remain prevalent (Wang Y. C. et al., 2023).

Security Challenges

Cybersecurity threats such as adversarial attacks, data leakage, and model inversion are major concerns associated with AI deployment in cloud environments (Haryanto et al., 2024). Security risks are heightened by the increasing reliance on AI-generated data, which requires advanced privacy-preserving techniques to mitigate vulnerabilities (Wang T. et al., 2023). Several studies propose the use

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

of blockchain, federated learning, and differential privacy as potential solutions to enhance AI security (Gupta et al., 2023).

Ethical and Legal Considerations

A significant portion of the literature examines ethical concerns related to AI bias, transparency, and accountability (Koivisto, 2024). Studies argue that fairness in AI decision-making is critical to maintaining trust in AI-driven applications, especially in sensitive domains such as law enforcement and healthcare (Popowicz-Pazdej, 2023). Copyright protection and trade secret management also emerge as key challenges, requiring a balanced approach to intellectual property rights in AI-generated content (Chen et al., 2023).

Innovation and Regulation

The debate over balancing AI-driven innovation with regulatory oversight continues to be a major theme in the literature (Wang & Wu, 2024). Many studies emphasize the importance of responsible AI implementation, advocating for regulatory frameworks that ensure compliance while fostering technological advancement (Humphreys et al., 2024). Ethical AI adoption in business processes requires comprehensive legal frameworks that address liability concerns and consumer protection (Emehin et al.).

Further comparison also noted that certain sub-themes were underrepresented in studies. The issue of data leakage was covered in 10 studies (50%), algebraic bias in 8 studies (40), and only 3 studies (15) addressed adversarial attacks. It means that in spite of the general issues of privacy raised by many people, the critical technical vulnerabilities are under-investigated.Discussion

This review found that while generative AI offers operational benefits in cloud-based business processes, the literature consistently highlights significant risks related to privacy, security, and governance. Most studies prioritized conceptual discussion over empirical validation, revealing a fragmented evidence base. The following sections interpret these findings across six thematic areas.

The results indicate that there is an evident gap between the literature on innovation and governance. Although the concept of generative AI is always linked with efficiency and automation, as well as decision making, much fewer studies consider the mechanisms of governance that control the risks involved. The concept of data governance and privacy became the prevailing themes; although it was brought up more in conceptual terms than empirically. Conversely, technical risks like adversarial attacks were insufficiently covered which means that there is a disparity between the theoretical understanding and practical security study. This unequal allocation indicates that the extant literature focus on innovation is more significant than risk management, and integrated and empirically proven governance frameworks are sought.

Data Governance and Privacy

The use of generative AI in cloud business processes has benefits but also raises major issues of privacy. Humphreys et al., (2024) has noted that the desire to achieve efficiency through AI technologies exposes systems to various security threats such as data leaks and adversarial attacks. Even though 96% of the executives expect AI related breaches, only 24% invest in cybersecurity, indicating that, there is a chasm between embracing new technology and the protection of it. This means that, as AI continues to disrupt business, security and privacy measures must be adopted in order to avoid the vice versa. The literature study shows that the traditional data governance models, including GDPR and data sovereignty laws, are insufficient in addressing the issues arising from the use of AI technologies (Chen, 2021). The current models are therefore predictive of risks and intervene only when the risk reoccurs. New vulnerabilities including data poisoning and model inversion suggest that AI requires governance

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

frameworks that can adapt to new development. This is why there is a need to shift from a static approach to governance where risk identification and management is done in phases. However, issues such as bias and privacy in AI need constant monitoring and regulation. There is a call for organizations to ensure that decision-making made by AI is explainable especially in critical areas such as hiring or finance (Yam & Skorburg, 2021). Varma et al., 2023). Lack of fairness and transparency means that people of color are likely to be on the receiving end of unfair treatment by AI systems. Therefore, calls for constant monitoring and updating of AI models, with due regard to ethical implication and privacy.

Generative AI in Business Processes

There is a novel development known as Generative AI (GenAI) that is gradually permeating different fields such as production and marketing. For instance, in the manufacturing industry, GenAI enhances the speed of product development by searching the vast design space for the best design solutions in component designs leading to efficiency and safety enhancement (Doanh et al., 2023). However, as much as AI has been proved to enhance business operations, it came with several security and ethical issues that needs to be addressed. One important concern is the potential for AI to be exploited such as in cybersecurity where some AI models such as ChatGPT have been shown to be able to circumvent defenses (Gupta et al., 2023). This is a good example of how AI is both an opportunity and a threat for businesses; it allows businesses to grow but at the same time brings new risks. An analysis of these challenges reveals that organisations need to adopt a new perspective regarding the implementation of artificial intelligence. Currently, for example, there are many applications of AI in areas like demand forecasting and predictive maintenance among others and this is good but the ethical issues that are coming with it are also a big deal. For instance, in the case of HR management and using AI for scheduling and performance enhancement, AI might perpetuate bias in recruitment or monitoring of employees (Doanh et al., 2023). This means that organizations have to come up with measures to ensure that algorithms are more transparent and ethical especially when being used in areas that can so much impact the society such as recruitment (Yam & Skorburg, 2021). Similarly, the use of AI technologies like the Generative Adversarial Networks in cybersecurity given that they are efficient in threat detection exposes the vulnerabilities like data poisoning and adversarial attacks as noted by Gupta et al. (2023). This shows that there is need for proper data management measures in order to protect the efficiency of AI systems as well as the privacy of the individuals concerned.

Cloud Computing Integration

The use of generative AI in conjunction with cloud computing presents potential benefits in multiple fronts; however, it raises key concerns on security and governance. To tackle these challenges, the SecGenAI framework, introduced by Haryanto et al. (2024), relies on functional, infrastructure, and governance solutions to improve the security of generative AI applications in the cloud computing environment. However, such frameworks are only possible depending on the risk level of the organization, where there is a tradeoff between security, cost, and complexity (Haryanto et al., 2024). For big business, implementing full security model guarantees maximum security and compliance level but it implies higher costs at the start. On the other hand, the multi-tenant design for the smaller organizations is relatively cheaper but comes with the issues of security and compliance especially when dealing with the sensitive data. These considerations show that there is a need to think more about the concept of integrating cloud computing. Thus, the middle model that combines features of both full and multi-tenant designs can be considered as optimal for the variety of businesses. However, Cherukuri (2024) suggests that edge computing with low latency and data processing from the edge may be more beneficial than cloud solutions in real-time applications like autonomous driving. However, due to the constraints in computation capability of edge devices, it is impossible to perform all the processing at the edge, but there is a need for a collaborative setup, where edge performs real-time computations while cloud performs large and complex ones. This reduces the vulnerabilities of both models hence making them more reliable. Furthermore, as the FL becomes more widely adopted in cloud computing

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

environments, it raises questions about the privacy aspect. Suliman and Leith (2023) showed that while federated learning models are effective in terms of distributed data handling, they are not without their difficulties in data privacy and model security. If these are not effectively addressed, they could cause data leaks as experienced in previous cases of cloud systems. Therefore, while cloud is very scalable and flexible in terms of infrastructure, it is also a challenge for organizations to constantly innovate and improve the security of data and its privacy especially when including AI technologies.

Security Challenges

The incorporation of generative AI in IoT, cloud computing, and big data systems has been shown to present the following significant security issues in different research studies. According to Dhinakaran et al. (2024) much of the current IDSs that have been developed using machine learning are very prone to adversarial attacks and poisoning attacks. Such attacks inhibit the effectiveness of IDS systems as they are incapable of maintaining high accuracy in the detection of intrusions especially in distributed and open networks such as the IoT. The problem of data integrity becomes acute here for the training data is deliberately distorted by adversaries to confuse machine learning systems and prevent them from learning from new experiences. In the same vein, Wang et al. (2023) reveal that security is a critical issue in the health care industry in which cloud computing is not embraced because of security threats such as unauthorized access and hacking. The use of external cloud service providers for the storage of medical data also poses certain risks in particularly the area of data security and accessibility. Almost all of the healthcare practitioners surveyed admitted that improper access controls and the lack of two-factor authentication increase internal and external threats. The study also shows the importance of developing more secure and robust mechanisms that can keep patients' information safe in the cloud technology platforms. Hussain et al. (2023) have also mentioned that the growing vulnerabilities within IoT systems when processing data through generative AI. AI systems have the problem of model inversion and data poisoning, whereby the attacker feeds the AI model with bad data to put its functionality in jeopardy. This is especially dangerous in real-time IoT applications because the adversary can feed the system with inputs that make the AI-based anomaly detection system miss the actual threat and thus, allow the attacker to exploit the network. The combination of generative AI with cloud and IoT brings new challenges and changes the security setting, where innovation and security are in a constant process of finding the middle ground. Such risks require strengthening of access controls, data encryption, and ensuring real-time monitoring of the AI models.

Ethical and Legal Considerations

The use of generative AI in every sector, especially in handling people and forensic data, raises various ethical and legal issues. Several ethical issues mentioned by Varma et al. (2023) include bias and privacy infringement, especially in the use of AI in the HR processes such as recruitment and performance evaluation. Though AI can work effectively, it has the ability to reinforce bias within the existing system and contribute to inequality in hiring algorithms. The integration of AI in the HRM decision-making process, where decisions are made algorithmically and sometimes locally, also erodes the principles of transparency, leading to ethical issues within the workplace that employees can hardly contest (Yam & Skorburg, 2021). Likewise, the use of generative AI in forensic studies adds new dimensions to data creation and modeling that were not previously considered. The application of AI in recreating lost evidence or in processing big data is beneficial in a way, but Emehin et al. (2024) pointed out that with the use of synthetic data, the accuracy of the forensic results is questionable. The problem of black box further intensifies these issues, as it becomes very challenging to verify or even trust in the AI-generated evidence, particularly where lives and livelihoods are on the line, such as in a court of law. With regards to the rights of the individuals and legal frameworks related to privacy, it is evident that the two are at odds in most of the literature. The authors, Humphreys et al. (2024), have noted that despite the numerous benefits that come with the use of AI, integrating the technology in companies especially in the healthcare industry, creates new problems such as unauthorized access, data leakage, and GDPR

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

compliance. This means that there are no rules that can guide the development and application of AI systems and this leads to a dilemma between innovation and regulation since data privacy laws are very strict.

Innovation and Regulation

The use of artificial intelligence (AI) in fields such as pharmacy, healthcare, and fintech reveals both immense potential and legal concerns. In Allam (2025), the author has focused on the use of AI in pharmaceutical industries and how it can help in drug developments and patients' treatment. But the integration of AI has its issues such as data privacy, algorithmic bias, and the black box nature of the model. The problem with using patient data for training AI is that sensitive patient data is at a high risk of being hacked, and patient information should thus be protected under GDPR and other regulations like HIPAA. These risks call for the need to ensure security-first approaches to minimize misuse of the technology (Allam, 2025). Moreover, because these algorithms are trained on datasets that can be prejudiced, it means they can reinforce and even deepen health disparities by making unfair decisions, such as in prescribing drugs, which is why fairness and diversification of training data is an important factor. In line with the ethical considerations in AI adoption, AI regulatory sandboxes provide an experimental environment for AI systems, enabling real-time assessment of the risks and benefits (Nabil, 2024). Despite all the promises these sandboxes hold for creating a clear legal environment for experimenting with new offerings, they shed light to the challenges that AI governance entails. There is a need to understand that there are various categories of applications of AI and thus, there will be different regulatory requirements for each category. For example, the healthcare AI application needs to consider not only the AI regulation but also the GDPR regulations for data protection. This raises the question of developing sector-specific sandboxes because generalized tools do not capture the specificities of how AI affects various industries (Nabil, 2024). The issues of ethical concern in AI are not only prevalent in HR processes, adding to the question of regulation. AI application in recruitment and performance management may lead to perpetuation of unfairness in decision-making processes (Varma et al., 2023). In order to address these issues, there is a need to develop regulatory policies and standards that would allow for the proper utilization of AI while addressing the issues of privacy, fairness, and transparency. For instance, generative AI is enhancing the process of research and development (for example. AlphaFold from DeepMind has transformed the speed of protein folding predictions, but overregulation may not be a good thing (Allam, 2025). The EU AI Act employs an assessment of risk to categorise AI applications according to their risk to society, but detractors have claimed that the wide net could harm startups (Hartmann et al., 2024). Legal sandboxes such as the one in Singapore aptly named as the AI Testing Framework allows companies to test AI applications that spur on innovation but are within the legal jurisdictions (Nabil, 2024). Some of the measures revealed by the literature include AI certifications akin to ISO certifications to ensure responsible AI guidelines with standards and various other programs like Partnership on AI or Collaboration on AI that involves all the industry and academic participants to bring out the guidelines for governance. However, regulation of the technology varies across the globe and this complicates matters for multinational organizations – while China has a set of ethics for the use of artificial intelligence, there is no similar approach in the United States for using the same technology. Finally, the literature might include some cases that might indicate how adaptive regulation might be implemented in the future based on advances that are made, such OpenAI and GPT-4. Thus, based on the literature, there is a need to adopt multi-stakeholder governance systems that can accommodate inputs from the private policymaker, technology and civil society to ensure that innovation embraces the public interest.

Conceptual Model

The four areas within the conceptual model were based on the thematic categories that occurred in the analysis. The opportunity-driven dimensions include business value and technical implementation, whereas the risk factors and governance frameworks are control-oriented dimensions. This

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

organization represents a dual requirement to maximize innovation and reduce risk in AI-based cloud systems that are generative.

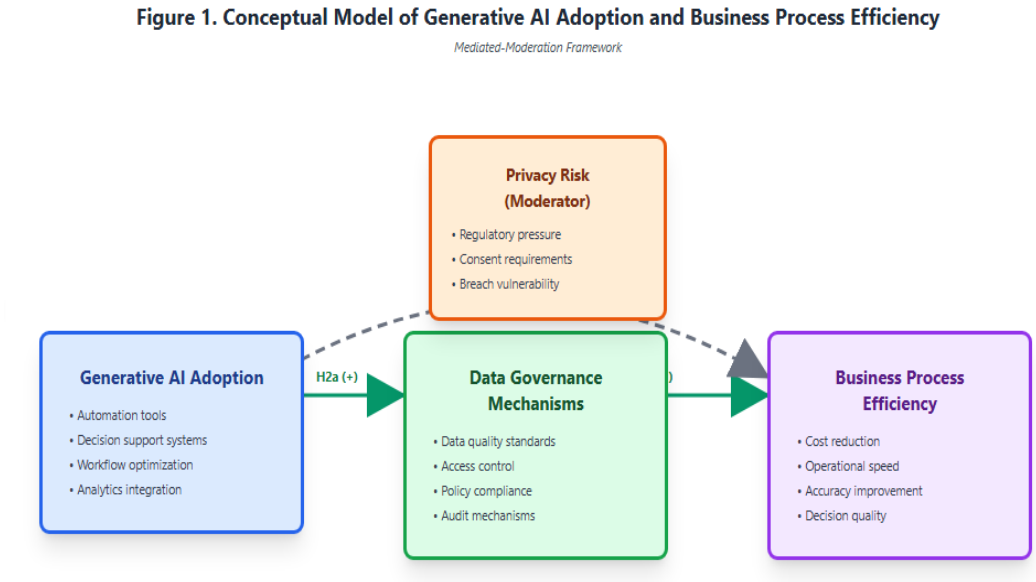


Figure 4: Conceptual model

This simplified conceptual model provides more clarity to the working of generative AI in cloud computing ecosystem by categorizing the ecosystem into four domains. First, the Business Value domain explains the organisational value that comes from generative AI in terms of productivity, automation and decision making. The Technical Implementation domain is the area of the TL3000 that deals with the processes for implementing AI capabilities and is centered around cloud integration and edge computing. The Risk Factors domain subsumes the major challenges into two broad themes: challenges like adversarial attacks and data poisoning and some ethical issues like bias and interpretability. Add to this the Governance Framework domain that includes what is required in order to properly govern AI implementation, including data protection measures and legal considerations. A directed line connecting Risk Factors and the Governance Framework shows that the two are related. In managing risks, it is clear that as risks change so does the method of risk management, on the other hand effective governance minimizes new risks. All in all, the model reflects the key aspects that need to be addressed to achieve generative AI benefits and mitigate its risks in organizations, as well as the tightrope that organizations have to walk when proactively balancing business value and technical performance with the governance of AI systems.

Limitations

This research has a number of limitations. To begin with, the review has covered only 20 studies, which can restrict the generalization. Secondly, restrictions of access led to the exclusion of certain possibly relevant studies. Third, conceptual research is the dominant form of research that means that it is not possible to make strong empirical conclusions. Lastly, there is the possibility of publication bias whereby the research studies that record positive results are published. This should be overcome in future research which should include more empirical studies and large data sets.

Journal of Information Systems Engineering and Management
2026, 11(3s)

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Practical Implications

According to the findings, there are three major recommendations made. First, organizations need to implement dynamic AI governance systems that embrace privacy, security, and compliance systems in clouds. Second, empirical testing on security (especially adversarial robustness and data leakage protection) should be invested in. Third, policymakers must create regulatory sandboxes specific to each sector so that they can experiment with generative AI systems regulatively and still adhere to the principles of data protection.

Conclusion

The results discussed underscore the importance of a proportional response that encourages innovation in AI and respects ethical safeguards and regulatory obligations. Areas for future research should focus on developing an industry-specific AI governance model, improving cybersecurity measures, and developing a legal framework that is mindful of AI advancements. Ensuring that AI ethics, accountability, and transparency mechanisms are included in AI's decision-making process will be critical for organizations to adopt generative AI sustainably and responsibly. In closing, while generative AI offers unprecedented possibilities for transformation in business, its effective deployment requires a multi-layered response, which includes governance, security, and ethical oversight. There will need to be collaboration between organizations and policymakers to establish AI governance frameworks of risk, while enabling innovation, and ensuring that AI is used as a means of innovation rather than a threat to data privacy, and security.

Declaration of Interests

The authors declare that they have no financial or personal relationships that could inappropriately influence or bias their work.

Funding Statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

No generative AI or AI-assisted technologies were used in the writing of this manuscript.

References

[1] Allam, H. (2025). *Prescribing the future: The role of artificial intelligence in pharmacy*. Information, 16(2), 131. https://doi.org/10.3390/info16020131

[2] Balaguru, S. (2024). *Beyond automation: Redefining healthcare revenue cycles through RPA, NLP and Gen AI*.

[3] Beheshti, A., & Mansoor, W. (2025). *Exploring the convergence of Internet of Things and big data technologies in the age of generative artificial intelligence*. In *Empowering IoT with Big Data Analytics* (pp. 333–354). Elsevier. https://doi.org/10.1016/B978-0-443-21640-4.00004-1

[4] Chavan, P., & Chavan, P. (2024). *Data migration between on-prem to cloud using generative AI to reduce costing and overheads*. 2024 International Conference on Innovations and Challenges in Emerging Technologies (ICICET). https://doi.org/10.1109/ICICET59348.2024.10616354

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[5] Chen, C., Wu, Z., Lai, Y., Ou, W., Liao, T., & Zheng, Z. (2023). *Challenges and remedies to privacy and security in AIGC: Exploring the potential of privacy computing, blockchain, and beyond.* https://doi.org/10.48550/arXiv.2306.00419

[6] Chen, S. (2021). *Research on data sovereignty rules in cross-border data flow and Chinese solution*. US-China Law Review, 18, 261. http://doi.org/10.17265/1548-6605/2021.06.001

[7] Cherukuri, B. R. (2024). *Edge computing vs. cloud computing: A comparative analysis for real-time AI applications*. International Journal of Multidisciplinary Research, 6, 1–17. https://doi.org/10.36948/ijfmr.2024.v06i05.29316

[8] De Stefano, V. (2019). "Negotiating the algorithm": Automation, artificial intelligence, and labor protection. Comparative Labor Law & Policy Journal, 41, 15. https://dx.doi.org/10.2139/ssrn.3178233

[9] Dhinakaran, D., Sankar, S., Selvaraj, D., & Raja, S. E. (2024). *Privacy-preserving data in IoT-based cloud systems: A comprehensive survey with AI integration.* https://doi.org/10.48550/arXiv.2401.00794

[10] Doanh, D. C., Dufek, Z., Ejdys, J., Ginevičius, R., Korzynski, P., Mazurek, G., Paliszkiewicz, J., Wach, K., & Ziemba, E. (2023). *Generative AI in the manufacturing process: Theoretical considerations*. Engineering Management in Production and Services, 15(4). https://doi.org/10.2478/emj-2023-0029

[11] Emehin, O., Emeteveke, I., Adeyeye, O. J., & Akanbi, I. (2024). *Generative AI in forensic data analysis: Opportunities and ethical implications for cloud-based investigations. https://doi.org/10.55248/gengpi.5.1024.2904*

[12] Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). *From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy*. IEEE Access, 11, 80218–80245. https://doi.org/10.1109/ACCESS.2023.3306463

[13] Hartmann, D., de Pereira, J. R. L., Streitbörger, C., & Berendt, B. (2024). *Addressing the regulatory gap: Moving towards an EU AI audit ecosystem beyond the AI Act by including civil society*. AI and Ethics. https://doi.org/10.48550/arXiv.2403.07904

[14] Haryanto, C. Y., Vu, M. H., Nguyen, T. D., Lomempow, E., Nurliana, Y., & Taheri, S. (2024). *SecGenAI: Enhancing security of cloud-based generative AI applications within Australian critical technologies of national interest*. https://doi.org/10.48550/arXiv.2407.01110

[15] Humphreys, D., Koay, A., Desmond, D., & Mealy, E. (2024). *AI hype as a cybersecurity risk: The moral responsibility of implementing generative AI in business*. AI and Ethics, 4(3), 791–804. https://doi.org/10.1007/s43681-024-00443-4

[16] Hussain, N., Austin-Gabriel, B., Ige, A., Adepoju, P., & Afolabi, A. (2023). *Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges*. Open Access Research Journal of Multidisciplinary Studies, 6(1), 51–59. https://doi.org/10.46325/oarjms.2023-6.1.05

[17] Kang, H.-G., Moon, A., & Jeon, S. (2024). *Examining the generative artificial intelligence landscape: Current status and policy strategies*. Asia Pacific Journal of Information Systems, 34(1), 150–190. https://doi.org/10.14329/apjis.2024.34.1.150

[18] Koivisto, T. (2024). *The use of AI in B2B sales and prospecting. https://doi.org/10.54941/ahfe1001456*

[19] Malacaria, S., Grimaldi, M., Greco, M., & De Mauro, A. (2023). *Business talk: Harnessing generative AI with data analytics maturity*. International Journal on Cybernetics & Informatics, 12(7), 1–10. https://doi.org/10.5121/ijci.2023.120701

[20] Mishra, R. K., & Agarwal, R. (2024). *Impact of digital evolution on various facets of computer science and information technology*. Digital Evolution: Advances in Computer Science and Information Technology, 17.

e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[21] Nabil, R. (2024). *Artificial intelligence regulatory sandboxes*. Journal of Law, Economics & Policy, 19, 295.

[22] Osmëni, T., & Ali, M. (2023). *Generative AI: Impactful considerations to responsible data practices in business execution*. 2023 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA). https://doi.org/10.1109/CoNTESA61248.2023.10384863

[23] Popowicz-Pazdej, A. (2023). *The proportionality between trade secret and privacy protection: How to strike the right balance when designing generative AI tools*. Journal of Data Protection & Privacy, 6(2), 153–166. https://doi.org/10.69554/ILGY4235

[24] Prangon, N. F., & Wu, J. (2024). *AI and computing horizons: Cloud and edge in the modern era*. Journal of Sensor and Actuator Networks, 13(4), 44. https://doi.org/10.3390/jsan13040044

[25] Rane, J., Kaya, Ö., Mallick, S. K., & Rane, N. L. (2024). *Generative artificial intelligence in agriculture, education, and business*. Deep Science Publishing. https://doi.org/10.70593/978-81-981271-7-4

[26] Rane, J., Mallick, S. K., Kaya, Ö., & Rane, N. L. (2024). *Future research opportunities for artificial intelligence in Industry 4.0 and 5.0*. Deep Science Publishing. https://doi.org/10.70593/978-81-981271-0-5

[27] Suliman, M., & Leith, D. (2023). *Two models are better than one: Federated learning is not private for Google Gboard next word prediction*. European Symposium on Research in Computer Security (ESORICS). https://doi.org/10.48550/arXiv.2210.16947

[28] Varma, A., Dawkins, C., & Chaudhuri, K. (2023). *Artificial intelligence and people management: A critical assessment through the ethical lens*. Human Resource Management Review, 33(1), 100923. https://doi.org/10.1016/j.hrmr.2022.100923

[29] Wang, X., & Wu, Y. C. (2024). *Balancing innovation and regulation in the age of generative artificial intelligence*. Journal of Information Policy, 14. https://doi.org/10.5325/jinfopoli.14.2024.0012

[30] Wang, Y.-C., Xue, J., Wei, C., & Kuo, C.-C. J. (2023). *An overview on generative AI at scale with edge–cloud computing*. IEEE Open Journal of the Communications Society, 4, 2952–2971. https://doi.org/10.48550/arXiv.2306.17170

[31] Yam, J., & Skorburg, J. A. (2021). *From human resources to human rights: Impact assessments for hiring algorithms*. Ethics and Information Technology, 23(4), 611–623. https://doi.org/10.1007/s10676-021-09599-7

[32] Yang, Y., Zhang, B., Guo, D., Du, H., Xiong, Z., Niyato, D., & Han, Z. (2024). *Generative AI for secure and privacy-preserving mobile crowdsensing*. IEEE Wireless Communications. https://doi.org/10.48550/arXiv.2405.10521

[33] Zhang, D., Xia, B., Liu, Y., Xu, X., Hoang, T., Xing, Z., Staples, M., Lu, Q., & Zhu, L. (2024). *Privacy and copyright protection in generative AI: A lifecycle perspective*. Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering. https://doi.org/10.48550/arXiv.2311.18252