Impacts of Cloud Computing

Anthony DuBois

IT 104-005

February 17, 2026

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on George Mason University Honor Code 2023-2024, and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy website."

Introduction

Cloud computing has become one of the most transformative developments of the modern age of computing. By enabling on-demand access to computing resources such as storage, processing power, and software applications over the internet, cloud computing allows organizations to scale rapidly while reducing infrastructure costs. It's safe to say that organizations across industries are relying more and more on cloud platforms, such as government agencies, financial institutions, healthcare providers, and educational organizations. These, as well as so many other places, have adopted cloud services to streamline operations and enhance digital transformation initiatives.

Despite all of these advantages, cloud computing also presents very complex and evolving security and privacy challenges. Unlike the traditional on-site systems, cloud environments rely heavily on virtualization and multi-tenant architectures that fundamentally alter risk exposure. Sensitive data is often stored across geographically dispersed data centers, shared infrastructure is logically rather than physically separated, and security responsibilities are divided between providers and customers. Researchers demonstrate that these characteristics constantly introduce new vulnerabilities related to data protection, infrastructure security, compliance, and governance. While cloud computing offers undeniable operational benefits, its architectural design and regulatory complexity create ongoing security and privacy risks that require layered technical controls and comprehensive governance frameworks.

Cloud Computing Architecture

Understanding the specifics of cloud security challenges requires examination of the architectural foundations of cloud computing. Cloud services are typically delivered through

three service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Each model abstracts different levels of control from the customer. In IaaS, users manage operating systems and applications but not physical hardware. In PaaS, even the operating system layer is also managed by the provider. In SaaS, users access fully managed applications with minimal direct infrastructure control. This abstraction simplifies deployment but reduces direct oversight.

Gonzalez et al (1), in their quantitative analysis of cloud security research, demonstrate that virtualization and shared infrastructure are central themes in cloud security literature. Virtualization enables multiple virtual machines (VMs) to run on a single physical server through the use of hypervisors. While this design maximizes hardware utilization and reduces costs, it introduces complexity. Elsherbiny et al (6) explain that hypervisors, virtual networks, APIs, and distributed management systems increase the overall attack surface. Each additional layer creates potential vulnerabilities that attackers may exploit.

Public cloud environments commonly use a multi-tenant model, where multiple customers share the same physical infrastructure while relying on separate logistical mechanisms. Unlike traditional data centers where organizations maintain physical separation of systems, cloud isolation depends on software-based controls. If these controls fail, the consequences may extend beyond a single organization.

Furthermore, cloud environments operate under a shared responsibility model. Cloud providers are typically responsible for securing the underlying infrastructure, and the customers are responsible for configuring applications, managing access controls, and protecting their data. Misunderstandings about these responsibilities frequently lead to misconfigurations. Many high-

profile cloud breaches result not from provider failures but from improper customer configurations, like publicly exposed storage buckets. Thus, the architectural structure of cloud computing directly influences its risk profile.

Data Security Challenges

Data protection remains the most prominent concern when it comes to cloud computing. Organizations store highly sensitive data within cloud platforms, like financial records, healthcare data, proprietary research, and government documents. If the contents of these were to be breached, the consequences would be very severe.

Al-Otaibi (2) identifies key data security challenges, including data leakage, improper segregation, data remoteness, and privacy exposure. Data leakage may occur due to weak authentication controls, misconfigured storage systems, or insufficient encryption. Improper segregation can arise when logical isolation mechanisms fail, allowing unintended access between tenants. With how hands-off cloud data is, the more complicated this is. Since data may be stored across multiple geographic regions, organizations may lack precise knowledge of its physical location. This uncertainty complicates compliance with national and international regulations.

Data security in the cloud must be considered across three states: data at rest, data in transit, and data in use. Encryption is commonly implemented to protect data at rest and in transit. But even encryption does not completely eliminate risks if key management practices are weak. Elsherbiny et al. (6) highlight authentication weaknesses, insecure APIs, and inadequate identity and access management (IAM) controls as recurring vulnerabilities. Even strong encryption mechanisms can be undermined if access credentials are compromised.

In order to address privacy concerns while data is being processed, researchers have explored advanced cryptographic approaches. Junior et al. (4) conduct a systematic review of homomorphic encryption techniques in cloud environments. Fully Homomorphic Encryption (FHE) enables computations to be performed directly on encrypted data without decrypting it, thereby preserving confidentiality during processing. In theory, FHE could eliminate a major vulnerability associated with cloud computing, the exposure of data during computation.

However, Junior et al. (4) also identify substantial performance limitations. FHE introduces high computational complexity, increased communication overhead, and significant energy consumption. This directly restricts real-time deployment in large-scale environments. This illustrates a broader theme in cloud security: stronger privacy protections often introduce performance trade-offs. Organizations must balance confidentiality with scalability and efficiency, particularly in environments that prioritize high availability and rapid processing.

Multi-Tenancy and Virtualization Vulnerabilities

Multi-tenancy is a defining characteristic of public cloud computing, yet it introduces distinct vulnerabilities. In a multi-tenant architecture, multiple customers share the same physical hardware, relying on virtualization to maintain logical isolation. While virtualization provides separation at the software level, physical resources such as CPU caches, memory, and storage devices remain shared.

Baig (3) examines security and privacy risks associated with multi-tenant environments, emphasizing cross-tenant vulnerabilities. Hypervisor flaws may allow attackers to escape virtual machine boundaries. Side-channel attacks can exploit shared hardware resources to infer

sensitive information. Wrong identification and improper access management configurations can unintentionally expose sensitive data across tenants.

Gonzalez et al. (1) demonstrate that virtualization security accounts for a significant portion of cloud security research, reflecting its importance. Elsherbiny et al. (6) further identify secure virtualization design as an ongoing research challenge. As cloud infrastructures scale globally, ensuring consistent and reliable isolation becomes increasingly complex.

While shared infrastructure is highly efficient in reducing operational costs and enabling scalability, the same efficiency enlarges the attack surface. With complete physical isolation, there would be the elimination of many cross-tenant risks, but that would also undermine the economic advantages of cloud computing. Therefore, cloud security must focus on strengthening logical isolation while acknowledging architectural trade-offs.

Privacy, Governance, and Adoption Barriers

Technical vulnerabilities are but a part of the cloud security equation. Privacy and governance concerns also influence decision-making, especially within government contexts.

Ukeje et al. (5) analyze information security and privacy challenges affecting government cloud adoption using a systematic PRISMA methodology. After screening hundreds of studies, they conclude that approximately 70% of major adoption barriers are directly linked to security and privacy concerns. Governments manage highly sensitive data related to national security, public health, taxation, and citizen records. The potential consequences of a breach extend far beyond financial loss to political and social instability.

Jurisdictional challenges further complicate adoption. When cloud data is stored across national borders, it may then become subject to the foreign legal systems in which it resides. And conflicts between national regulations can create uncertainty regarding lawful access requests and data sovereignty. Gonzalez et al. (1) note that governance and legal issues receive comparatively less research attention than technical vulnerabilities, suggesting an imbalance in current scholarship.

With the absence of comprehensive frameworks that are specifically tailored for the public sector, cloud implementation continues to be hesitant. Governments require clear accountability structures, transparent provider practices, and robust compliance mechanisms. Without structured governance models, technical safeguards alone are insufficient to build trust.

Future Directions and Remaining Gaps

Despite the ongoing research and technological advancements, there still remains several gaps within cloud security. Limitations associated with advanced encryption techniques must be addressed to enable scalable implementation. Improvements in virtualization isolation mechanisms are necessary to reduce cross-tenant risks.

Additionally, research should expand its focus on governance and compliance frameworks, particularly for government and highly regulated industries. Gonzalez et al. (1) highlight disparities in research emphasis, suggesting the need for more comprehensive approaches.

With the emergence of technology like artificial intelligence, threat detection driven by AI and cloud-native security architectures may improve real-time monitoring capabilities.

However, these technologies introduce new complexities and potential vulnerabilities. As cloud adoption continues to expand globally, the threat landscape will evolve accordingly.

Conclusion

Cloud computing has revolutionized information technology by offering scalable, flexible, and cost-effective computing solutions. However, its architectural reliance on virtualization, distributed storage, and multi-tenancy introduces persistent security and privacy challenges. Data breaches, cross-tenant vulnerabilities, regulatory uncertainty, and governance gaps remain significant obstacles in both sustainability and companies wanting to implement cloud computing.

Research demonstrates that while encryption and infrastructure safeguards provide meaningful protection, performance trade-offs and policy limitations continue to hinder comprehensive security. Effective cloud security requires a layered approach that integrates technical controls, secure virtualization design, identity management systems, advanced cryptographic techniques, and structured governance frameworks. As organizations increasingly depend on cloud services, addressing these challenges will be essential to maintaining trust, protecting sensitive information, and ensuring sustainable technological innovation.

References

(1) **Gonzalez, N., Miers, C., Redígolo, F., et al. (2012).** *A quantitative analysis of current security concerns and solutions for cloud computing.* Journal of Cloud Computing: Advances, Systems and Applications, 1, 11.

https://doi.org/10.1186/2192-113X-1-11.

Annotation:

This article provides a systematic taxonomy of cloud computing security issues and related solutions by analyzing the existing body of research and quantifying attention across different concern categories. It highlights key risks such as virtualization vulnerabilities, legal and governance concerns, and data security, illustrating where research is concentrated and where gaps remain. This study is relevant to the topic because it connects specific cloud characteristics (e.g., multi-tenancy and virtualization) with emerging security challenges and helps identify areas needing further research

(2) **Al-Otaibi, S. Z. (2025).** *Data security challenges and solutions in cloud computing: Critical review.* Communications in Mathematics and Applications, 13(2), Article 2032.

https://doi.org/10.26713/cma.v13i2.2032

Annotation:

This critical review examines the most pressing data security issues in cloud computing—such as data leakage, remoteness, privacy, and segregation—by synthesizing findings from recent studies. It also discusses proposed solutions like encryption and access management, situating them within broader cloud security debates. The source is directly relevant because its focus on data security speaks to one of the core concerns obstructing broader adoption and trust in cloud systems.

(3) **Baig, M. M. A. (2022).** *An Investigation Into Recent Security And Privacy Issues In Cloud Multi-Tenancies.* Webology, 19(2), 3733-3747.

http://mutex.gmu.edu/login?url=https://www.proquest.com/scholarly-journals/investigation-into-recent-security-privacy-issues/docview/2695105228/se-2

Annotation:

This investigation surveys research on security and privacy concerns unique to multi-tenant cloud environments, where shared infrastructure can permit cross-tenant vulnerabilities and complicate isolation. It covers risks posed by virtualization, shared resources, and identity/access misconfigurations, along with efforts to address these. The study connects directly to your topic by explaining *how the cloud's architectural design creates specific security and privacy challenges*.

(4) **Junior, M. A., Appiahene, P., Appiah, O., & Adu, K. (2025)**. *Cloud data privacy protection with homomorphic algorithm: a systematic literature review*. Journal of Cloud Computing, 14(1), 84. https://doi.org/10.1186/s13677-025-00774-5

Annotation:
This systematic literature review analyzes cloud data privacy challenges with a focus on homomorphic encryption (HE) as a solution for secure data processing. Reviewing studies published between 2017 and 2024, the authors evaluate different homomorphic encryption approaches—particularly fully homomorphic encryption (FHE)—and assess their performance based on encryption efficiency, execution time, communication overhead, and energy consumption. Although FHE enables computations on encrypted data without exposing plaintext, the study identifies significant computational complexity and performance limitations that restrict real-time implementation. This source is valuable for a research paper on cloud computing issues because it provides an in-depth evaluation of advanced cryptographic solutions while highlighting the practical limitations that still challenge secure cloud adoption.

(5) **Ukeje, N., Gutierrez, J., & Petrova, K. (2024).** *Information security and privacy challenges of cloud computing for government adoption: a systematic review*. International Journal of Information Security, 23(2), 1459-1475. https://doi.org/10.1007/s10207-023-00797-6

Annotation:
This article examines information security and privacy as primary barriers to government

adoption of cloud computing. Using the PRISMA systematic review methodology, the authors screened 758 studies and analyzed 33 relevant articles to identify key challenges affecting cloud adoption in public-sector institutions. The findings reveal that security and privacy concerns account for approximately 70% of the major gaps hindering adoption, with both factors independently contributing significant barriers. The study also emphasizes the absence of comprehensive security frameworks tailored to government cloud implementation. This source strengthens research on cloud computing issues by providing empirical evidence of adoption challenges and underscoring the need for structured policy and security frameworks in public-sector cloud environments.

(6) **Elsherbiny, S., Eldaydamony, E., Alrahmawy, M., & Reyad, A. E. (2020).** *Secure cloud infrastructure: A survey on issues, current solutions, and open challenges.* Applied Sciences, 11(19), Article 9005. https://pure.port.ac.uk/ws/portalfiles/portal/94821551/Secure_cloud_infrastructure.pdf

Annotation:
This comprehensive survey examines key **security challenges in cloud infrastructure**, including multi-tenancy risks, virtualization vulnerabilities, authentication and access control issues, and data confidentiality concerns. The authors also evaluate existing mitigation strategies—such as encryption techniques, intrusion detection systems, and secure virtualization designs—while identifying open research problems. This source is useful for grounding the paper's discussion in both *current security issues* and *potential technical solutions* within cloud computing environments.

Appendix: ChatGPT Usage in Research Paper

This appendix outlines the use of ChatGPT in creating this research paper. Below are the key prompts and contributions:

Draft Suggestions:

- Prompt: “Can you draft an introduction to a research paper on the challenges found with cloud computing, with an emphasis on data breaches?”
- Response: Provided a draft introduction, which was rewritten for originality
- Prompt: “Can you provide some examples of how quotes to references used should be implemented in body paragraphs?”
- Response: Provided plenty of examples, which were used throughout the paper

Proofreading Assistance:

- Prompt: “Can you refine this paragraph by checking for grammar and punctuation?”
- Response: Identified grammatical errors and suggested rephrased sentences for clarity.

Summary Assistance:

- Prompt: “Can you summarize what the author(s) discussed in the text?”
- Response: Discussed key details and provided an explanation on how it can help the research paper.

All responses from ChatGPT were verified and supplemented with additional research to ensure accuracy and depth. ChatGPT was used as a tool for inspiration and refinement, but the final content reflects original analysis and critical thinking.