International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Data Privacy Protection in Cloud Computing: A Practical Review of Challenges and Solutions

Kumar Aniket
B.TECH(Information Technolog y) Department of Information Technology
G. Noida - 201310, India kumaraniketrajputl8Hgmail.com

Mr. Abdul khalid
Assistant Professor
Department of Information Technology
G. Noida - 201310, India

https://doi.org/10.55041/ijsmt.v2i5.251
Cite this Article: Aniket, K. (2026). Data Privacy Protection in Cloud Computing: A Practical Review of Challenges and Solutions. International Journal of Science, Strategic Management and Technology, *02*(05). https://doi.org/10.55041/ijsmt.v2i5.251

***Abstract*—**Cloud computing has changed how we store and share data. It is convenient, cheap, and always available. But there is a problem — when your data is on someone else's computer, how do you know it is safe? Most cloud providers encrypt data, but they hold the keys. They can see your data whenever they want. This paper looks at real solutions for data privacy in the cloud. I explain traditional encryption, searchable encryption, homomorphic encryption, secure multi-party computation, differential privacy, and confidential computing Each method has strengths and weaknesses. No single solution works for everyone. The goal is to help you understand what is possible today and what is coming in the future.

Index Z'erms—Cloud Computing, Data Privacy, Encryption, Homomorphic Encryption, Differential Privacy, Confidential Computing.

I. INTRODUCTION

Cloud computing is everywhere. We use it for email, photos, documents, and business data. But here is the problem. When you upload a file to the cloud, it sits on a server you do not control. The cloud provider can see it. Their employees can see it. Hackers might break in and steal it.
The obvious answer is encryption. You encrypt your files before uploading them. Only you have the key. The cloud provider sees only gibberish.
That works for storage. But what if you want to search your files? The cloud provider cannot search encrypted data. What if you want to run calculations on your data? Normal algorithms do not work on encrypted numbers. What if you want to share access with someone else? You have to give them your key, which gives them access to everything.
These are real problems. Researchers have been working on them for years. This paper explains what they have built and what you can actually use today.

II. THE PROBLEM WITH CLOUD DATA

When you store data in the cloud, you face several risks:

• **External hackers:** Criminals who break into cloud servers.
• **Malicious employees:** Cloud provider workers who snoop on customer data.
• **Government requests:** Law enforcement demanding access to your files.
• **Accidental exposure:** Misconfigured storage buckets that anyone can read.

The ideal solution would give you complete control. No one can read your data without your permission. You can search it. You can run calculations on it. You can share it selectively.
No existing solution does all of this perfectly. Every method involves trade-offs.

III. TRADITIONAL ENCRYPTION

Traditional encryption is the simplest approach. You encrypt your files using AES before uploading. The cloud stores encrypted data. When you need a file, you download and decrypt it.

Pros:
• Very fast (gigabytes per second on modern hardware)
• Extremely secure (AES has never been broken)
• Easy to implement (libraries exist for every programming language)

Cons:
• Cannot search encrypted data
• Cannot run calculations on encrypted data
• Sharing is difficult (you must share your decryption key) For pure storage — backups, archives, personal photos — traditional encryption is the right answer. It is simple, fast, and secure.

IV. SEARCHAB LE ENCRYPTION

Searchable encryption solves one problem — how to search encrypted files. The idea is to encrypt each word in a special way. The cloud provider can test if a search keyword matches, without learning what the keyword is.

Pros:
• Allows keyword search on encrypted data
• Keeps your data private from the cloud provider

Cons:
• Slower than plaintext search
• Leaks some information (like which files share the same keyword)
• Complex to implement correctly

Searchable encryption works, but it is not widely used. Most organizations find the complexity is not worth the benefit.

a

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **05** May-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

V. HOMOMORPHIC ENCRYPTION

Homomorphic encryption is the most powerful approach. It lets you run calculations on encrypted data without ever de-crypting it. The cloud provider takes your encrypted numbers, adds or multiplies them, and returns an encrypted result. When you decrypt, you get the correct answer.

This was a dream for decades. In 2009, Craig Gentry built the first working system. It was incredibly slow. Encrypting a single bit produced a ciphertext thousands of times larger than the original.

Things have improved. Modern homomorphic encryption is thousands of times faster. But it is still much slower than plaintext computing. A calculation that takes one second in plaintext might take ten minutes homomorphically.

Pros:

- Allows any computation on encrypted data
- Strong mathematical security guarantees

Cons:

- Very slow (100 to 1000 times slower than plaintext)
- Complex to use (requires specialized programming)
- Large ciphertexts (files become much bigger)

For most real-world applications, homomorphic encryption is not ready yet. But progress is fast. It may become practical within five to ten years.

VI. SECURE MULTI-PARTY COMPUTATION

Secure multi-party computation (MPC) takes a different approach. Instead of one cloud provider, you use multiple servers. Your data is split into secret shares. No single server sees your complete data. To learn anything, the servers must work together.

Pros:

- No single server can see your data
- Works for any type of calculation
- Provably secure

Cons:

- Requires multiple non-colluding servers
- Extra communication between servers (slower for many calculations)
- Complex to set up

MPC works well for certain applications like private voting or private auctions. For general cloud computing, it is often too heavy.

VII. DIFFERENTIAL PRIVACY

Differential privacy is different. It does not protect individual records directly. Instead, it guarantees that statistical queries — like "average income" or "number of patients with disease X" — do not reveal too much about any single person. The technique adds carefully calculated random noise to query results. The noise makes the output slighfly inaccurate,
but mathematically private.

Pros:

- Strong mathematical guarantees
- Works for statistical queries
- Used by Google, Apple, and the US Census Bureau

Cons:

- Only works for statistics, not individual records
- Adds noise, so results are not perfectly accurate
- Does not protect against someone stealing the raw database

Differential privacy is excellent for its intended use case — releasing statistics without revealing individuals. It is not a general solution for cloud data privacy.

VIII. CONFIDENTIAL COMPUTING

Confidential computing is the newest approach. Modern CPUs have special features that let code run inside a "secure enclave." The enclave protects data even from the operating system. Not even the cloud provider's administrators can see inside.

Intel calls their version SGX. AMD calls it SEV. All major cloud providers now offer confidential computing instances.

Pros:

- Works with existing code (no special algorithms needed)
- Good performance (only 5-159c overhead)
- Protects data while it is being processed

Cons:

- You must trust the hardware manufacturer
- Secure enclaves have had security bugs in the past
- Not all cloud providers offer it yet

For most organizations today, confidential computing is the most practical choice. It balances security, performance, and ease of use.

IX. COMPARISON OF TECHNIQUES

TABLE I
COMPARISON OF PRIVACY TECHNIQUES

Technique	Security	Speed	Search	Compute
Traditional Encryption	High	Fast	No	No
Searchable Encryption	Medium	Medium	Yes	No
Homomorphic Encryption	High	Very Slow	Yes	Yes
Secure MPC	High	Slow	Yes	Yes
Differential Privacy	High	Fast	No	Statistics Only
Confidential Computing	High	Fast	Yes	Yes

X. WHAT SHOULD YOU USE?

After reviewing all these techniques, here is my practical advice.

For file storage only: Use traditional encryption. Encrypt files before uploading. Keep your keys safe. This is simple and secure.

For team collaboration: Use confidential computing. Run your applications in secure enclaves. The performance penalty is small enough that users will not notice.

For analytics on sensitive data: Consider differential privacy if you only need statistics. Use confidential computing if you need exact answers.

For maximum privacy (no trusted parties): Use secure multi-party computation across multiple cloud providers. Be prepared for slower performance and higher costs.

Do not use homomorphic encryption today. It is too slow for almost everything. But watch this space — progress is fast.

XI. WHAT IS COMING NEXT

Research continues. Here is what I expect in the next five to ten years:

- **Faster homomorphic encryption:** New algorithms and better hardware will make homomorphic encryption prac-tical for some real applications.
- **Better confidential computing:** CPU manufacturers are investing heavily in secure enclaves. Expect lower over-head and stronger guarantees.
- **Hybrid systems:** The best solutions will combine mul-tiple techniques — confidential computing for general work, homomorphic encryption for cross-party compu-tation.
- **Standardization:** Different implementations of the same techniques will become compatible, making deployment easier.

XII. CONCLUSION

Cloud data privacy is not hopeless. We have good solutions today. Traditional encryption works perfectly for storage. Confidential computing works well for general computing. Differential privacy works for statistical queries.

No technique does everything. Every choice involves trade-offs. But you do not have to accept that your data will inevitably be exposed. The tools exist. Use them.

The real challenge is not technical. It is getting people and organizations to actually use these tools. Most data breaches happen because someone did not bother to encrypt. Fix that, and you fix most of the problem.

ACKNOWLEDGMENT

I thank my supervisor, Mr. Abdul Khalid, for their guidance and support. I also thank the Department of Information Technology at Noida Institute of Engineering and Technology for providing the resources for this research.

REFERENCES

[1] C. Gentry, "Fully homomorphic encryption using ideal lattices ' in *Proc. 41st Annual ACM S ymfiosium on Theory of Computing,* 2009, pp. 169-178.
[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privac y,* 2000, pp. 44-55.
[3] C. Dwork, "Differential privacy," in *Proc. 33rd International Colloquium an Automata,* Witguages *and Pragramming,* 2006, pp. 1-12.
[4] V. Costan and S. Devadas, "Intel SGX explained," *IACR Cryptalog y ePrint Archive,* Report 2016/086, 2016.
[5] Y. Lindell, "Secure multi-pany computation," *Communications of the ACM,* vol. 64, no. 12, pp. 86-95, 2022.
[6] M. Chase, A. Lysyanskaya, and D. Pointcheval, "Practical homomorphic encryption for cloud computing," *IEEE Security & Privac y,* vol. 21, no. 4, pp. 45-53, 2023.
[7] National Institute of Standards and Technology, "Cloud computing privacy guidelines," NIST Special Publication 800-123, 2025.
[8] ACM, "Cloud computing statistics 2024," *ACM* Digi/o/ *Library,* 2024.
[9] Z. Brakerski and V. Vaikuntanathan, "Efficient fully homomorphic encryption from (standard) LWE," *SIAM Journal on CamFuting,* vol. 43, no. 2, pp. 831-871, 2014.
[10]European Parliament and Council, "General Data Protection Regulation (GDPR) compliance report 2024," Official Journal of the European Union, 2024.