Page 5848 - 5858

DOI: *https://doij.org/10.10000/IJLMH.1110653*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Cloud Data Security with Enhanced Cryptography

SEEMA DEVI[1] AND DR. KALPNA MIDHA[2]

ABSTRACT

Cloud computing is the outgrowth of ongoing developments in Internet grounded services and the technology assiduity. All pall services need a high- performance pall storehouse room in order to satisfy client demands. still, cloud surroundings' participated residency and natural distributed nature give serious security pitfalls, especially with regard to data vacuity, confidentiality, and integrity. Even though they're abecedarian, traditional cryptographic ways constantly fail to handle the particular complexity of cloud data. In the environment of cloud surroundings, we will explore the fundamentals, uses, and difficulties of bettered cryptographic results similar post-quantum cryptography block chain- grounded security, homomorphic encryption, and trait- grounded encryption. The thing of the study is to present a thorough analysis of the state- of- the- art and implicit future paths in cloud data security using advanced cryptographic ways. We will delve into the principles, applications, and challenges of enhanced cryptographic solutions such as Homomorphic Encryption, Attribute-Based Encryption, Block chain-based security, and Post-Quantum Cryptography in the context of cloud environments. The paper aims to provide a comprehensive overview of the current state-of-the-art and future directions in securing cloud data with sophisticated cryptographic mechanisms.

Keywords: *Cloud Security, Data Encryption, Homomorphic Encryption, Attribute-Based Encryption, Blockchain, Post-Quantum Cryptography, Data Confidentiality, Data Integrity, Access Control.*

I. INTRODUCTION

The paradigm shift towards cloud computing has brought about substantial changes in data processing, administration, and storage. Cloud service providers (CSPs) are increasingly being relied upon by businesses to store their critical apps and sensitive data. This provides a lot of benefits, but it also opens up a new attack surface and security vulnerabilities. Data breaches, unauthorized access, and compliance issues remain the top concerns for cloud adopters. The foundation of data security is cryptography, the science of safe communication against hackers.

[1] Author is a Phd Scholar at Shri khushal Das University, Hanumangarh, India.
[2] Author is an Assistant Professor at Shri khushal Das University, Hanumangarh, India

However, simple "encrypt-at-rest" or "encrypt-in-transit" solutions are often insufficient due to the dynamic and multi-tenant nature of cloud environments. This study argues that better cryptographic methods that offer stronger guarantees than mere confidentiality are required to truly secure data in the cloud.

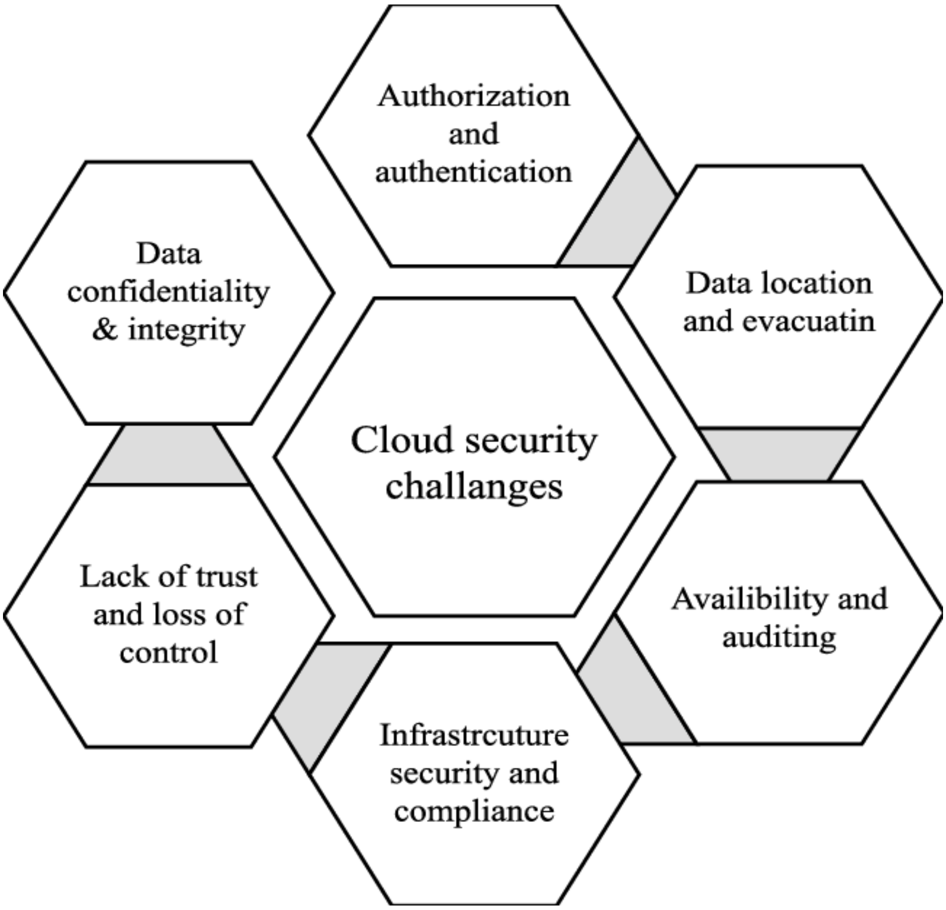
Authorization and authentication
Data location and evacuatin
Data confidentiality & integrity
Cloud security challanges
Lack of trust and loss of control
Availibility and auditing
Infrastrcuture security and compliance

Fig 1. Challenges in Cloud Data Security

II. CHALLENGES IN CLOUD DATA SECURITY

Securing data in the cloud is complex due to several factors:

i. **Data Encryption:** Even though encryption is commonly used for data in transit, breaches can still happen when the data is at rest.To avoid unwanted access, it is essential to make sure that data stored in the cloud is appropriately encrypted.

ii. **Insider Threats**: Workers or service providers who have access to cloud systems may abuse their authority, resulting in data breaches whether on purpose or accidentally. To lessen these risks, proper monitoring and access controls are crucial.

iii. **Data Sovereignty and Location**: Compliance and security depend on knowing where your data is physically located. Concerns around data sovereignty and access may arise because some cloud providers store data in several different places throughout the world.

iv. **Loss of Control**: •Cloud services provide third-party access to your data and apps, leading to a loss of control. Issues with data availability, ownership, and access may arise as a result of this lack of direct control.

v. **Forensics and Incident Response**: Examining security events in a cloud setting can be challenging.

vi. **Data Backup and Recovery**: It can be dangerous to rely on cloud services for these tasks. To guarantee data availability in the event of outages or data loss, a strong backup and recovery plan must be in place.

vii. **Shared Responsibility Model:** While CSPs are responsible for the security *of* the cloud infrastructure, users are responsible for security *in* the cloud, including data, applications, and access management. This can lead to confusion and misconfigurations.

viii. **Loss of Control:** Organizations relinquish direct physical control over their data when moving to the cloud, relying on the CSP's security measures.

ix. **Multi-Tenancy:** Data from multiple clients often resides on the same physical infrastructure, raising concerns about data isolation and potential leakage.

x. **Data in Various States**: Information must be protected while it is being used (during computation), in transit (during network communication), and at rest (during storage)**.**

xi. **Compliance and Regulations:** Meeting stringent regulatory requirements (e.g., GDPR, HIPAA, PCI DSS) for data privacy and security is a significant challenge in a global cloud environment.

xii. **Key Management:** Securely managing cryptographic keys in a cloud environment, especially across different services and regions, is a critical and often underestimated challenge.

xiii. **Evolving Threats:** The landscape of cyber threats is constantly evolving, with new attack vectors emerging that can target cloud vulnerabilities.

III. Enhanced cryptographic methods for protecting cloud data

CRYPTOGRAPHY

The human language is the language that people use to communicate with one another. Plain text is its form. Clear text is another name for it. Because they are not codified, communications expressed in plain language may be understood by anybody. Hence, to guarantee message security, it has to be formalized. Once encoded, the communication will be impenetrable to everyone without authorization. Those capable of deciphering the code will not be able to view it. Cryptography is now nearly synonymous with encryption. Encryption is a method of transforming readable data into an unintelligible format. One process is encryption, while the other is decryption. Historically, a cipher has been thought of as a pair of algorithms. Its primary function is to encrypt text. The algorithm has carefully observed the cipher's functioning. Additionally, it uses a "key" to keep tabs on each instance. The ordered list of components is a cryptosystem. A limited set of possible plaintexts and ciphertexts make it up.The finite feasible keys are also part of the cryptosystem. There are methods for both encryption and decryption that operate inside it as well. These are touching every key. The Keys play a crucial function. It is easy to break ciphers that do not use changeable keys. All that's needed to decipher it is the details of the encryption that was utilized. Direct use of ciphers for encryption and decoding was commonplace in bygone days. Extra procedures, such as authentication or integrity checks, were missing.

To address the aforementioned challenges, several advanced cryptographic techniques are being researched and developed:

Homomorphic Encryption (HE) Homomorphic encoding is a type of cryptography that permits data to be transformed while being made encrypted. Homomorphic encryption allows calculations on encrypted statistics to be performed concurrently, as opposed to regular encryption, which requires statistics to be decrypted for each meaningful operation.This preserves privacy by allowing a CSP to process a client's encrypted data without ever seeing the plaintext. It has a wide range of capabilities, including collaborative machine mastering, privacy-preserving records analysis, and reliable outsourcing. Even if it encounters challenging circumstances, such limitations are increasingly being lessened by continued research and development. In a time where records sharing and analysis are commonplace, homomorphic encryption offers the promise of privacy as we continue to navigate the statistics-driven world.

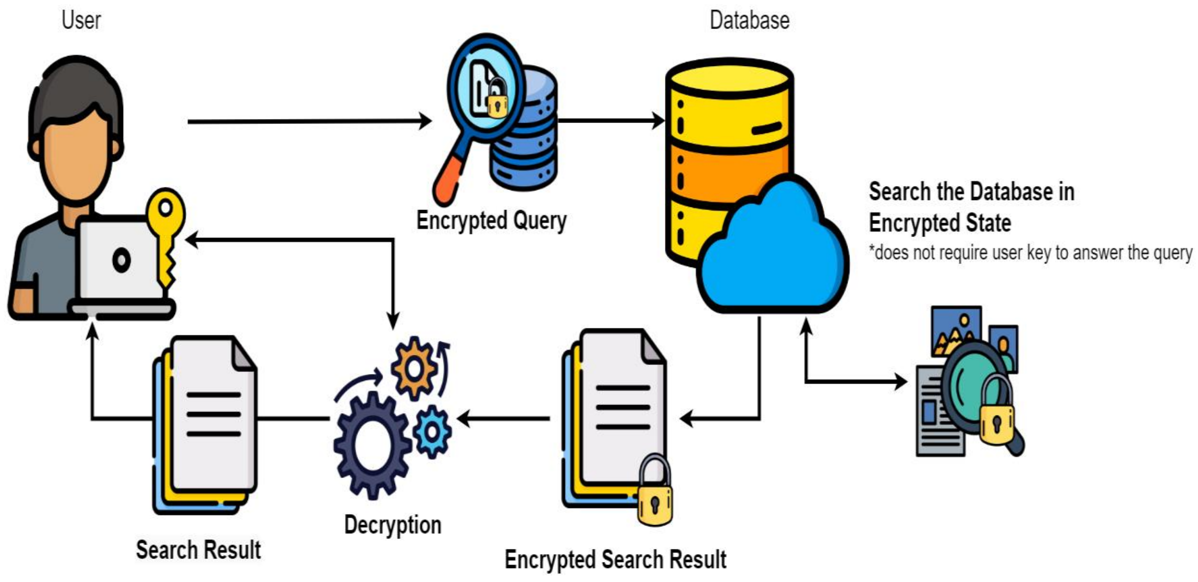

Fig 2. Homomorphic Encryption

HE Types: Partially Homomorphic Encryption (PHE): Allows for an infinite number of operations of a single kind, such as multiplication or addition. A small number of distinct procedures are supported by somewhat homomorphic encryption (HE).

i. **Cloud-based AI/ML:** Training AI models on sensitive medical or financial data without exposing the raw data.

ii. **Challenges:** High computational overhead, complexity of implementation, and large ciphertext expansion. Ongoing research focuses on improving efficiency.

iii. **Privacy-Preserving Data Analytics:** Cloud providers can perform statistical analysis, machine learning model training, or queries on encrypted datasets without compromising data privacy.

iv. **Secure Outsourced Computation:** Clients can outsource complex computations to the cloud, knowing their sensitive input data remains encrypted throughout the process.

Table 1. Comparative table of different type of Encryption

Feature	Encryption Using Asymmetric Public-Key Cryptography	Another name for symmetric encryption is secret-key or private-key cryptography.
Number of Keys	Both encryption and decoding may be accomplished with a single key.	A private key for decryption and a public key for encryption are arithmetically connected.

Key Sharing	The single, secret key must be securely shared between all communicating parties.	While the private key must be trusted by its owner, the public key can be freely distributed.
Speed/Efficiency	Generally much faster and more efficient, especially for large amounts of data.	Considerably more computationally demanding and slower, particularly when dealing with huge data.
Primary Use Cases	Encrypting large amounts of data (data at rest, full disk encryption, VPNs, Wi-Fi, bulk data transfer).	Secure key exchange for symmetric keys (TLS/SSL handshakes), digital signatures, authentication, and email encryption.
Security Challenge	Strongly distribution the distinct secret key is the leading challenge. If compromised, all data encrypted with it is at risk.	Ensuring the private key remains private. Protection against quantum attacks is an emerging concern.
Data Size Suitability	Ideal for encrypting large datasets.	More suitable for smaller data (e.g., session keys, hashes for signatures).

Attribute-Based Encryption (ABE) ABE is a type of public-key encryption that enables fine-grained access control over encrypted data.Instead of encrypting data for specific users, ABE encrypts data based on attributes (e.g., "Department: HR," "Role: Manager," "Location: Delhi").Decryption is only possible if a user's attributes match the policy defined in the ciphertext (Ciphertext-Policy ABE - CP-ABE) or if their key holds an access structure that satisfies the ciphertext's attributes (Key-Policy ABE - KP-ABE).

Blockchain for Cloud Data Security

The way businesses store, retrieve, and handle data has been completely transformed by cloud computing. Data breaches, illegal access, and data integrity loss, however, continue to be issues. Because blockchain technology is decentralized, transparent, and impenetrable, it presents a viable way to improve cloud data security. Blockchain, a distributed ledger technology, offers inherent security properties like immutability, transparency, and decentralization, which can significantly enhance cloud data security.

i. **Safe Storage of Data:** By offering decentralized storage, blockchain lowers the possibility of data breaches and single-point failures.

ii. Unauthorized access is very difficult because data is encrypted and dispersed among nodes.

iii. **Verification of Data Integrity** P: On the blockchain, no transaction can be undone.Users of the cloud do not have to trust the cloud provider to confirm that data they have stored has not been changed.

iv. **Identity and Access Management (IAM)** : that is decentralized Blockchain authentication relies on cryptographic keys. By controlling permissions, smart contracts make sure that only people with permission can view or alter data.

v. **Safe Exchange of Data** :Multiple parties can share data in a transparent and verifiable manner thanks to blockchain technology. particularly helpful for businesses working together across organizations and regions.

vi. **Improved Compliance and Audit Trails:** Blockchain keeps an unchangeable record of every alteration and access. ensures accountability and transparency, which aids in meeting regulatory obligations (such as GDPR and HIPAA).

vii. **Decentralized Access Control and Key Management:**Blockchain can manage and distribute cryptographic keys in a decentralized and tamper-proof manner, reducing reliance on a single central authority.

viii. **Data Integrity and Auditability:** Immutability of blockchain ensures that data logs, access records, and change histories cannot be altered, providing a reliable audit trail for compliance.

ix. **Secure Data Sharing and Provenance:** Blockchain can track the origin and movement of data across different cloud services and organizations, enhancing data governance and preventing unauthorized modifications.

x. **Decentralized Cloud Storage:** Emerging concepts of decentralized cloud storage leveraging blockchain can distribute data across a network of nodes, reducing single points of failure and enhancing resilience.

Post-Quantum Cryptography (PQC) The advent of quantum computing poses a significant threat to many currently used public-key cryptographic algorithms (e.g., RSA, ECC) which underpin cloud security.PQC focuses on developing new cryptographic algorithms that are secure against attacks by future quantum computers. Data encrypted today needs to remain secure for decades. Data that has already been intercepted might be decrypted by a quantum computer. PQC will be crucial for secure authentication and digital signatures in a post-quantum world. Research is focused on various mathematical problems believed to be hard for quantum computers, including lattice-based cryptography, multivariate cryptography, hash-based cryptography, and code-based cryptography. Standardization (NIST is leading efforts), performance overhead compared to current algorithms, and the complex transition from classical to quantum-resistant cryptography in existing cloud infrastructures.

IV. Hybrid approaches and future directions

The most robust cloud data security solutions will likely involve hybrid approaches, combining the strengths of different enhanced cryptographic techniques. For instance, ABE could be used for access control, while HE handles secure computations on sensitive data, and a blockchain logs access and key management. PQC will be integrated to ensure long-term security against quantum threats.

i. **Secure Multi-Party Computation (SMC):** This has strong implications for collaborative data analysis in the cloud. Allows several parties to compute a function over their private inputs without disclosing them to one another.

ii. **Trusted Execution Environments (TEEs):** Hardware-based solutions that create isolated environments for secure code execution and data processing, offering another layer of protection.Cryptography can be integrated with TEEs to further strengthen security.

iii. **Verifiable Computation:** Enables a client to outsource computation to the cloud and then efficiently verify that the computation was performed correctly without re-executing it.

V. Conclusion

Cloud data security is a dynamic and critical field. While traditional encryption remains fundamental, the unique challenges of cloud environments necessitate the adoption of enhanced cryptographic techniques. Homomorphic Encryption offers unprecedented privacy for computations on encrypted data, Attribute-Based Encryption provides fine-grained access control, and Blockchain introduces decentralization and immutability for enhanced data integrity and auditability. Furthermore, the imperative of preparing for the quantum era makes Post-Quantum Cryptography a crucial area of research and deployment.The clever integration of these cutting-edge cryptographic methods will create private, reliable, and future-proof cloud environments, Which is the key to the future of cloud data security. Unlocking the full potential of cloud computing while protecting sensitive data will require ongoing research and development in these areas, industry cooperation, and standardization initiatives.

*****

VI. References

1. Mostafa, A.M.; Ezz, M.;Elbashir, M.K.; Alruily, M.; Hamouda,E.; Alsarhani, M.; Said, W.Strengthening Cloud Security: AnInnovative Multi-Factor Multi-LayerAuthentication Framework for CloudUser Authentication. Appl. Sci. 2023,13, 10871.

2. Tabassum, Nadia & Naeem, Humaria & Batool, Asma. (2023). The Data Security and multi-cloud Privacy concerns: Nadia Tabassum, Humaria Naeem and Asma Batool. International Journal for Electronic Crime Investigation. 7. 49-58. 10.54692/ijeci.2023.0701128.

3. S. Subasree and N. K. Sakthivel, "Design of a new security protocol using hybrid cryptography algorithms," International Journal of Research and Reviews in Applied Sciences, vol. 2, no. 2, Feb. 2010.

4. S. M. Seth, R. Mishra, "Comparative analysis of encryption algorithms for data communication," International Journal of Scientific Engineering and Applied Science, vol. 2, no. 2, pp. 495-498, 2016.

5. E. Ramaraj, S. Karthikeyan, M. A. Hemalatha, "A design of security protocol using hybrid encryption technique(AES - Rijndael and RSA)," International Journal of The Computer, the Internet and Management, vol. 17. no. 1, pp. 78-86, 2009.

6. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102-114, Aug. 2002.

7. Aluvalu, Rajanikanth & Viswanadhula, Uma Maheswari & Chennam, Krishnakeerthi & Shitharth,. (2021). Data Security in Cloud Computing Using Abe-Based Access Control. 10.1007/978-981-16-0386-0_4.

8. Bhushan, Kriti & Gupta, Brij B. (2015). Security Challenges in Cloud Computing: State-of-art. International Journal of Big Data Intelligence. 4. 10.1504/IJBDI.2017.10002912.

9. Coppolino, L., D'Antonio, S., Mazzeo, G. and Romano, L., 2017. Cloud security: Emerging threats and current solutions. Computers & Electrical Engineering, 59, pp.126-140.

10. Yan, Z., Deng, R.H. and Varadharajan, V., 2017. Cryptography and data security in cloud computing.

11. Singh, Santosh. (2023). Blockchain Based Model for Cloud Computing Security. 12. 7-19. 10.17148/IJARCCE.2023.12802.

*****