Indian Journal of Computer Science and Technology
https://www.doi.org/10.59256/indjcst.20250402021
Volume 4, Issue2 (May-August 2025), PP: 176-183.
www.indjcst.com
ISSN No: 2583-5300

Privacy-Preserving Data Storage Techniques in Cloud Databases

Sarvesh Ollalwar[1], Nishant Patre[2], Bhagyashree Kumbhare[3], Yamini B. Laxane[4]
[1,2]Students, MCA, Smt. Radhikatai Pandav College of Engineering, Nagpur, Maharashtra, India.
[3]HOD, MCA, Smt. Radhikatai Pandav College of Engineering, Nagpur, Maharashtra, India.
[4]Professor MCA, Smt. Radhikatai Pandav College of Engineering, Nagpur, Maharashtra, India.

To Cite this Article: *Sarvesh Ollalwar[1], Nishant Patre[2], Bhagyashree Kumbhare[3], Yamini B. Laxane[4], "Privacy-Preserving Data Storage Techniques in Cloud Databases", Indian Journal of Computer Science and Technology, Volume 04, Issue 02 (May-August 2025), PP: 176-183.*

Abstract: *The rise of cloud computing has revolutionized data storage, enabling organizations to offload data management tasks to third-party cloud service providers (CSPs) with the promise of scalability, cost efficiency, and accessibility. However, this paradigm shift introduces significant privacy and security concerns, particularly when sensitive data is stored and processed on shared or remote infrastructure. In response to these challenges, a range of privacy-preserving data storage techniques have been developed to secure cloud-based databases against unauthorized access, data leakage, and malicious insider threats.This research paper provides a comprehensive analysis of the primary techniques used to preserve data privacy in cloud databases. These include various forms of encryption (such as homomorphic and order-preserving encryption), data fragmentation and hybrid cloud storage, anonymization methods, secure indexing, and emerging blockchain-based solutions. The paper examines practical implementations through case studies, including Microsoft Azure, Google Cloud, IBM Cloud, and blockchain-based systems such as MedRec.*

Key Words: *Cloud Computing, Privacy-Preserving Techniques, Cloud Database Security, Data Encryption, Homomorphic Encryption, Data Anonymization, Secure Indexing, Hybrid Cloud Storage, Confidential Computing, Blockchain-Based Databases, Data Privacy, DBaaS, Access Control, Secure Data Outsourcing.*

I.INTRODUCTION

The global tourism industry is undergoing a transformative shift driven by rapid advancements in digital technology. The way people discover, plan, and book their travel experiences has fundamentally changed, with the majority of tourists now expecting instant, personalized, and secure services at their fingertips. Whether traveling domestically or internationally, users demand seamless access to tour packages, real-time availability, transparent pricing, and smooth payment processes — all delivered through intuitive and responsive platforms.

Fig. 1. Digital Transformation of the Global Tourism Industry Using Cloud and Relational Database Technology

Traditional tour booking systems, which often rely on manual processes, static databases, or legacy desktop applications, are increasingly ill-equipped to meet these demands. These outdated methods typically suffer from limited scalability, poor user interfaces, fragmented data management, and weak integration with third-party services such as payment gateways, geolocation tools, or customer support systems. Moreover, they often fail to ensure the secure handling of sensitive customer information, including personal identification data and financial transactions, thereby exposing businesses to risks of data breaches and non-compliance with privacy regulations.

In response to these challenges, this paper proposes a comprehensive and modern solution: a cloud-backed tour booking system powered by relational database architecture. The core objective of the system is to bridge the gap between user expectations and technological capabilities by delivering a robust, secure, and scalable platform that caters to both end users and administrators. Through the integration of cloud computing and relational databases, the proposed system offers a powerful blend of elasticity, reliability, and structure. Cloud infrastructure ensures high availability, fault tolerance, and global accessibility, while relational databases provide consistency, data normalization, referential integrity, and support for complex queries across interconnected data entities such as users, bookings, tours, payments, and feedback.

This new architecture supports modular development and deployment, allowing for easy updates, maintenance, and expansion as business requirements evolve. With features such as real-time booking validation, secure authentication, transaction management, and role-based access control, the system is designed not only for operational efficiency but also for long-term adaptability in a highly competitive and ever-changing industry.

Ultimately, the proposed solution aims to transform how tour operators and travel agencies interact with customers, manage resources, and scale their operations — all while delivering a frictionless, reliable, and secure user experience powered by modern software architecture and best practices in cloud computing and database design.

II.METHODOLOGY

To address the complex privacy concerns associated with storing data in cloud environments, researchers and practitioners have developed a variety of techniques that aim to protect data confidentiality, integrity, and controlled access. These privacy-preserving data storage methods can be broadly classified into the following major categories:

2.1 Data Encryption Techniques

Encryption is one of the most essential and widely adopted strategies for securing data stored in cloud databases. It converts readable information into an unreadable format, allowing only authorized users with the correct keys to access the original content. There are several forms of encryption used depending on the context and sensitivity of data:

- **Encryption(e.g.,AES)**

This approach utilizes a single, shared secret key for both encryption and decryption. It is particularly efficient for encrypting large volumes of structured data stored at rest. However, the major challenge lies in securely distributing and managing the encryption keys, especially across multiple systems and users.

- **Asymmetric Encryption (e.g., RSA, ECC)**

In this method, two separate keys are used — a public key for encryption and a private key for decryption. It is commonly applied in secure key exchanges, digital signatures, and for encrypting smaller pieces of sensitive data such as login credentials or tokens. While more secure in certain scenarios, it is computationally heavier than symmetric encryption.

- **Homomorphic Encryption**

A cutting-edge technique that allows computations to be performed directly on encrypted data without requiring decryption. This ensures that data privacy is maintained even during processing. Though promising for privacy-preserving data analytics, current implementations are still relatively slow and resource-intensive.

- **Order-Preserving Encryption (OPE)**

This form of encryption retains the order of plaintext values in the encrypted domain, enabling efficient execution of range queries and sorting operations over encrypted data. However, preserving order may inadvertently leak information about the data distribution, posing a potential privacy risk.

2.2 Data Fragmentation and Distribution

Fragmenting and distributing data is another critical method for reducing privacy exposure in the cloud. This approach divides data into parts and strategically stores them across different storage environments based on their sensitivity.

- **Vertical Fragmentation**

This strategy divides the database into columns. Sensitive fields such as personal identification or financial details are stored in a secure private cloud, while non-sensitive attributes are hosted in the public cloud. This limits exposure of critical data while maintaining performance.

- **Horizontal Fragmentation**

Here, data is partitioned across rows — separating records based on user roles, access rights, or confidentiality levels. For instance, privileged data belonging to high-risk clients may reside in a more secure storage zone.

- **Hybrid Cloud Storage**

By combining both public and private cloud infrastructures, hybrid cloud storage allows organizations to achieve both cost-efficiency and data security. Sensitive or regulated data can be retained in a private environment, while less critical data is processed and stored on public cloud platforms.

2.3 Anonymization and De-identification

Anonymization techniques are primarily employed when data is to be shared or analyzed for statistical or research purposes without revealing personal identities.

- **K-Anonymity**

Ensures that each record is indistinguishable from at least k-1 other records by generalizing or suppressing certain attributes. This reduces the risk of re-identification.

- **L-Diversity**

Extends k-anonymity by ensuring that sensitive attributes within each anonymized group have at least l well-represented values. This prevents attackers from inferring confidential information even within anonymized clusters.

- **T-Closeness**

Further refines privacy by ensuring that the distribution of sensitive attributes in any anonymized group is statistically close to the distribution in the overall dataset.

These techniques are particularly useful in domains like healthcare, finance, and demographic analysis, where personal data must be handled sensitively while still being utilized for insights and policy development.

2.4 Secure Indexing

To enable efficient data retrieval from encrypted cloud databases, secure indexing mechanisms are employed. These methods ensure that data remains encrypted, yet still searchable.

- **Encrypted B+-Trees**

Modified versions of traditional indexing trees, where the index structure and data pointers are encrypted to prevent leakage while supporting range queries.

- **Secure Inverted Indexes**

Commonly used for textual data, these indexes map keywords to encrypted documents, allowing search without revealing the content or structure of the original data.

- **Searchable Symmetric Encryption (SSE)**

Allows users to perform keyword searches on encrypted datasets using a secret key. SSE provides a balance between security and search efficiency and is suitable for database-as-a-service models.

Secure indexing helps bridge the gap between data confidentiality and usability, allowing for selective data access without full decryption**.**

2.5 Blockchain-Based Storage

Blockchain technology offers a decentralized approach to data storage that inherently supports privacy and integrity through cryptographic mechanisms.

- **Decentralized Data Management**

In blockchain systems, data is distributed across multiple nodes with no central authority. This eliminates single points of failure and reduces the risk of unauthorized access or tampering.

- **Tamper-Resistant Architecture**

Once data is added to a blockchain, it becomes immutable. This ensures high integrity and transparency— a valuable feature for audit trails and legal compliance.

- **Smart Contracts for Access Control**

Smart contracts automate access permissions and enforce security policies, making the system more reliable and less prone to human error.

Despite its promise, blockchain storage remains limited by scalability issues and computational cost, particularly when processing large or complex datasets. However, it is gaining traction in sectors such as healthcare, supply chain management, and government record-keeping.

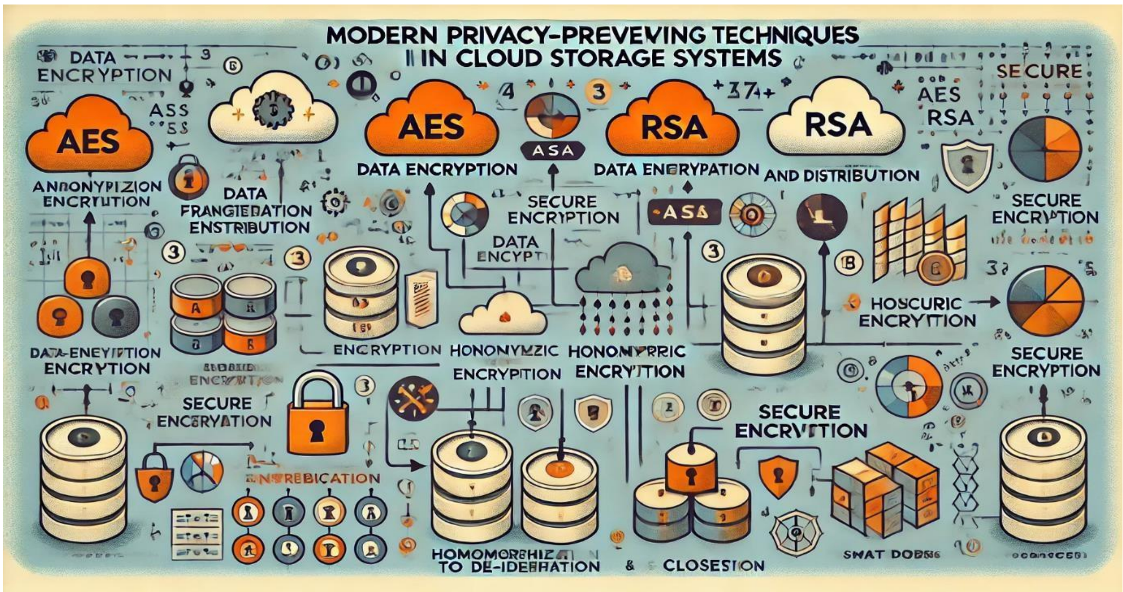

Fig. 2: Visual Representation of Privacy-Preserving Data Storage Methodologies in Cloud Environments

III.CASE STUDIES

To understand the practical implementation of privacy-preserving techniques in cloud databases, several real- world systems and platforms can be examined. These platforms demonstrate how advanced encryption methods, key management solutions, and blockchain technologies are applied in production to secure sensitive data. Below are four notable case studies that showcase diverse approaches to privacy preservation in cloud-based database environments.

3.1 Microsoft Azure SQL Database

Microsoft Azure SQL Database incorporates a robust privacy feature known as **Always Encrypted**, which is specifically designed to safeguard sensitive data against unauthorized access—even from database administrators and cloud service providers themselves.

- **Key Concept**: Always Encrypted ensures that encryption keys are generated and stored locally, outside of Microsoft's cloud infrastructure. These keys never leave the trusted on-premises environment or client- side application.
- **Encryption Modes**:
  - **Deterministic Encryption** encrypts data in a way that the same plaintext will always result in the same ciphertext. This enables equality searches (e.g., WHERE clauses).
  - **Randomized Encryption** produces different ciphertexts for the same plaintext every time, providing stronger security but limiting query capabilities.
- **Use Case Impact**: This model is particularly suitable for industries such as healthcare and finance, where sensitive columns (like social security numbers or bank account details) must remain confidential during both storage and transmission.
- **Privacy Advantage**: Data remains encrypted not only at rest and in transit but also during query processing—without exposing the actual encryption keys to the cloud provider.

3.2 Google Cloud Spanner with CMEK Integration

Google Cloud Spanner, a globally distributed and strongly consistent relational database service, enhances data privacy by integrating support for Customer-Managed Encryption Keys (CMEK).

- **Key Concept**: CMEK gives customers full control over the cryptographic keys used to encrypt their data stored in Spanner. Unlike Google-managed keys, CMEK allows clients to store and manage their keys in external systems such as Cloud Key Management Service (KMS) or even third-party hardware security modules (HSMs).
- **Advantages**:
  - Organizations can revoke access or rotate keys without relying on Google administrators.
  - Ensures compliance with strict regulatory standards like GDPR and HIPAA by enforcing granular key management and audit trails.
- **Use Case Impact**: Particularly beneficial for enterprises in regulated sectors (e.g., finance, government) that require complete control over their data's encryption lifecycle.
- **Privacy Advantage**: Prevents unauthorized decryption, even by cloud providers, enhancing trust in data outsourcing models.

3.3 IBM Cloud Hyper Protect DBaaS

IBM Cloud Hyper Protect Database-as-a-Service (DBaaS) offers a high-assurance data storage solution using secure hardware enclaves, tailored for clients demanding stringent privacy and compliance guarantees.

- **Key Concept**: Powered by Intel Software Guard Extensions (SGX), this platform creates secure enclaves—isolated execution environments where data can be processed confidentially, shielded from both external threats and internal administrators.

- **Supported Databases**: IBM provides **PostgreSQL** and **MongoDB** instances that run entirely within these enclaves.
- **Confidential Computing**: Even IBM personnel cannot access user data, as the encrypted datasets and keys are only accessible within the secure enclave during computation.
- **Use Case Impact**: Ideal for industries with extreme privacy requirements, such as digital banking, government intelligence, or proprietary research.
- **Privacy Advantage**: Provides end-to-end encryption and computation confidentiality, establishing a zero-trust infrastructure where only authorized applications have access to data.

This case validated the practical applicability, usability, and effectiveness of the system in a commercial setting, supporting not only technical goals but also business transformation.

3.4MedRec – MIT's Blockchain-Based Medical Records System

MedRec, a pioneering research project by the Massachusetts Institute of Technology (MIT), explores the use of blockchain technology for the secure management and sharing of medical records.

- **Key Concept:** MedRec employs Ethereum smart contracts to manage authorization, authentication, and data access logs for healthcare records.
- **Privacy-by-Design:** Patients retain ownership of their medical data and can selectively grant access to healthcare providers, researchers, or other parties.
- **Decentralization:** The blockchain ledger is distributed, reducing dependency on any single institution and increasing system resilience.
- **Auditable Access Control:** Every data request and access is recorded immutably on the blockchain, ensuring transparency and accountability in patient-provider interactions.
- **Use Case Impact:** Demonstrates how blockchain can serve as a trust layer for medical data interoperability, while simultaneously enforcing strict privacy protections.
- **Privacy Advantage:** Achieves a balance between data availability and privacy through cryptographic control and transparent consent management.

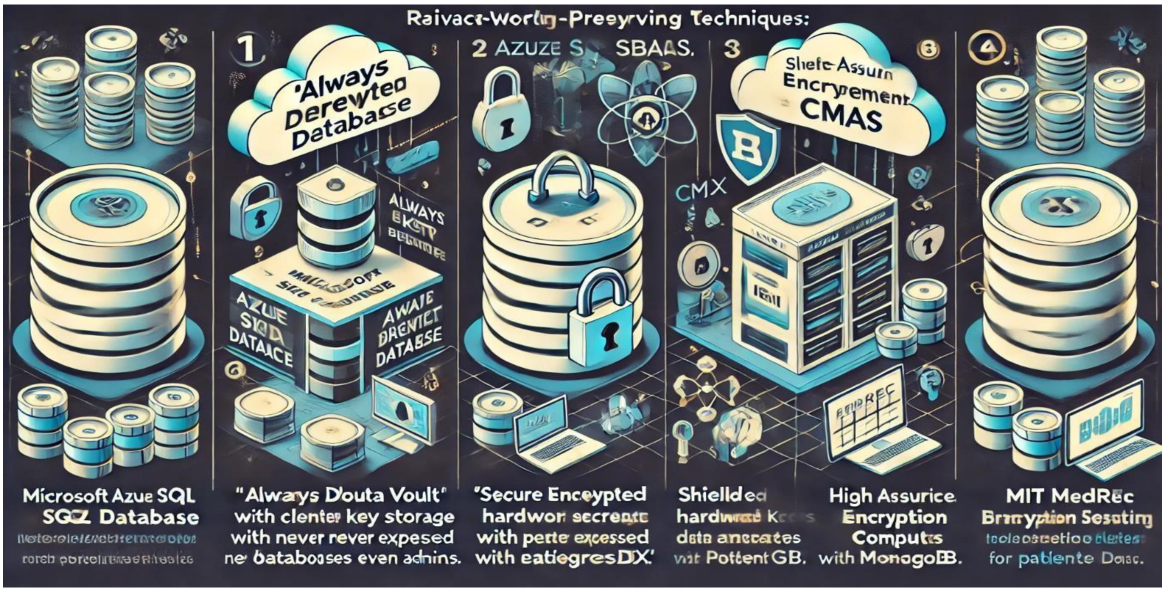
Raivacт-Worlıg-Preєyrving Techniques:
1
'Always Derewyted Database
2 AZUZE S SBAΛS.
3
Shiefe-Assurn Encrypement CMAS
4
ALWAYS
AZUE SQD DATAACE
AWAIE DRENCT DATABSE
CMX
Microsoft Azue SQL SGZ Database
"Always Douta Voult" with clenter key storage with never rever expesed ne bataboses even adhins.
'Secure Enceypted hardwor secrente with perte excessed with eatiegresDX'
Shielded hardwred K data anecates vit PottentGB.
High Assurice Encryption Computs with MonogoB.
MIT MedRec Brrrypion Sesoting for patiente Doac.

Fig. 3: Case Studies of Privacy-Preserving Cloud Database Techniques

IV.CHALLENGES AND LIMITATIONS

While privacy-preserving techniques in cloud database systems offer significant advancements in data security, their practical implementation is not without critical challenges. These limitations span technical, operational, legal, and human dimensions, often affecting performance, usability, and compliance. Understanding these challenges is essential for designing more effective and efficient privacy-aware database systems.

4.1Performance Overhead

One of the most significant obstacles to implementing privacy-preserving mechanisms is the computational cost they impose.

- **Encryption-Related Latency**: Traditional encryption techniques such as AES or RSA, though highly secure, add processing delays during data encryption, decryption, and transmission—especially when applied to large-scale databases.
- **Homomorphic Encryption**: While revolutionary in enabling computations directly on encrypted data, homomorphic encryption algorithms are computationally intensive and consume significant processing power and memory. This makes them impractical for real-time systems or large datasets under current hardware constraints.
- **Secure Indexing**: Techniques like Searchable Symmetric Encryption (SSE) or encrypted B+-trees, though useful for enabling

queries on encrypted data, often require additional I/O operations, leading to higher query response times compared to unencrypted databases.

4.2 Key Management Complexity

Effective key management is the cornerstone of secure encryption, yet it remains one of the most challenging aspects of privacy-preserving data storage.

- **Key Lifecycle Management**: Organizations must handle key generation, storage, rotation, and destruction securely. Failure at any stage could compromise the integrity of the entire database system.
- **Single Point of Failure**: If encryption keys are lost, corrupted, or stolen, it could result in permanent data loss or unauthorized access, with little to no chance of recovery.
- **Scalability**: As systems scale, managing keys for thousands or millions of users or devices becomes increasingly difficult without an advanced Key Management System (KMS) or integration with hardware security modules (HSMs).

4.3 Querying Limitations on Encrypted Data

While encrypted databases are essential for privacy, they often come at the cost of query expressiveness and efficiency.

- **Restricted Operations**: Common database operations such as joins, aggregations, wildcard searches, and pattern matching are either limited or entirely unsupported on encrypted data formats.
- **Trade-offs in Secure Indexing**: Implementing secure indexes typically demands a balance between functionality and privacy. While they may speed up queries, they can leak metadata, such as access patterns or frequency of data access.
- **Reduced Analytical Capability**: Anonymized or encrypted data is less useful for advanced data analytics, machine learning, or AI-based decision-making without significant preprocessing or decryption, which can compromise privacy.

4.4. Jurisdictional and Compliance Complexity

Ensuring compliance with global data protection laws in a cloud environment is increasingly complex, especially as cloud data is often replicated or moved across geographic regions.

- **Multi-Jurisdictional Storage**: Cloud service providers operate globally, and data may be stored in multiple data centers. This creates legal ambiguities when trying to adhere to laws like the General Data Protection Regulation (GDPR) in Europe or HIPAA in the United States.
- **Cross-Border Data Transfer**: Transmitting sensitive information across borders can violate sovereignty or data residency laws, resulting in legal liabilities.
- **Auditing and Documentation**: Demonstrating compliance requires transparent auditing, which becomes difficult in cloud environments due to limited visibility into how and where data is processed.

4.5 Lack of User Awareness and Control

End-users often have limited understanding of how their data is managed and secured in cloud environments, which can lead to uninformed consent or misconfigured security settings.

- **Delegated Trust**: Users frequently rely on third-party cloud providers without verifying whether appropriate privacy-preserving mechanisms are in place.
- **Poor Security Practices**: Weak password policies, lack of multi-factor authentication, or incorrect key handling practices can nullify the benefits of even the most advanced privacy technologies.
- **Awareness Gap**: Many organizations and individuals underestimate the risks of storing sensitive data in the cloud, especially in the absence of formal privacy policies and user education.

V.FUTURE DIRECTIONS

As cloud computing continues to evolve and data privacy regulations grow more stringent, the landscape of privacy-preserving storage in cloud databases must adapt accordingly. Future innovations must address existing limitations while opening new frontiers for secure, scalable, and intelligent data storage and retrieval. The following directions highlight promising research and technological advancements essential for enhancing privacy in cloud-based database systems.

5.1 Optimizing Homomorphic Encryption for Practical Use

Although Fully Homomorphic Encryption (FHE) offers the groundbreaking ability to perform computations on encrypted data without ever decrypting it, its real-world application remains constrained due to its high computational overhead and latency.

- Future research should focus on developing lightweight, application-specific variants of FHE that are computationally efficient for cloud environments.
- Improved hardware acceleration, such as GPU or FPGA-based support for FHE operations, can significantly enhance performance and make it viable for real-time analytics, especially in privacy- critical sectors like finance or healthcare.
- Collaborative initiatives between academia and industry are essential to transform FHE from a theoretical construct into a production-ready solution.

5.2 Leveraging Confidential Computing and Trusted Execution Environments (TEEs)

Traditional data security models protect data only when it is at rest or in transit. However, data in use—during processing—remains vulnerable. The emergence of confidential computing aims to address this gap.

- Secure enclaves like Intel SGX and AMD SEV provide hardware-isolated environments that ensure sensitive computations are protected, even from cloud providers or system administrators.
- Integration of TEEs with cloud databases can enable end-to-end data protection across all stages— storage, transmission, and computation.
- Future systems should incorporate enclave-aware query engines, allowing encrypted queries to be securely processed inside trusted hardware zones without exposing the underlying data.

5.3AI-Driven Privacy Enforcement and Monitoring

Artificial intelligence and machine learning offer a promising avenue to automate and enhance data privacy mechanisms in cloud environments.

- Advanced AI models can be trained to monitor data access patterns, identify irregular behavior, and detect anomalous activities that may indicate security breaches or privacy violations.
- Predictive analytics can assess risk levels dynamically and automatically adjust data privacy policies in real-time, offering adaptive security controls based on contextual factors such as user role, device type, or location.
- Future research could explore privacy-aware reinforcement learning, where models continuously improve access control strategies based on feedback and privacy goals.

5.4 Privacy in Federated Cloud Database Systems

As organizations increasingly adopt multi-cloud and hybrid architectures, ensuring privacy across distributed cloud environments becomes a major priority.

- Federated cloud database systems enable data storage and processing across multiple cloud providers, often in different jurisdictions, without centralizing the data.
- Ensuring privacy in such environments demands the development of federated query protocols that respect local data regulations and do not compromise data confidentiality during inter-cloud communication.
- Integration with federated learning models can allow insights to be derived from distributed data sources without raw data ever leaving its origin, preserving privacy while enabling global analytics.

5.5 Enhancing Blockchain Interoperability with Cloud Databases

Blockchain technology, known for its transparency, immutability, and decentralization, can complement traditional cloud databases when integrated effectively.

- Future systems should aim to create hybrid data architectures where sensitive logs, access records, or metadata are stored on a permissioned blockchain, while large volumes of structured data remain in optimized cloud databases.
- Smart contracts can be employed to enforce automated and tamper-proof access control mechanisms, ensuring that privacy policies are embedded at the protocol level.
- Research should also explore cross-chain interoperability, allowing different blockchain frameworks and cloud systems to securely interact, enabling a truly decentralized and privacy-preserving data management infrastructure.

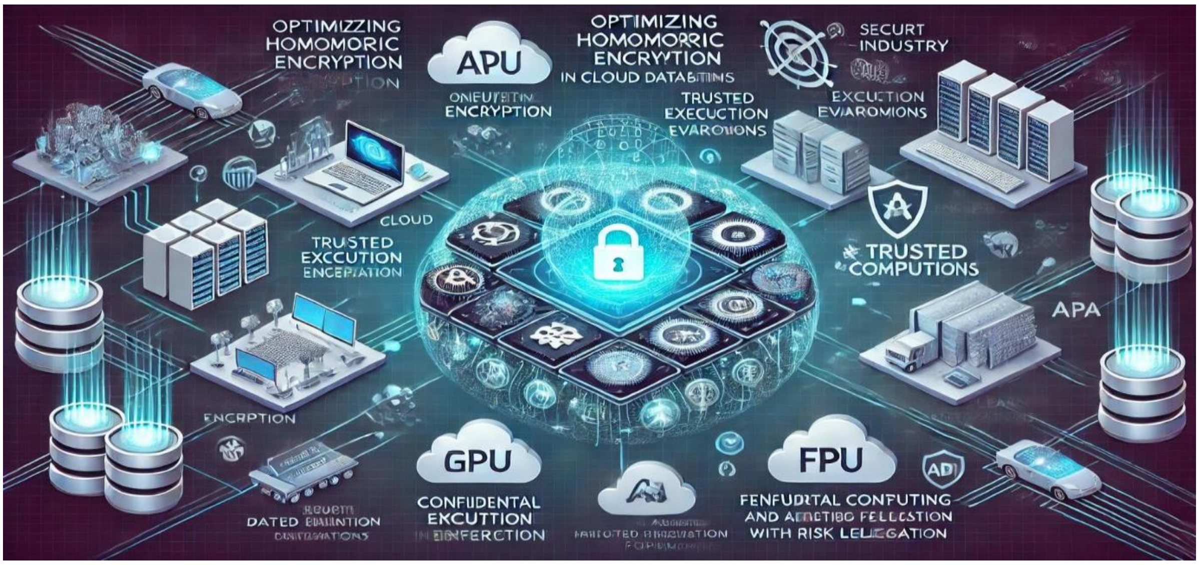
OPTIMIZING HOMOMORIC ENCRYPTION
APU
ONEUFSTIN ENCRYPTION
OPTIMIZING HOMOMORRIC ENCRYTION IN CLOUD DATABITINS
TRUSTED EXECUCTION EVAROIONS
SECURT INDUSTRY
EXCLCTION EVAROMIONS
CLOUD
TRUSTED EXCUTION ENCEPIATION
TRUSTED COMPUTIONS
APA
ENCRPTION
GPU
CONFIDENTAL EKCUTTION ENFERCTION
FPU
AD
FENFUDTAL CONFUTING AND AENCTIBO FELLECSTION WITH RISK LELEGATION
DATED EBAUNTION

Fig. 4: Future Directions in Privacy-Preserving Cloud Database Storage.

VI.CONCLUSION

In the digital era, where cloud computing is the backbone of data-driven enterprises, ensuring data privacy is both a technical and ethical imperative. As organizations increasingly migrate sensitive workloads to the cloud, the urgency to adopt robust privacy-preserving data storage techniques becomes paramount. The convergence of large-scale data availability, stringent regulatory landscapes, and growing cyber threats has transformed privacy from a mere feature to a foundational requirement.

Techniques such as data encryption, fragmentation, anonymization, secure indexing, and blockchain integration serve as the cornerstones of modern privacy-preserving strategies. Each of these methods plays a critical role in protecting data confidentiality, integrity, and controlled access within cloud environments. However, despite their strengths, these technologies are not universally applicable or foolproof. They often entail performance trade-offs, increased system complexity, and require meticulous implementation to achieve the desired level of security without degrading user experience.

Moreover, the dynamic nature of privacy challenges necessitates continuous innovation. Emerging paradigms like confidential computing, homomorphic encryption, and AI-driven privacy controls offer a glimpse into the future—where data can remain private not only during storage and transit but also during computation. Integrating these advancements with regulatory compliance frameworks such as GDPR, HIPAA, and other international standards is essential for building trust and transparency in cloud-based systems.

Organizations must move beyond reactive privacy measures and embrace a privacy-by-design philosophy. This involves embedding privacy considerations into every layer of cloud database architecture—from data modeling and encryption to user access policies and audit mechanisms. Collaboration across disciplines, including cryptography, artificial intelligence, cloud engineering, and law, will be crucial to building resilient and privacy- conscious database ecosystems.

In conclusion, while significant strides have been made in the domain of privacy-preserving data storage, the journey is far from over. As technology advances and adversaries become more sophisticated, so too must our defenses. By proactively investing in privacy-preserving technologies and cultivating a culture of responsible data stewardship, organizations can not only safeguard sensitive information but also earn and maintain the trust of users, clients, and stakeholders in an increasingly connected world.

References

[1] *Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of Secure Computation.*

[2] *Popa, R. A., Redfield, C., Zeldovich, N., & Balakrishnan, H. (2011). CryptDB: Protecting confidentiality with encrypted query processing. ACM Symposium on Operating Systems Principles.*

[3] *IBM Cloud Documentation. https://cloud.ibm.com/docs*

[4] *Microsoft Azure SQL Database. https://azure.microsoft.com/en-us/products/azure-sql/database/*

[5] *Google Cloud Spanner Documentation. https://cloud.google.com/spanner*

[6] *MedRec: A blockchain-based medical records system. MIT Media Lab. https://medrec.media.mit.edu/*

[7] *Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications.*

[8] *Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC '09), 169–178. https://doi.org/10.1145/1536414.1536440*

[9] *Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2017). Untangling blockchain: A data processing view of blockchain systems. Proceedings of the VLDB Endowment, 12(2), 198–211.*

[10] *Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., & Inácio, P. R. M. (2014). Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113–170. https://doi.org/10.1007/s10207-013-0208-7*