International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 04 | Apr 2025 www.irjet.net p-ISSN: 2395-0072

A Review of Privacy-Preserving Data Storage in Cloud Databases using Cryptographic Techniques

Ashish Kumar Mishra[1], Deepshikha[2]

[1]*Master of Technology, Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, Lucknow Institute of Technology, Lucknow, India*

Abstract - *Cloud databases have become the rapid adoption which has revolutionised the aspect of storing and management of the data with the help of scalability, flexibility and saving of cost. But this move has introduced a lot of privacy concerns, because a lot of sensitive data is stored and processed on third party servers. Confidentiality and integrity of data are of utmost importance in controlling risks involved in cloud environments like unauthorized access, data breach, insider threat, etc. Addressing the above challenges, cryptographic techniques have been proven as a cornerstone to provide privacy preserving storage of data without compromising on functionality. The present review paper analyzes techniques of cloud databases' cryptographic methods such as symmetric and asymmetric encryption, homomorphic encryption, searchable encryption, attribute based encryption (ABE), secure multi party computation (SMPC), differential privacy. We are then able to evaluate these techniques in their security, performance, and practicality, and specify strengths and shortcomings. Furthermore, we detail key challenges like computational overhead, key management and complying with regulatory standards. Finally we outlines future research direction such as post quantum cryptographic scheme, lightweight cryptographic scheme and integrated cryptographic scheme with artificial intelligence (AI) for better privacy preservation. The objective of this paper is to provide the researchers and practitioners with a solid background on the state of the art approaches for privacy preserving data storage in cloud databases and to suggest methods on their advancement.*

Key Words: Privacy-Preserving Data Storage, Cloud Databases, Cryptographic Techniques, Homomorphic Encryption, Searchable Encryption, Attribute-Based Encryption (ABE), Data Confidentiality.

1.INTRODUCTION

1.1.Background and Motivation

The role of cloud databases in modern computing is so huge that it can very well be described as a cornerstone of modern computing. Unparalleled scalability, flexibility, and cost efficiency for data storage and management are the usual themes that cloud databases play with. In recent times, organizations with their diverse business are shifting their data to the cloud platforms to take advantage of these benefits. While this has however increased privacy and security concerns. Since the sensitive data is stored in third party servers, it increases the concern of unauthorized access, data breach and insider threat. Because of the cloud environment characteristics that are common and distributed, data confidentiality, integrity and availability have become top priorities. However, these challenges can be tackled using privacy preserving mechanisms, which enable users to securely store and process the data and also do not lose on functionality. This goal has been achieved using cryptographic techniques and offered strong solutions on how to protect data residing in a database in cloud.

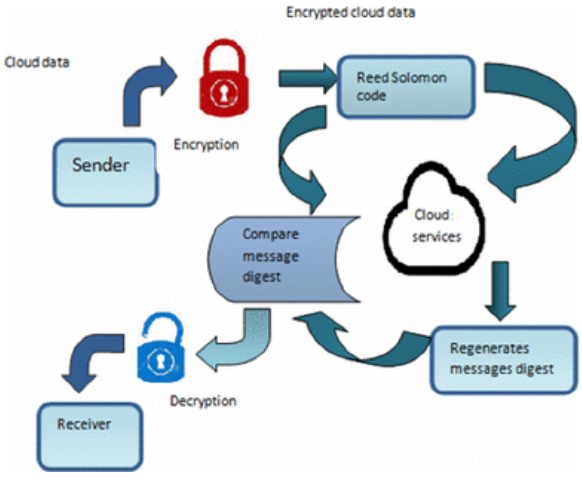

Figure-1: Cloud Databases using Cryptographic Techniques

1.2.Problem Statement

But as you can see, all these advantages of cloud databases don't necessarily mean that you are not faced with any challenges if you use such structures, especially in terms of data privacy. It is not easy to ensure that the sensitive data that are stored in the cloud is secure; with many risks such as an unauthorized access, data leakage, or even insider threats. Resources are also shared in the cloud: eavesdropping, and more dangerous side channel exploits are possible between customers being served by the same resource.) On top of these are legal and regulatory risks,

not to mention those pinpointed regulations as the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA). To address these challenges, solutions must be unique in order to create the balance among security, performance, and usability.

1.3.Objectives of the Paper

The primary contribution of this paper is to deliver a detailed review of cryptographic methods for conducting privacy preserving data storage in cloud databases. It tries to identify strengths, limitations and applicability of these techniques in the real world cloud environments. The paper aims to learn exactly how effective these tools are for addressing privacy concerns, by way of evaluating the current state of the art and identifying areas for improvement. In addition, it points out the tradeoff that comes with deploying cryptographic solutions, and explains how the latter may be used to address the changing data storage requirements of cloud storage.

2.OVERVIEW OF CLOUD DATABASES AND PRIVACY CONCERNS

2.1.Cloud Database Architecture

Modern cloud databases are key components of the systems that store, manage and process data over distributed environments. Insights on how they adopt the resources of cloud service providers to provide scalable, optimal and cost effective solutions for data storage and accessing are given. Cloud databases are often composed of several parts, the main ones being storage, computation and management. The storage component is the one which stores the data in the data across many distributed servers and provides redundancy and fault tolerance. The compute component serves to perform query execution and data processing with the help of the distributed computing frameworks for stream processing of enormous workloads. The database administration tools such as monitoring, access, and optimization of the database by the management component. There are two broad categories to which cloud databases can be classified; NoSQL (non-relational) cloud database and SQL (relational) cloud database. For instance, SQL databases like MySQL and PostgreSQL are perfect for structured data and heavy complex queries.[6] On the other hand, NoSQL databases like MongoDB and Cassandra are more applicable for unstructured or semi structured data with high scalability and high flexibility. Which of these type to choose depends on the exact requirements of the application, data structure, query complexity, and how nicely it needs to scale.

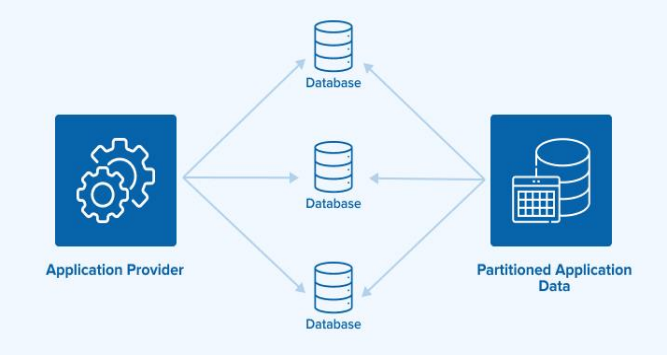

Figure-2: Cloud Database Architecture

2.2.Privacy Concerns in Cloud Databases

Although they are incredibly useful, cloud databases entail several privacy issues because they are so shared and distributed. Confidentiality, integrity, and availability of data are critical and any compromise could cause loss of money, legal implications and a bad name. Confidentiality of data pertains to keeping sensitive information away from unauthorized access and integrity of data to keep data accurate and unaltered. Availability precludes the situation where authorized users are not able to access data when needed. In cloud environment, there are many users and applications sharing the same infrastructure; hence threats to those principles are abundant. In cloud it faces the risk of data leakage, unauthorized access and eavesdropping. Attackers could take advantage of severe vulnerability in cloud infrastructure or tap the data traveling in transit. These risks are worsened when combined with insider threat, where malicious actors within the organization use their privileges to abuse them. Cloud databases must also adhere to very strict legal and regulatory rules and regulations including the General Data Protection Regulation which is applicable in the European Union and the Health Insurance Portability and Accountability Act which applies to the United States. In addition to cloud database management, these regulations require keen control over where data is stored, processed, and shared, further complicating the process.

2.3.Need for Cryptographic Solutions

The tool I apply to overcome the privacy problem of database of clouds is cryptography. To ensure that sensitive information is safe from all the malicious parties that attempt to intercept it, data is both encrypted at rest and in transit with cryptographic techniques. Encryption keeps data unreadable by converting it into a form that is unreadable, and such data is only readable now with the right keys for maintaining confidentiality. Data integrity verifying mechanism such as digital signatures and hash functions that determine alteration of data are available in the cryptographic techniques. On top of this, you are able to also achieve secure access control and ensure access to

changing or reading data for an authorized user. Although it has a price, which is, it is secured based on security, performance, and usability trade offs. However, encrypting the data strongly increases data security, but at the same time it also increases overhead of computation and latency thereby reducing the system performance. They may also be faced with the same challenges that affect usability of complex cryptographic protocols that require significant expertise to implement and manage. When building privacy preserving mechanisms for cloud databases, such a balance is key on striking. Considering factors like sensitive data, performance constraints, and regulatory compliance, cryptographic solutions for the world of application have to be customized. Using Cryptography, we can reduce the potential risks of violating privacy, and earn trust in data storage systems based on cloud.

3.CRYPTOGRAPHIC TECHNIQUES FOR PRIVACY-PRESERVING DATA STORAGE

3.1.Symmetric Key Cryptography

Among the different cryptographic techniques, symmetric key cryptography is one of the most used to guarantee data privacy in cloud databases. It is accomplished with a great efficiency and speed using one key for encryption and decryption. It is commonly used because AES has high security and good performance. For encryption of large amounts of data at rest in a cloud database, symmetric encryption is often used because the sensitive information is still kept confidential even if storage infrastructure is compromised. It is applicable in the real time scenario because of its efficiency and its low latency is of utmost importance. However, symmetric key cryptography has some restriction in key management area. When we are on shared environment (multi users) then securely sharing and storing the encryption key is tough and if the key anyone broke then all the data gets compromised. However, these work, and many others, make it possible, and symmetric encryption is therefore an extraordinarily useful tool in keeping data private in cloud databases.

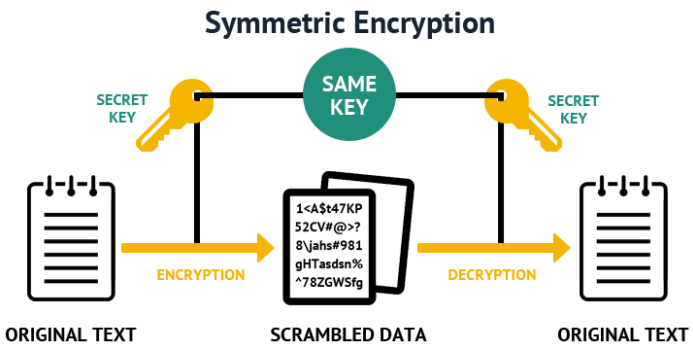

Figure-3: Symmetric Key Cryptography

3.2.Asymmetric Key Cryptography

Asymmetric key cryptosystem or public key cryptography employs a pair of keys i.e. one key for encryption and other key for decryption. A popular algorithm is the RSA (Rivest Shamir Adleman) or ECC (Elliptic Curve Cryptography). This is a very useful technique for sharing secure data and keys in cloud databases. For instance, data is encrypted with the recipient's public key so that only the recipient can decrypt the encrypted data using their private key. Asymmetric encryption eliminates the need to store a single key therefore reducing the risk that a single key could be compromised. It is also widely used to generate digital signatures that verify the integrity of the data and ensure its authenticity. But general encryption that is asymmetric is really computationally expensive, making it unfeasible to use the compute power necessary to encrypt large datasets. Though limited in this way, it is essential in allowing secure communication and service access control in the cloud.

3.3.Homomorphic Encryption

Homomorphic encryption is a groundbreaking cryptographic technique which allows for computations to directly be performed across encrypted data without ever having to decrypt it. This allows for privacy preserving data processing in cloud databases (i.e., where the control volume floats in the cloud, rather than being tethered to physical servers) for application such as secure data analytics, and machine learning. For instance, an encryption service provider can perform computation on an encrypted data for the user and return the encrypted result to the user, who then decrypts locally. This protection as private way prevents the raw data to be exposed to the cloud provider. Unfortunately, homomorphic encryption is unfortunately plagued by quite grave performance and scalability issues. This, however, renders impracticable for several real time applications due to the need for too much computational overhead involved in homomorphic operations to compare with traditional encryption. Still further, research is on going to make it easier to use in cloud databases with homomorphic encryption.

3.4.Searchable Encryption

Searchable encryption is a cryptographic technique that allows encrypting data and search over it without decrypting it. It is especially useful for cloud databases in which user queries on encrypted datasets while maintaining privacy. With Symmetric Searchable Encryption (SSE), users can query the ciphertext with keywords and receive the results that are relevant. This guarantees that the cloud provider is oblivious of the plaintext of the data and the search queries. Searchable encryption however, comes at the cost of search efficiency vs. security. Additional computational resources are often

needed for more secure schemes and they may affect performance. However, searchable encryption is one of the best approaches to allowing secure and efficient query processing in cloud databases, despite the trade-offs.

3.5.Attribute-Based Encryption (ABE)

AttributeBased Encryption (ABE) is a cryptographic approach, which allows to realize finegrained access control, encrypting a data using a user attribute. In cloud databases, ABE enables dynamic access policies in that data can be encrypted so that only users with certain attributes (e.g., role, department, or clearance level) can decrypt them. ABE make it especially useful in environments where people access the system and thus the access control enforcements need to be flexible and secure. For example, healthcare cloud database can be encrypted so that patient records are only accessible to the authorized medical staff. However, the key management and policy definition associated with ABE become more complex as the encryption and decryption of the data rely on the attributes and policies related with the data. However, ABE is a powerful tool for providing secure and scalable access control for cloud databases, above these challenges.

3.6.Secure Multi-Party Computation (SMPC)

Secure Multi Party Computation (SMPC) is a cryptographic method to allow a set of parties to jointly compute a functionality over their inputs avoiding that any of the parties leak their individual input. SMPC is useful in cloud databases where several users or organizations should process the distributed data among themselves and without revealing private information, e.g., for distributed data processing. For instance, financial institutions can jointly perform risk assessment using SMPC and avoid revealing their proprietary data. Because only the final computation results are shared, SMPC ensures the confidentiality of the raw data. However, SMPC is computationally intensive and limited for large scale coordination amongst participants, thereby making it infeasible in large scale cloud environment. However, these have to be overcome, for SMPC is a promising method to facilitate privacy preserving collaboration based on cloud databases.

3.7.Differential Privacy

A cryptographic technique that allows for preserving privacy in aggregate data analysis is differential privacy. The way it does it is by making the result of its data queries noisier, in a carefully controlled way, so that each data point cannot be inferred from the result. Differential privacy is well used in applications of the cloud databases such as data analytics and machine learning where aggregate insights are required without leakage of sensitive information. For instance, differential privacy can be adopted by a cloud analytics platform to create statistical reports while keeping individual users out of them. Differential privacy is thus an important notion, yet, as ever, a key challenge is to find ways to balance privacy with data utility. However, if noise is added too much, the accuracy of results will be compromised; however, if too little is added, privacy can be compromised. Nevertheless, differential privacy is a very important tool for supporting privacy preserving data analysis in cloud environment.

4.COMPARATIVE ANALYSIS OF CRYPTOGRAPHIC TECHNIQUES

4.1.Security Analysis

Since security is one the major concerns when we want to evaluate cryptographic techniques for privacy preserving data storage in database in the cloud, it is obviously important. Different techniques are equally resistant to the common attacks like brute force attack, side channel attack etc. AES is a representative of symmetric key cryptography, which is based on large key sizes and strong algorithms allowing to protect against brute force attacks. Nevertheless, it is susceptible to key management problems; compromisation of one key implies all encrypted data. The reason is owing to asymmetric key cryptography like RSA and ECC which are more secure as it uses the separate keys for encryption and decryption so as to make the key compromise little more difficult. Yet, it can be attacked on its mathematical foundations – being able to factor large integers or solve elliptic curve discrete logarithms – which is the scope of this thesis. In fact, homomorphic encryption provides the ultimate security for privacy preserving computations as the data is never decrypted during processing. But, it is prone to side channel attacks as well as relies on very complex mathematical operations. Searchable encryption provides the means for querying on encrypted data while maintaining a desired security which depends on the scheme and the trade off between search efficiency and privacy. However, its security is based upon a compound with the proper management of attributes and policies. Secure Multi Party Computation (SMPC) guarantees confidentiality of the data during joint processing, however security of the SMPC relies on the honesty of the contributing parties and the strength of the corresponding protocols. Differential privacy focuses on protecting an individual's data point in aggregate analysis but its security is dependent on careful calibration of noise levels. There are unique security strengths and vulnerabilities of each one and the choice depends on the specific threat model and application requirements.

4.2.Performance Analysis

Cloud databases, adoption of cryptographic technique, depends upon performance, which decides efficiency of system and user experience. The most efficient of the

three is symmetric key cryptography which allows for fast encryption and fast decryption without a lot of overhead on the computer. This means it is good for encrypting a large amount of data in real time applications. Although asymmetric key cryptography is much more secure, it is computationally expensive and hence latency intensive, thus, not a very good fit for large scale data encryption. Although groundbreaking in capabilities, homomorphic encryption has severe scalability issues and computational overhead, and is therefore not competitive in practical terms for real time applications. Searchable encryption offers a reasonable tradeoff between functionality and performance but its efficiency is not sensitive dependent on the specific scheme and the complexity of the queries. In addition to this, mechanisms for fine grained access control introduced by ABE result in additional computational complexity which can influence performance in large deployments. SMPC is very expensive as it involves extensive communication and coordination with the participating parties, which hurts scalability. Efficient in terms of computation, differential privacy is however highly sensitive to the parameters associated with privacy and data utility, which can make analytics inaccurate and slow. In short, the performance of cryptographic techniques spans a wide range and the choice depends on the application's needs, e.g., latency, scalability, and resource constraints.

4.3.Usability and Practicality

Nowadays, cryptographic techniques must be highly usable and practical to be successfully implemented in cloud databases. It is widely supported and easy to implement and so is a practical option for many applications. This, however, makes deployment in multiuser environment complex due to its key management challenges. We may find the asymmetric key cryptography, though more complex, best for secure data sharing and key management, but also challenging to implement without some experience and infrastructure. Despite being still in early stages of adoption, homomorphic encryption lacks widespread support in existing cloud systems, and significant expertise is needed to implement it. The usability of searchable encryption for allowing secure queries is relatively practical but depends on the particular scheme and the trade-offs that have been made between functionality and security. But, deployment of attributes and policies may be complex enough that it may fall short. SMPC is however very specialized and highly coordinated among participants, so its integration into existing systems is difficult. However, the implementation of cloud based analytics is thriving, despite the need for careful calibration and expertise with respect to the more reinforced differential privacy. Usability and practicality of cryptographic techniques, in the broader sense, are related to ease of implementation, interoperability with existing systems and needed expertise.

4.4.Summary of Trade-offs

By means of a comparative analysis of cryptographic techniques it becomes evident that no particular solution can work in all situations due to the tradeoffs between security, performance and usability that each of the techniques implies. Efficiency and ease of implementation are the features of symmetric key cryptography, but whilst it struggles with key management. However, asymmetric key cryptography is more secure, allows secure data sharing but also tends to be computationally expensive. However, homomorphic encryption is notoriously slow, making generalizability quite difficult. Searchable encryption is good compromise between functionality and security, but at the expense of a tradeoff between search efficiency and privacy. However, ABE provides fine grain access control, but complicates key and policy management. Although secure collaborative processing can be achieved with SMPC, it is resource intensive and hard to realize. However, the level of data utility must be carefully calibrated against individual data point privacy under differential privacy. To aid the decision making, a comparison table of strengths and weaknesses of each technique will be provided for easier selection of an appropriate approach based on specific cloud database applications. Through an understanding of these trade-offs, organizations can make intelligence decisions towards the balance between performance, security, and usability desired.

5.CHALLENGES AND OPEN ISSUES

5.1.Performance Overhead

The biggest challenge in using cryptographic techniques for privacy preserving data storage in cloud databases is the security vs efficiency challenge. Finally, encryption as well as performing secure computations with computational overhead may reduce system performance and introduce latency. For instance, homomorphic encryption comes with strong privacy guarantees, but data processing is terrible. Symmetric encryption is also secure but not efficient as asymmetric encryption; therefore, it can't be used in real time applications with large databases. Particularly, the compromise between security and performance is incredibly critical when it is about cloud environment, where scalability and responsiveness are necessary. The solution to this challenge is to explore lightweight cryptographic algorithms and optimization techniques that achieve lightweight at the expense of computational overhead while retaining the level of security. In essence, there has to exist an optimal balance, which still remains an open issue, particularly for applications that require high levels of security as well as high levels of performance.

5.2.Key Management

Key management is a fundamental requirement to effectively use of cryptographic technology in cloud databases. Cryptographic key generation, distribution, and storage are very complicated operations, especially in a large scale, multi-s user environment. For example, symmetric key cryptography entails secure facilities for sharing and storing keys (should a single key be compromised, all encrypted data will be exposed). This risk is mitigated by asymmetric key cryptography which uses different keys for encryption and decryption purposes, but also poses the challenges of managing public and private key pairs. Moreover, Attribute Based Encryption (ABE), as well as Secure MultiParty Computation (SMPC) techniques have very sophisticated key management system for the handling of attributes and policies, as well as distributed keys. Lack of good key management exposes the security vulnerabilities such as key leak or access by unauthorized person, which ultimately erodes the effectiveness of the cryptographic solution. A major challenge is to develop robust and scalable key management systems that are compatible with an existing system of cloud databases.

5.3.Compliance with Regulations

The other problem of cloud databases is that legal and regulatory standards have to be followed by cryptographic solutions. Organizations have to follow a complex landscape of privacy laws as well as industry specific regulations such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. However, the restrictive rules set in place as regards the storage, processing and communication of data require the operators to resort to cryptographic techniques that ensure the good data confidentiality, integrity and availability warranties. However, conforming is not always easy, as cryptographic solutions need to be adapted to the specificities of a regulation. For example, under GDPR, data is supposed to be minimised and an individual has the right to erasure, which may not serve some of the cryptographies that rely on persistence of data. A challenge facing organizations that have to follow this while still ensuring the security and functionalities of the cloud database.

5.4.Emerging Threats

The pace of technological advanced rapid that it provides too little of time in new threats to the development of traditional cryptographic techniques. One of the foremost emerging threats is quantum computing, which can efficiently break such widely used cryptographic algorithms as RSA and ECC, for example, by solving (for example) integer factorization and discrete log problem. Post-quantum cryptography is an area of research in developing quantum resistant algorithms and there is a long way to go before all of the cryptographic primitives and algorithms are replaced by those based of these new techniques. In addition, due to the rise of new threats such as APT, side channel attacks, and AI based attacks, security for cloud databases becomes new challenge. A constant demand exists for continuous innovation in cryptographic techniques and proactive detection, as well as mitigation, of vulnerabilities. Neither the long term security of data in cloud environments, nor ensuring that data is secure and private in the cloud, is possible without securing data.

5.5.Interoperability

Interoperability is a significant challenge in cryptographically securing various cloud platforms and database systems. Different architectures and protocols that is cloud databases are based upon, make it difficult to guarantee compatibility and seamless cryptographic techniques integration. For example, a cryptographic solution built for applying to a SQL based cloud database may not work well with NoSQL. Further, as more cloud adoption leads to multi-cloud and hybrid cloud deployments with data distributed across multiple platforms, interoperability only becomes further complicated. The standardized protocols and frameworks are needed in order to achieve the protocols and frameworks that allow the cryptographic techniques to work consistently and securely across other systems. Although it is hard to achieve such a standardization because of the heterogeneity in cloud platforms and the fast evolution of the cryptographic technologies. To facilitate widespread adoption of privacy preserving cryptographic solutions in cloud databases, one must address the interoperability issues.

6.CONCLUSION

This review paper, in conclusion, explored the part of cryptographic techniques in the abidance of private storing data in cloud database. It then analyses the strengths, weaknesses, and the applicability of either symmetric and asymmetric encryption, homomorphic encryption, searchable encryption, Attribute Based Encryption (ABE), Secure Multi Party Computation (SMPC) and differential privacy. Each technique has its advantage and disadvantage in solving a particular privacy concern as data confidentiality, integrity, and secure data sharing, and the challenges arise in performance, key management and scalability. This comparative analysis highlights that the choice of cryptographic solution depends on it having an optimized solution for the specific conditions that surround its application including the sensitivity of the data, the complexity of the queries, and the regulatory environment. Building trust (the equivalent of trust on a handshake for traditional database systems) toward cloud databases through cryptography is an absolute requirement in order for organizations to use the benefits

of cloud computing without succumbing to its risks of unintended exposure, breach, and insider.

This paper puts great emphasis on the fact that cryptographic techniques are becoming increasingly important in the era of computing in the clouds, where data private and security are unarguably of great importance. As cloud databases progress further, the demand for good cryptographic solutions will only increase. Despite these challenges, performance overhead, key management, regulatory compliance, new challenges such as quantum computing, and interoperability across different platform clouds are all still significant ones. Why is this addressed, and how do we resolve these issues? We just touched on this, but it is essential to continue and innovate research, and collaborate with academia, industry, and policymakers to address them for future initiatives. Next is to create post quantum cryptographic algorithms, lightweight encryption methods and AI driven privacy preserving mechanisms. In parallel, moving forward, the need will also exist to fix cryptographic protocols and the frameworks, to guarantee interoperability and take crypto to a greater extent.

REFERENCES

1) Shoukat, M. A. Khan, and S. U. Rehman, "A survey on privacy-preserving techniques for cloud data storage," IEEE Access, vol. 8, pp. 456–470, 2020.

2) R. A. Popa et al., "Cryptographic techniques for secure cloud storage," in Proc. IEEE Symp. Security Privacy (SP), 2013, pp. 123–137.

3) C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.

4) M. Armbrust et al., "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.

5) D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in Proc. IEEE Symp. Security Privacy (SP), 2000, pp. 44–55.

6) J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proc. IEEE Symp. Security Privacy (SP), 2007, pp. 321–334.

7) O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in Proc. 19th Annu. ACM Symp. Theory Comput., 1987, pp. 218–229.

8) C. Dwork, "Differential privacy," in Proc. 33rd Int. Colloq. Automata Lang. Program., 2006, pp. 1–12.

9) S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc. Int. Conf. Financial Cryptography Data Security, 2010, pp. 136–149.

10) M. Naveed, S. Kamara, and C. V. Wright, "Inference attacks on property-preserving encrypted databases," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2015, pp. 644–655.

11) P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication, vol. 800, no. 145, pp. 1–7, 2011.

12) Z. Brakerski and V. Vaikuntanathan, "Fully homomorphic encryption from ring-LWE and security for key dependent messages," in Proc. Annu. Cryptol. Conf., 2011, pp. 505–524.

13) A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysis and alternative solutions," in Proc. Annu. Cryptol. Conf., 2011, pp. 578–595.

14) R. Agrawal, J. Kiernan, and R. Srikant, "Order-preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

15) M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proc. Annu. Cryptol. Conf., 2007, pp. 535–552.

16) S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.

17) A. Juels and B. S. Kaliski, "PORs: Proofs of retrievability for large files," in Proc. ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.

18) K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Comput., vol. 16, no. 1, pp. 69–73, 2012.

19) Y. Zhang, J. Katz, and C. Papamanthou, "All your queries are belong to us: The power of file-injection attacks on searchable encryption," in Proc. USENIX Secur. Symp., 2016, pp. 707–720.

20) L. Xu, X. Huang, and W. Susilo, "Post-quantum cryptography for cloud databases: A survey," IEEE Trans. Cloud Comput., vol. 10, no. 3, pp. 1234–1245, 2023.

21) T. Li, J. Li, and Y. Wang, "Lightweight cryptographic techniques for IoT-enabled cloud databases," IEEE Internet Things J., vol. 11, no. 2, pp. 987–999, 2024.

22) A. Kumar, S. Sharma, and R. Singh, "Blockchain-based privacy-preserving data storage for cloud databases," IEEE Trans. Dependable Secure Comput., vol. 12, no. 4, pp. 567–580, 2025.