IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Check for updates

Privacy-preserving based encryption techniques for securing data in cloud computing environments

Ramesh Bishukarma *

Independent Researcher

International Journal of Science and Research Archive, 2023, 09(02), 1014–1025

Publication history: Received on 07 June 2023; revised on 16 August 2023; accepted on 20 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0441

Abstract

A successful strategy for comprehensive data processing and storage is cloud computing. Nevertheless, in cloud environments maintaining confidentiality for critical data remains one of the biggest concerns for end-users as well as service providers. Homomorphic encryption has been proved to be one of the efficient techniques to handle the data securely in cloud while keeping the data secret. The importance of privacy preserving encryption in cloud computing environments is discussed in this paper to justify the significance of these protocols within the IT Industry that has evolved through the availability of elastic, on-demand resources. This paper presents an overview of privacy-preserving encryption techniques that enhance data security in cloud computing. We explore various encryption methodologies, including Symmetric, Asymmetric, and homomorphic encryption, as well as Encryption Protocols like SMPC, ZKPs, PRE and Functional Encryption. These protocols ensure data confidentiality and regulatory compliance while addressing the challenges of maintaining data utility and minimising exposure risks. By proposing a comprehensive framework that integrates these techniques, we aim to provide a robust solution for safeguarding data privacy in cloud environments, ultimately fostering trust and confidence in cloud services. However, as cloud adoption continues to grow, optimising these encryption protocols for computational efficiency and adaptability remains essential to achieving seamless, secure cloud operations across industries.

Keywords: Cloud computing; Data Security; Encryption techniques; Community cloud; Symmetric and Asymmetric Encryption

1. Introduction

Cloud computing is a well-known technology that is expected to boost the efficiency of the IT business. Because of the many issues with earlier technologies, cloud computing plays a crucial part in IT-enabled concepts. Following cloud computing's development [1][2]. The ability to access a wide range of scalable computing resources online whenever needed is a revolutionary transformation in the way data is managed, processed, and stored [3][4]. The several service models that make up this technology—including IaaS, PaaS, and SaaS—are designed to meet the varying demands of organisations when it comes to scalability and flexibility[5][6][7]. Elasticity, cost effectiveness, and low IT maintenance requirements are only a few of the advantages that have prompted broad adoption [8]. However, these benefits come with trade-offs in control and security, necessitating a re-evaluation of traditional security practices to suit the unique, distributed nature of cloud environments[9][10]. Figure 1 depicts the characteristics of cloud computing that are explained in the above and the below part.

[*] Corresponding author: Ramesh Bishukarma

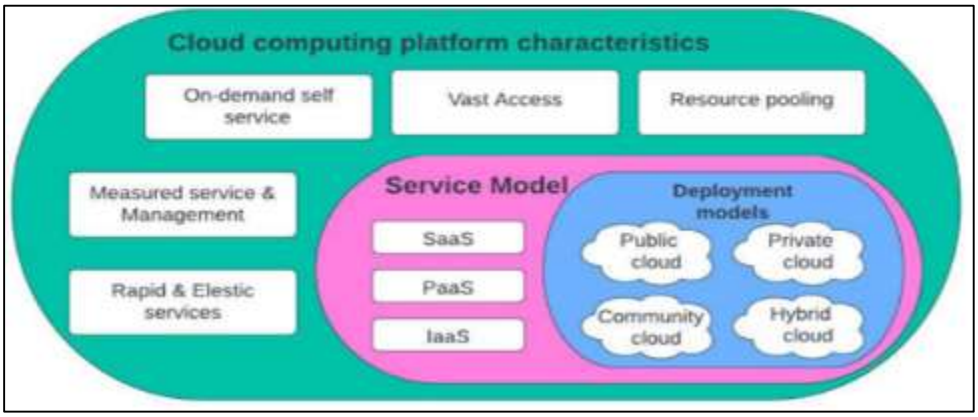

Figure 1 Elements of Cloud Computing

The cloud computing infrastructure uses four primary deployment types and three service models, which are explained below[11].

- **Service Models**
  - **Software as a Service (SaaS):** The SaaS paradigm is a way to distribute software programs via web-based subscription services. Without the need for local installation or maintenance, users may access the program from any device with an internet connection.
  - **Platform as a Service (PaaS):** PaaS allows developers to build, release, and manage programs in the cloud without being concerned with the underlying technology.
  - **Infrastructure as a Service (IaaS):** IaaS provides cloud-based, virtualised server, storage, and networking capabilities. Instead of buying expensive hardware, users may rent these resources as needed, giving them more leeway and scalability when it comes to managing workloads and operating applications.

- **Deployment models**
  - **Public Cloud**: A cloud environment that is publicly accessible and manageable by an enterprise or third-party cloud service provider is represented by a cloud infrastructure in this paradigm[11].
  - **Private Cloud**: Private organisations are responsible for managing and running this type of infrastructure. A primary objective of a cloud model is to maintain a constant level of privacy and security.
  - **Community Cloud**: This type of architecture shares infrastructure among enterprises or communities that have similar objectives and visions, such as security and jurisdiction. Enterprises and external parties can handle these services[7].
  - **Hybrid Cloud**: This kind of deployment model blends two or more cloud models; each is linked but remains distinct.

Protecting sensitive data from cyber threats, breaches, and unauthorised access requires ensuring data security in cloud computing [12]. This includes enforcing data confidentiality, integrity, and availability through encryption, secure APIs, and multi-layered authentication methods[13][14][15]. Since cloud data is frequently processed on shared, third-party infrastructure, the risks are compounded by potential data breaches, account hijacking, and malicious insider access[16][17]. With increasing regulatory pressure, it has become crucial for cloud service providers to implement advanced security protocols that not only protect data but also offer transparency and control to the end-users[18].

The core architecture of the cloud, where shared storage and multi-tenancy make managing data access more difficult, gives rise to privacy problems in cloud computing [19][20] Issues such as data location transparency, cross-border data transfers, and compliance with data protection regulations challenge organisations aiming to safeguard personal information[21][20]. Privacy risks are further amplified by the evolving nature of cloud services, with research suggesting that adaptive privacy measures must be incorporated. Frameworks like STRIDE, used for systematic threat assessment, help classify and mitigate cloud vulnerabilities. Despite such frameworks, the need remains for advanced, scalable privacy solutions that can adapt to the cloud's dynamic, open environment[22].

1.1. Structure of the paper

The study is structured as follows: Section II introduces the conceptual framework for privacy-preserving encryption techniques in cloud computing. Section III outlines key principles of these methods, including data confidentiality and regulatory compliance. Section IV explores encryption's role in securing cloud data. Section V reviews types of encryption techniques like symmetric and homomorphic encryption. Conclusions and suggestions for further study are finally presented in Section VI.

2. Privacy-Preserving Encryption: An Overview

Privacy-preserving encryption is a security approach that means the data will be encrypted to ensure that it is secret, whether in transit or when in the process or stored in unsecured areas like the cloud. This encryption technique provides an opportunity to manipulate data while excluding third parties from its content, combining data utility and security. Several approaches exist in privacy-preserving encryption, including homomorphic encryption[18][19], where computation is conducted on the encrypted data without decryption and secure multi-party computation, where multiple parties compute results without disclosing the underlying data. These methods meet the requirements of both data utility and security, so common in regulatory requirements, and only allow access to data by authorised users or systems for authorised computation[23]. Figure 2 shows the Data Privacy Protection Mechanisms in Cloud.

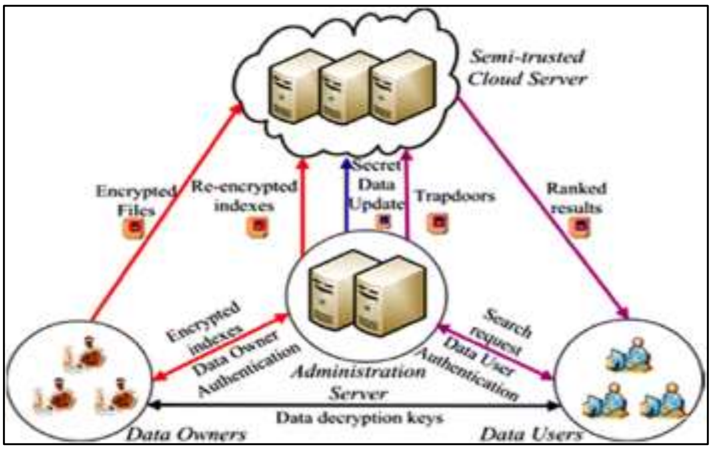

Figure 2 Data Privacy Protection Mechanisms in Cloud

Also, ensuring each participant’s data confidentiality, secure multi-party computing allows numerous participants to compute a function of their data inputs. It is helpful for business applications in cloud environments wherein the groups need to merge data from numerous sources while preserving privacy. Taken together, these privacy-preserving techniques directly meet both the data utility and security requirements that organisations need to meet in order to adhere to strict data protection rules such as GDPR, whereby the data must always be kept private while at the same time being usable only by authorised personnel[24].

2.1. Key Principles of Privacy-Preserving Encryption

There are several principles of privacy-preserving encryption which make data processing more secure and sensitive data is not disclosed. It makes a number of guarantees on behalf of data privacy and use, particularly in areas such as the cloud and multiparty settings.

2.1.1. Data Confidentiality through Encrypted Processing

There are several principles of privacy-preserving encryption which make data processing more secure and sensitive data is not disclosed. These principles assure the privacy and usage of the data in various settings, such as in cloud environments as well as in different multi-party projects [25][26]. The method that can be used is homomorphic encryption and the like so that analysis can be done right on encrypted data without decrypting it, thus maintaining data authenticity. Cloud computing and similar applications rely on this concept heavily since it ensures that only authorised organisations may access encrypted data stored on third-party infrastructure [27].

2.1.2. Data Minimization and Access Control

The way that privacy-preserving encryption works meets the principle of data minimisation; data is only collected and processed when it is necessary to do so and is otherwise kept confidential. Secure multi-party computation (SMPC) supports this by allowing multiple entities to compute functions on them without exchanging the raw data hence limiting data exposure [28][29]. This principle is very crucial in fields like health and economics, where data contains elements that have to be shared between organisations but should not reveal the details of the concerned data[30].

2.1.3. Compliance with Data Protection Regulations

Privacy-preserving encryption complements and sustains legislation such as the GDPR or HIPAA that dictate what kind of encryption technologies should be deployed to meet legal demands of data privacy and security[31][32]. This principle requires that user rights to privacy and protection of data are upheld through encryption protocols being implemented [33][34]. For example, the technique of methods such as attribute-based encryption, grants very specific access to data to specific people without compromising on the general security of the data.

2.1.4. Scalability and Efficiency in Encryption Mechanisms

Scalability is another big principle, or rather, potential capacity of protection, allowing for use of data protection techniques when dealing with large amounts of data and computationally extensive analyses [35][36]. Complex and optimised homomorphic encryption methods, as well as lightweight SMPC methods, let input data be processed and analysed in real-time, which is crucial to many cloud-based applications and services.

2.2. Role of Encryption in Cloud Data Security

Encryption of data is required in cloud environment because the data is typically transformed, retrieved, and transmitted across numerous computers and networks [37][38]. In cloud computing, encryption is vital in minimising vulnerability to unauthorised access and other compromising of data confidentiality because of its federated and multitenant architecture [39][40].

- **Encryption as a Foundational Security Measure:** Encryption is the way to keep breaches and unauthorised access away from the data which is stored in the cloud.
- **Protection on Third-Party Infrastructure:** Encryption protects data that is located on the servers of the cloud providers on behalf of the customers in multi-tenant arrangements.
- **Role of Decryption Keys:** Data confidentiality across platforms is maintained by ensuring that only an authorised user with the decryption key, used to decrypt the encrypted data may access the data.
- **End-to-End Data Protection:** Encryption gives data security in many modes: at rest; when being transported for use at a remote location; and at use; making cloud data security a holistic approach.
- **Secure Data Lifecycle Management:** Security of data is ensured from the time data is stored in cloud servers, when it is being transmitted in the network.
- **Encrypted Data Processing:** New methods like homomorphic encryption made it possible for data to be used and actually be computed on in an encrypted form thus being rid of the need for it to be unencrypted during computation.
- **Utility for Regulated Information:** The necessity of protection based on encryption present for industries to handle sensitive data for finance and personal health result in compliance with regulations.
- **Fine-Grained Access Control:** Encryption facilitates role-based access control, making it possible for providers of cloud services to limit data decryption, and processing to only individuals within their line of authority.
- **Attribute-Based Encryption for Compliance:** Algorithms such as attribute-based encryption restrict access to data on the basis of user attributes and thus will help to meet legal requirements such as GDPR and HIPAA.
- **Controlled Data Access:** Customized security of access helps in reducing cases of access by unauthorised personnel thus making data stored in cloud accessible only to allowed users in specific environments.

3. Types of Encryption Techniques in Cloud Computing

Cloud computing requires encryption methods to help achieve confidentiality, accessibility, and data integrity. These techniques prevent data leakage while at rest and in transfer, allowing users to manage their data in shared or external spaces. Below are some primary encryption techniques widely used in cloud computing.

3.1. Symmetric Encryption

The two parties involved in a secure communication utilise the same key in symmetric encryption, which is also called private key cryptography. Such encryption or decryption of data cannot be possible without use of this key which both parties possess[41]. The mechanisms of symmetric encryption can be grouped into two main groups: the block cyphers and the stream cyphers[42]. Whereas in block cyphers, the data is encrypted in blocks where the cypher takes in plain text in chunks of segments at a time, while in stream cyphers, the cypher works at bit or character level [43]. Two examples of a block cypher that are common and considered standard for the cryptographic measure are the DES and the AES. These paradigms define a key for secure encryption in symmetric cryptosystems and are current mainly due to their efficiency in protecting information.

One critical aspect of symmetric encryption is key management, as the security of this approach hinges on the secure handling of the shared secret key. Key management involves key creation, distribution, and periodic updating to ensure that communication remains secure[44][45]. However, managing keys securely can be challenging, especially in large networks, as any compromise of the key jeopardises the integrity of the entire encrypted communication. The efficiency and speed of symmetric encryption make it a popular choice for encrypting huge amounts of data, as long as strong key management procedures are followed. Figure 3 and the list of components of symmetric encryption as below[46][47]:

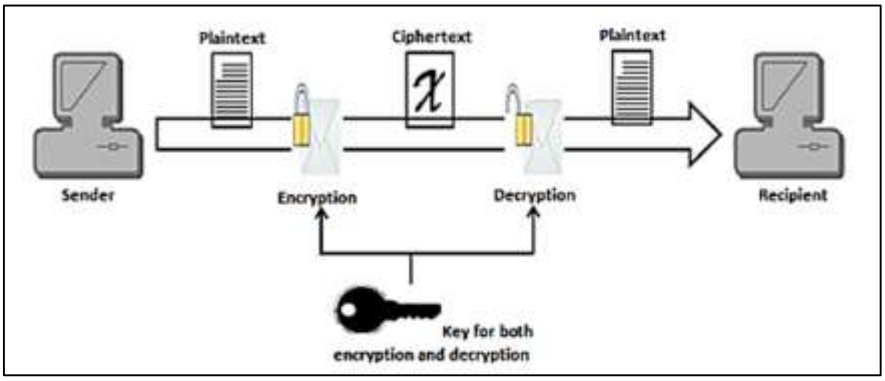

Figure 3 Explanation of whole process of symmetric encryption

- **Plaintext:** This is the first piece of information that the sender is prepared to impart to the recipient. Input these details into the encryption program.
- **Encryption algorithm:** A secret key is used to conduct a set of operations that, when done in plaintext, yield ciphertext.
- **Secret key:** This value is used to convert plaintext to ciphertext; however, it is not reliant on plaintext itself.
- **Ciphertext:** This is the result of running the encryption method on the original plaintext. The plaintext version will be much different.
- **Decryption algorithm:** Executes a series of operations on ciphertext with the employ of a secret key after recovering the original plaintext.

3.2. Asymmetric Encryption

Asymmetric encryption, sometimes known as public-key cryptography, is a method whereby a message is encrypted using the public key of the receiver and decrypted using the private key of the sender. Even on a public network, this method provides a safe route for data exchange by limiting access to the message to the intended receiver alone [48][6]. In Figure 4 the whole process explains in the asymmetric encryption. Digital signature technologies, which rely on public-key cryptography, are essential for ensuring the validity and integrity of communications or documents. Two of the most prominent digital signature mechanisms based on asymmetric encryption are the RSA and DSA methods[49].

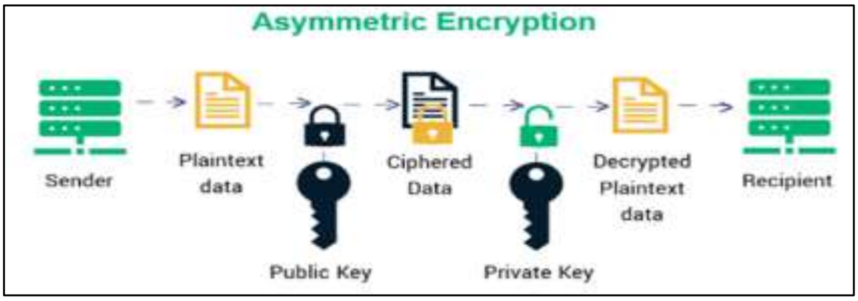

Figure 4 Asymmetric Encryption

Public-key cryptography techniques rely on the computational difficulty of specific "hard problems." For example, the security of the RSA algorithm is based on the integer factorisation problem, which involves factoring a large number into its prime components. The discrete logarithm issue is another computationally difficult obstacle that Diffie-Hellman and DSA use to ensure security. In recent years, elliptic curve cryptography (ECC) has gained popularity, offering a secure alternative with lower computational requirements. ECC's security is grounded in the complexity of number-theoretic problems related to elliptic curves, making it highly efficient for constrained environments like mobile devices[50].

3.3. Homomorphic Encryption

The distinctive feature of homomorphic encryption is that it enables computations to be applied directly to non-plain text, producing an encrypted version that, upon decoding, reproduces the outcomes of the operations performed on the plain text. Both completely homomorphic and partly homomorphic cryptosystems are common. Partially homomorphic encryption is thought to be less secure than FHE[51]. Figure 5 depicts the whole mechanism of Homomorphic Encryption.

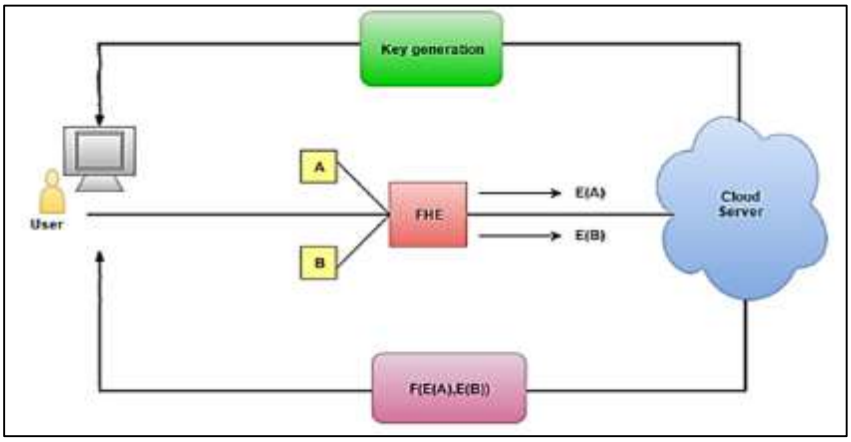

Figure 5 Mechanism of Homomorphic Encryption in Cloud Computing

If a cryptosystem exhibits either the multiplicative or additive homomorphism feature but not both, it is considered partly homomorphic. Examples of such cryptosystems are ElGamal (based on multiplicative homomorphism), Paillier (based on additive homomorphism), and RSA (based on multiplicative homomorphism).

A cryptosystem is considered completely homomorphic if it exhibits the properties of multiplicative and additive homomorphism. The first (and only) system that was previously discussed is a cryptosystem that is based on lattices [52]. FHE is said to be far more potent and an excellent method of effectively securing the data that is outsourced. Gentry's suggested plan consists of three important parts:

- A somewhat homomorphic encryption scheme (SWHES).
- A bootstrappable encryption scheme (BES).
- A combination of above two components

The capacity to do homomorphic computing on low-degree polynomials was possessed by this approach. For homomorphic encryption systems, the research community is attempting to identify potential situations regarding the malleability feature.

4. Privacy-Preserving Encryption Protocols in Cloud Computing

Privacy-preserving encryption techniques are crucial to protecting sensitive data in the quickly changing world of cloud computing, particularly as consumers and businesses depend more and more on cloud storage and service[53]. These encryption protocols allow data to remain secure even when processed, ensuring confidentiality and compliance with privacy regulations. Key methods include SMPC, Zero-Knowledge Proofs, Functional Encryption, and Proxy Re-Encryption.

4.1. Secure Multi-Party Computation (SMPC)

SMPC makes it possible for many people to work together to calculate a function without disclosing private information. It's crucial for scenarios needing data analysis without exposure, like healthcare and finance. Research focuses on improving scalability and efficiency for federated learning, although challenges include high computational costs[54].

4.2. Zero-Knowledge Proofs (ZKPs)

ZKPs enable one side to demonstrate the veracity of a claim without disclosing information. In cloud security, ZKPs aid in secure authentication and data integrity. Advancements in zk-SNARKs and zk-STARKs improve efficiency, reducing communication needs and making ZKPs more suitable for cloud applications.

4.3. Functional Encryption (FE)

FE enables users to compute functions on encrypted data, supporting fine-grained access control without decrypting entire datasets. It's valuable for privacy-preserving analytics, but key management remains complex. Research aims to optimise FE for practical cloud applications.

4.4. Proxy Re-Encryption (and)

PRE allows a third party to re-encrypt data for secure sharing across users without exposing plaintext. It's widely used in data-sharing applications, with current research improving flexibility and reducing proxy trust requirements, although key management remains a challenge.

5. Literature Review

Enhancing cloud computing security via the use of privacy-preserving encryption algorithms has been the primary emphasis of prior research in this field.

In this paper Das, (2018), The user's data is encrypted using a Hybrid Encryption method based on RSA (i.e., HE-RSA) with a padding technique called OAEP to preserve Integrity and Confidentiality while allowing several parties to calculate a function on their inputs. Cloud users may be certain that their data is secure and private when they use HE on encrypted files without decrypting them and use SMPC [55].

In this work, Pronika and Tyagi, (2021), cryptographic algorithms are used to mitigate security concerns. With the proposed method, cloud storage frameworks may use several encryption algorithms, like AES with S-box and the Feistel Algorithm, to increase security. The structure utilises the information-transferring, cutting, ordering, encryption, merging, unscrambling, and recovery cycle to guarantee the security of the huge volumes of data kept in the multi-cloud. The main applications of cryptographic algorithms are secure network transmission and non-human readable data storage in systems [56]. P

In this work, Patil and Biradar, (2018), demonstrates how completely homomorphic encryption may be performed in parallel on encrypted cloud data. Here, FHE is carried out over many nodes using Gentry's encryption technique. Compared to operating on a sequential process, this parallel processing yields superior performance. Another big worry with cloud computing is security. This also demonstrates another effort to improve a security of client data in the cloud by using a data partitioning technique. Several client data files of the same size will be divided up and kept on different servers. Furthermore, public is generated on the client side; this public key is used to save and retrieve data from cloud storage [57].

In this paper, Joseph Manoj et al., (2017), A new, secure hybrid EHR system is advised. This solution protects data privacy and offers fine-grained access control by combining two powerful encryption algorithms. After the health records are divided using a vertical partitioning mechanism, each section is encrypted using multi-authority and key-based encryption algorithms. In the Public Domains (PUDs), multi-authority encryption methods are the most common, although in the Personal Domains (PSDs), key-based encryption schemes are more common [58].

This work, Azzani and Alkalbani, (2022), seeks to identify weaknesses in cloud computing applications' cybersecurity and provide a contemporary solution that prioritises both security and performance. The first stage in examining the security of the cloud computing environment is to simulate and assess the security and performance of three contemporary security techniques for cloud applications. The findings of the analysis provide a crucial indication for the implementation of this security mechanism and highlight the need to create an ideal security mechanism that covers the primary security characteristics of the cloud environment [59].

In this work, Suganya and Sasipraba, (2022), Using the genetic crossover methodology, a novel encryption technique is created to safeguard sensitive and non-sensitive data kept in a heterogeneous multi-cloud environment from the most vulnerable activities, including data breaches, insider attacks, and man-in-the-middle attacks. To make data storage in numerous cloud settings more secure, the suggested prime crossover approach is utilised to encrypt the file. Data availability, confidentiality, and integrity are safeguarded in this manner [60].

Here's a structured Table 1 summarising the related work on privacy-preserving encryption techniques for securing data in cloud computing environments. The table includes various columns to encapsulate key aspects of each paper:

Table 1 Summarizing the related work on privacy-preserving encryption techniques for securing data in CC environments

Paper	Encryption Technique	Key Features	Main Contributions	Security Aspects Addressed	Challenges	Future Work
[55]	OAEP with HE-RSA	Hybrid encryption; enables computation on encrypted data	Allows multiple parties to compute functions while preserving integrity and confidentiality	Integrity, confidentiality, secure multi-party computation	Computational overhead and complexity in homomorphic operations	Explore more efficient algorithms for homomorphic encryption
[56]	AES with S-Box and Feistel Algorithm	Improved cloud storage security; various encryption processes	Utilises multiple encryption algorithms for enhanced data security in multi-cloud environments	Data confidentiality and secure data transmission	Complexity in managing multiple encryption methods	Investigate further optimisation of encryption processes for scalability
[57]	Gentry's Fully Homomorphic Encryption	Parallel processing of encrypted data; improved performance	Demonstrates the benefits of parallel processing in homomorphic encryption for cloud data	Security through data partitioning and encrypted processing	Scalability issues in large-scale cloud environments	Research alternative algorithms that reduce computational demands
[58]	Multi-authority and Key-based encryption	Vertical partitioning of health records; fine-grained access control	Combines two encryption methods for effective data privacy in electronic health records	Access control and data privacy in public and personal domains	Managing multiple authorities and key distribution	Development of automated key management systems
[59]	Modern security mechanisms (unspecified)	Performance and security optimisation	Analyses cybersecurity weaknesses in cloud applications and evaluates security mechanisms	Overall security enhancement in cloud environments	Identifying comprehensive security parameters	Propose a unified framework for security mechanism integration
[60]	Novel genetic crossover technique	Encrypts sensitive/non-sensitive data;	Introduces a unique encryption	Data integrity, confidentiality, and availability;	Ensuring compatibility across	Explore enhancements to the genetic

		protects against vulnerabilities	algorithm using genetic techniques for data storage	protection against attacks	heterogeneous cloud environments	algorithm for better performance

6. Conclusion

Cloud computing has revolutionised IT by offering scalable, on-demand access to computer resources, but it also presents new privacy and security issues. Privacy-preserving encryption protocols and techniques by enabling secure data processing and sharing in untrusted environments. These protocols and techniques provide solid solutions for data security and, at the same time, maintain the advantage of use, which is especially crucial for industries which deal with confidential information, such as healthcare and finance. The implementation of stiff encryption techniques not only protects the information but also fulfils legal requirements of privacy and customer confidence. However, the application of these encryption methods is not easily deployable and requires further enhancement to support efficiency and effectiveness in cloud computing.

Future Scope

Future studies should concentrate on improving the scalability and effectiveness of privacy-preserving encryption techniques in order to better manage the enormous amounts of data that cloud applications demand. There may also be improvements in post-quantum cryptography, which would contribute to the strengthening of these protocols against quantum dangers, strengthening them. Also, the combination between privacy-preserving encryption and artificial intelligence for dynamic protection of data and to meet new regulations is an opportunity to analyse.

References

[1] D. Rountree and I. Castrillo, *The Basics of Cloud Computing: Understanding the Fundamentals of Cloud Computing in Theory and Practice*. 2013. doi: 10.1016/C2012-0-02521-5.

[2] S. A. and A. Tewari, AI-Driven Resilience: Enhancing Critical Infrastructure with Edge Computing, *Int. J. Curr. Eng. Technol.*, vol. 12, no. 02, pp. 151–157, 2022, doi: https://doi.org/10.14741/ijcet/v.12.2.9.

[3] D. M. Bamasoud, A. S. Al-Dossary, N. M. Al-Harthy, R. A. Al-Shomrany, G. S. Alghamdi, and R. O. Algahmdi, Privacy and Security Issues in Cloud Computing: A Survey Paper, in *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, 2021. doi: 10.1109/ICIT52682.2021.9491632.

[4] V. K. Y. Nicholas Richardson, Rajani Pydipalli, Sai Sirisha Maddula, Sunil Kumar Reddy Anumandla, Role-Based Access Control in SAS Programming: Enhancing Security and Authorization, *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 6, no. 1, pp. 31–42, 2019.

[5] A. Jain, P. Singh, and E. A. Jain, Survey Paper on Cloud Computing, *Artic. Int. J. Innov. Eng. Technol.*, 2014.

[6] R. Goyal, The Role Of Business Analysts In Information Management Projects, *Int. J. Core Eng. Manag.*, vol. 6, no. 9, pp. 76–86, 2020.

[7] R. Goyal, Software Development Life Cycle Models: A Review Of Their Impact On Project Management, *Int. J. Core Eng. Manag.*, vol. 7, no. 2, pp. 78–87, 2022.

[8] S. K. R. A. Sai Charan Reddy Vennapusa, Takudzwa Fadziso, Dipakkumar Kanubhai Sachani, Vamsi Krishna Yarlagadda, Cryptocurrency-Based Loyalty Programs for Enhanced Customer Engagement, *Technol. Manag. Rev.*, vol. 3, no. 1, pp. 46–62, 2018.

[9] P. Khare, The Impact ofAI on Product Management:A Systematic Review and Future Trends, *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 736–741, 2022.

[10] R. K. Patchmuthu, A. T. Wan, and W. S. Suhaili, Exploring Data Security and Privacy Issues in Internet of Things Based on Five-Layer Architecture, *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 1, Apr. 2022, doi: 10.17762/ijcnis.v12i1.4345.

[11] R. Goyal, The Role Of Requirement Gathering In Agile Software Development: Strategies For Success And Challenges, *Int. J. Core Eng. Manag.*, vol. 6, no. 12, pp. 142–152, 2021.

[12] Y. Yao, X. Chang, J. Misic, and V. B. Misic, Lightweight and Privacy-Preserving ID-as-a-Service Provisioning in Vehicular Cloud Computing, *IEEE Trans. Veh. Technol.*, 2020, doi: 10.1109/TVT.2019.2960831.

[13] S. Bauskar, BUSINESS ANALYTICS IN ENTERPRISE SYSTEM BASED ON APPLICATION OF ARTIFICIAL INTELLIGENCE, *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 04, no. 01, pp. 1861–1870, 2022, doi: DOI : https://www.doi.org/10.56726/IRJMETS18127.

[14] S. G. Thomas Jubin, Kirti Vinod Vedi, Enhancing Supply Chain Resilience Through Cloud-Based SCM and Advanced Machine Learning : A Case Study of Logistics, *JETIR*, vol. 8, no. 9, pp. 357–364, 2021.

[15] J. Thomas, The Effect and Challenges of the Internet of Things (IoT) on the Management of Supply Chains, *Int. J. Res. Anal. Rev.*, vol. 8, no. 3, pp. 874–878, 2021.

[16] H. S. Chandu, A Survey of Memory Controller Architectures: Design Trends and Performance Trade-offs, *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 930–936, 2022, [Online]. Available: https://www.ijrar.org/papers/IJRAR22D3204.pdf

[17] H. Cheng, C. Rong, M. Qian, and W. Wang, Accountable privacy-preserving mechanism for cloud computing based on identity-based encryption, *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2851599.

[18] B. Alouffi, M. Hasnain, A. Alharbi, W. Alosaimi, H. Alyami, and M. Ayaz, A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies, *IEEE Access*, 2021, doi: 10.1109/ACCESS.2021.3073203.

[19] Z. Wang, Y. Xu, Y. Yan, Y. Zhang, Z. Rao, and X. Ouyang, Privacy-preserving indoor localization based on inner product encryption in a cloud environment, *Knowledge-Based Syst.*, 2022, doi: 10.1016/j.knosys.2021.108005.

[20] K. V. V. and S. G. Jubin Thomas , Piyush Patidar, An analysis of predictive maintenance strategies in supply chain management, *Int. J. Sci. Res. Arch.*, vol. 06, no. 01, pp. 308–317, 2022, doi: DOI: https://doi.org/10.30574/ijsra.2022.6.1.0144.

[21] J. Thomas, H. Volikatla, V. V. R. Indugu, K. Gondi, and D. S. Gondi, Machine Learning Approaches for Fraud Detection in E-commerce Supply Chains, *Innov. Comput. Sci. J.*, vol. 8, no. 1, 2022.

[22] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, Efficient and privacy preserving access control scheme for fog-enabled IoT, *Futur. Gener. Comput. Syst.*, 2019, doi: 10.1016/j.future.2019.04.003.

[23] Sahil Arora and Apoorva Tewari, Zero trust architecture in IAM with AI integration, *Int. J. Sci. Res. Arch.*, vol. 8, no. 2, pp. 737–745, Apr. 2023, doi: 10.30574/ijsra.2023.8.2.0163.

[24] H. Fang and Q. Qian, Privacy preserving machine learning with homomorphic encryption and federated learning, *Futur. Internet*, 2021, doi: 10.3390/fi13040094.

[25] V. Kumar, V. V. Kumar, N. Mishra, F. T. S. Chan, and B. Gnanasekar, Warranty failure analysis in service supply Chain a multi-agent framework, in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[26] V. V. Kumar, A. Sahoo, and F. W. Liou, Cyber-enabled product lifecycle management: A multi-agent framework, in *Procedia Manufacturing*, 2019. doi: 10.1016/j.promfg.2020.01.247.

[27] S. Kumar, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh, Privacy preserving security using biometrics in cloud computing, *Multimed. Tools Appl.*, 2018, doi: 10.1007/s11042-017-4966-5.

[28] V. K. Y. Mohamed Ali Shajahan, Nicholas Richardson, Niravkumar Dhameliya, Bhavik Patel, Sunil Kumar Reddy Anumandla, AUTOSAR Classic vs. AUTOSAR Adaptive: A Comparative Analysis in Stack Development, *Eng. Int.*, vol. 7, no. 2, pp. 161–178, 2019.

[29] K. Patel, An Analysis of Quality Assurance Practices Based on Software Development Life Cycle (SDLC) Methodologies, *J. Emerg. Technol. Innov. Res.*, vol. 9, no. 12, pp. g587–g592, 2022.

[30] V. K. Yarlagadda and R. Pydipalli, Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity, *Eng. Int.*, vol. 6, no. 2, pp. 211–222, Dec. 2018, doi: 10.18034/ei.v6i2.709.

[31] R. Bishukarma, Adaptive AI-Based Anomaly Detection Framework for SaaS Platform Security, *Int. J. Curr. Eng. Technol.*, vol. 12, no. 07, pp. 541–548, 2022, doi: https://doi.org/10.14741/ijcet/v.12.6.8.

[32] R. Bishukarma, The Role of AI in Automated Testing and Monitoring in SaaS Environments, *Int. J. Res. Anal. Rev.*, vol. 8, no. 2, pp. 846–852, 2021, [Online]. Available: https://www.ijrar.org/papers/IJRAR21B2597.pdf

[33] S. C. R. V. Bhavik Patel, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, Kishore Mullangi, Advancements in 5G Technology: Enhancing Connectivity and Performance in Communication Engineering, *Eng. Int.*, vol. 10, no. 2, pp. 117–130, 2022, [Online]. Available:

https://scholar.google.com/citations?view_op=view_citation&hl=en&user=kl24IcEAAAAJ&citation_for_view=kl24IcEAAAAJ:zYLM7Y9cAGgC

[34] V. V. Kumar, F. T. S. Chan, N. Mishra, and V. Kumar, Environmental integrated closed loop logistics model: An artificial bee colony approach, in *SCMIS 2010 - Proceedings of 2010 8th International Conference on Supply Chain Management and Information Systems: Logistics Systems and Engineering*, 2010.

[35] K. Patel, Quality Assurance In The Age Of Data Analytics: Innovations And Challenges, *Int. J. Creat. Res. Thoughts*, vol. 9, no. 12, pp. f573–f578, 2021.

[36] R. P. Vamsi Krishna Yarlagadda, Secure Programming with SAS: Mitigating Risks and Protecting Data Integrity, *Eng. Int.*, vol. 6, no. 2, pp. 211–222, 2018, doi: 10.18034/ei.v7i2.711.

[37] M. R. Kishore Mullangi, Vamsi Krishna Yarlagadda, Niravkumar Dhameliya, Integrating AI and Reciprocal Symmetry in Financial Management: A Pathway to Enhanced Decision-Making, *Int. J. Reciprocal Symmetry Theor. Phys.*, vol. 5, no. 1, pp. 42–52, 2018.

[38] A. P. A. Singh, Strategic Approaches To Materials Data Collection And Inventory Management, *Int. J. Bus. Quant. Econ. Appl. Manag. Res.*, vol. 7, no. 5, 2022.

[39] S. A. and A. Tewari, Security Vulnerabilities in Edge Computing: A Comprehensive Review, *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 936–941, 2022, [Online]. Available: https://www.ijrar.org/papers/IJRAR22D3205.pdf

[40] M. M. Potey, C. A. Dhote, and D. H. Sharma, Homomorphic Encryption for Security of Cloud Data, in *Procedia Computer Science*, 2016. doi: 10.1016/j.procs.2016.03.023.

[41] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, Assessment and improvement of intelligent controllers for elevator energy efficiency, in *IEEE International Conference on Electro Information Technology*, 2012. doi: 10.1109/EIT.2012.6220727.

[42] M. Z. Hasan, R. Fink, M. R. Suyambu, and M. K. Baskaran, Assessment and improvement of elevator controllers for energy efficiency, in *Digest of Technical Papers - IEEE International Conference on Consumer Electronics*, 2012. doi: 10.1109/ISCE.2012.6241747.

[43] M. N. Alenezi, H. Alabdulrazzaq, and N. Q. Mohammad, Symmetric encryption algorithms: Review and evaluation study, *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 2, pp. 256–272, 2020.

[44] M. Z. Hasan, R. Fink, M. R. Suyambu, M. K. Baskaran, D. James, and J. Gamboa, Performance evaluation of energy efficient intelligent elevator controllers, in *IEEE International Conference on Electro Information Technology*, 2015. doi: 10.1109/EIT.2015.7293320.

[45] M. R. S. and P. K. Vishwakarma, An Efficient Machine Learning Based Solutions for Renewable Energy System, *Int. J. Res. Anal. Rev.*, vol. 9, no. 4, pp. 951–958, 2022, [Online]. Available: https://www.ijrar.org/papers/IJRAR22D3208.pdf

[46] M. Ubaidullah and Q. Makki, A Review on Symmetric Key Encryption Techniques in Cryptography, *Int. J. Comput. Appl.*, 2016, doi: 10.5120/ijca2016911203.

[47] M. Bellare, K. G. Paterson, and P. Rogaway, Security of symmetric encryption against mass surveillance, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014. doi: 10.1007/978-3-662-44371-2_1.

[48] A. P. A. Singh, Streamlining Purchase Requisitions and Orders : A Guide to Effective Goods Receipt Management, *J. Emerg. Technol. Innov. Res.*, vol. 8, no. 5, pp. g179–g184, 2021.

[49] P. P. Santoso *et al.*, Systematic literature review: Comparison study of symmetric key and asymmetric key algorithm, *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, 2018, doi: 10.1088/1757-899X/420/1/012111.

[50] S. Chandra, S. Paira, S. S. Alam, and G. Sanyal, A comparative survey of symmetric and asymmetric key cryptography, in *2014 International Conference on Electronics, Communication and Computational Engineering, ICECCE 2014*, 2014. doi: 10.1109/ICECCE.2014.7086640.

[51] V. Biksham and D. Vasumathi, Homomorphic Encryption Techniques for securing Data in Cloud Computing: A Survey, *Int. J. Comput. Appl.*, vol. 160, no. 6, pp. 1–5, 2017, doi: 10.5120/ijca2017913063.

[52] C. Gentry, Fully Homomorphic Encryption Using Ideal Lattices, in *Proceedings of the Annual ACM Symposium on Theory of Computing*, 2009. doi: 10.1145/1536414.1536440.

[53] M. T. VISHWA VIJAY Kumar, MUKUL Tripathi, SATISH KUMAR Tyagi, SK Shukla, An integrated real time optimization approach (IRTO) for physical programming based redundancy allocation problem, *Proc. 3rd Int. Conf. Reliab. Saf. Eng. Udaypur, Rajasthan, India*, pp. 692–704, 2007.

[54] J. Zhou, Y. Feng, Z. Wang, and D. Guo, Using secure multi-party computation to protect privacy on a permissioned blockchain, *Sensors*, 2021, doi: 10.3390/s21041540.

[55] D. Das, Secure cloud computing algorithm using homomorphic encryption and multi-party computation, in *International Conference on Information Networking*, 2018. doi: 10.1109/ICOIN.2018.8343147.

[56] Pronika and S. S. Tyagi, Secure data storage in cloud using encryption algorithm, in *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, 2021. doi: 10.1109/ICICV50876.2021.9388388.

[57] R. S. Patil and P. Biradar, Secure Parallel Processing on Encrypted Cloud Data Using Fully Homomorphic Encryption, in *Proceedings of the 4th International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2018*, 2018. doi: 10.1109/iCATccT44854.2018.9001284.

[58] R. Joseph Manoj, A. Alsadoon, P. W. C. Prasad, N. Costadopoulos, and S. Ali, Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud, in *Proceedings - 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2017*, 2017. doi: 10.1109/MobileCloud.2017.38.

[59] A. Al Azzani and A. Alkalbani, Optimal Solution for Data Storage Security in Cloud Computing (OSDSS-CC), in *2022 IEEE 8th International Conference on Computing, Engineering and Design, ICCED 2022*, 2022. doi: 10.1109/ICCED56140.2022.10010354.

[60] M. Suganya and T. Sasipraba, Security and Privacy-Efficient Encryption Algorithm for Cloud Data Using Genetic Prime Crossover Technique, in *2022 1st International Conference on Computational Science and Technology, ICCST 2022 - Proceedings*, 2022. doi: 10.1109/ICCST55948.2022.10040375.