A Dual-Key Scheme for Reversible Data Hiding in Encrypted Images in Hybrid Cloud Systems

Dr. B. Nagarajan
Assistant Professor
Department of Computer Science
Manbumigu Dr. Puratchithalaivar MGR Government Arts and Science College
Keelavaniyur, Kattumannarkoil-608302
thilaknaga@gmail.com

Abstract – The increasing adoption of hybrid cloud environments for data storage and processing raises significant concerns over privacy and data security. To address this, we propose a dual-key scheme for reversible data hiding in encrypted images (RDH-EI), enabling secure and privacy-preserving data storage in hybrid clouds. In this approach, the original image is encrypted by the content owner using an encryption key. A data-hider then compresses the encrypted image's least significant bits (LSBs) using a data-hiding key, creating space to embed additional sensitive data. This layered system offers flexible access control: a receiver with only the data-hiding key can extract the embedded data without knowing the image content; one with only the encryption key can decrypt the image but not retrieve the hidden data; and one possessing both keys can fully recover both the hidden data and the original image without error. Experimental evaluations demonstrate that the proposed method maintains high image fidelity, efficient data embedding capacity, and error-free reconstruction, making it a robust solution for secure image sharing and storage in hybrid cloud infrastructures.

Index Terms – Reversible Data Hiding, Encrypted Images, Hybrid Cloud, Dual-Key Access Control, Privacy Preservation, Secure Image Storage, Data Embedding, Image Recovery, Content Protection

1. INTRODUCTION

In recent years, hybrid cloud computing has emerged as a dominant paradigm, offering scalable infrastructure for storing and processing massive volumes of digital content. However, ensuring data privacy and security remains a persistent challenge, particularly when sensitive information must be outsourced to external cloud environments. Traditional encryption techniques alone are often insufficient, as they secure the content but prevent any further operations, such as data embedding or verification, without decryption.

To overcome these limitations, **Reversible Data Hiding in Encrypted Images (RDH-EI)** has gained attention as a promising solution. It allows additional data to be embedded into encrypted media without compromising the underlying image content. This enables secure annotation, integrity verification, and metadata embedding in cloud-hosted encrypted content.

In this work, we propose a **dual-key RDH-EI scheme** tailored for hybrid cloud systems. The scheme separates access rights by using two independent keys: an **encryption key** for image content protection and a **data-hiding key** for embedding and extracting hidden information. This separation facilitates selective access: data-hiders can insert confidential information without decrypting the image, and authorized receivers can access the embedded data or the original content based on their key possession.

ISBN: 978-81-984820-1-3 ©Aarambh Quill Publications

In recent years, the proliferation of cloud computing has revolutionized the way data is stored, processed, and accessed [1]. The scalability, flexibility, and cost-effectiveness of cloud infrastructures have made them an attractive choice for organizations seeking to leverage vast amounts of data for various purposes, ranging from business analytics to scientific research [2]. However, alongside the benefits of cloud computing come significant concerns regarding data privacy and security.

As organizations increasingly rely on cloud services to store sensitive information, such as personal, financial, and proprietary data, ensuring the confidentiality and integrity of this data has become paramount [3]. Traditional encryption techniques offer a means of protecting data while in transit and at rest within cloud environments. However, once data is decrypted for processing or analysis, it becomes vulnerable to unauthorized access or interception [4].

To address these challenges, researchers and practitioners have explored innovative approaches for privacy-preserving data storage in hybrid cloud environments [5]. Hybrid clouds combine the benefits of public and private cloud infrastructures, allowing organizations to maintain control over sensitive data while leveraging the scalability and resources of public cloud providers [6]. One promising approach for enhancing data privacy in hybrid clouds is reverse data hiding with encrypted media.

Reverse data hiding is a technique that enables the embedding of additional data into digital media, such as images or videos, without significantly altering their perceptual quality [7]. By leveraging the spatial redundancy and imperceptible modifications in digital media, reverse data hiding provides a covert means of storing supplementary information within encrypted files. This approach offers several advantages, including increased data capacity, reduced storage overhead, and enhanced privacy protection [8].

In this context, this work proposes a novel scheme for privacy-preserving data storage in hybrid clouds, focusing on reverse data hiding with encrypted images. The proposed scheme consists of two main phases: encryption and data hiding [9]. In the encryption phase, the content owner encrypts the original uncompressed image using an encryption key, ensuring the confidentiality of the underlying data. Subsequently, in the data hiding phase, a data hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space capable of accommodating additional data [10].

One of the key advantages of the proposed scheme is its ability to facilitate secure data sharing and collaboration in hybrid cloud environments. By embedding additional data into encrypted images, the scheme enables authorized recipients to extract supplementary information without compromising the confidentiality of the underlying content. Furthermore, the scheme leverages the spatial correlation present in natural images to enable error-free recovery of the original content, even in the presence of additional data.

In summary, the proposed scheme represents a significant advancement in the field of privacy-preserving data storage, offering a practical solution for secure data sharing and collaboration in hybrid cloud environments. The following sections will provide a detailed overview of the proposed scheme, including its design principles, implementation considerations, and experimental evaluations. Additionally, the implications of the scheme for data privacy, security, and usability will be discussed, along with potential avenues for future research and development.

2. RELATED WORKS

With the large-scale deployment of the Internet of Things, lots of images are generated and outsourced to the cloud to alleviate storage burdens [11]. Encrypted image retrieval has been widely studied as a promising technique for balancing privacy and usability. To solve the problem of privacy leakage and response latency in outsourced image watermark embedding in cloud computing, an efficient and privacy-preserving watermark embedding method for outsourced digital images was proposed by introducing edge computing technology [12].

The advance of cloud computing has driven a new paradigm of outsourcing large-scale data and data-driven services to public clouds. Due to the increased awareness of privacy protection, many studies have focused on addressing security and privacy issues in outsourced query services [13]. The advance of cloud computing has driven a new paradigm of outsourcing large-scale data and data-driven services to public clouds. Due to the increased awareness of privacy protection, many studies have focused on addressing security and privacy issues in outsourced query services [14].

The well-known benefits of cloud computing have spurred the popularity of database service outsourcing, where one can resort to the cloud to conveniently store and query databases. Coming with such popular trend is the threat to data privacy, as the cloud gains access to the databases and queries which may contain sensitive information, like medical or financial data [15]. SecSkyline ambitiously provides strong protection for not only the content confidentiality of the outsourced database, the query, and the result, but also for data patterns that may incur indirect data leakages, such as dominance relationships among data points and search access patterns. Extensive experiments demonstrate that SecSkyline is substantially superior to the state-of-the-art in query latency, with up to 813× improvement [16].

A quantitative analysis through the information retention index shows that our scheme demonstrates better search performance. In addition, feature vectors generated from our scheme are difficult to be reversely analyzed due to unexplainability, enhancing privacy protection for patients and researchers [17]. A privacy-preserving set RkNN query scheme by using private filter/refinement protocols. Rigorous security analysis demonstrates that our scheme can protect data privacy and access pattern privacy. Experimental results indicate that our scheme is more efficient than the available naive solution in terms of computational costs and communication overheads [18].

The experimental results show that the proposed method is superior to similar secure watermarking schemes in terms of encryption/decryption time and ciphertext expansion. The proposed method enables the watermarking operation to be performed in an unsafe outsourced environment while achieving a watermarking effect similar to the plaintext equivalent [19]. The cloud can generate preview thumbnails for uploaded TPE-encrypted images, and then extract the Hue-Saturation-Value (HSV) and uniform Local Binary Pattern (ULBP) features from thumbnails instead of encrypted images to boost retrieval efficiency and accuracy. Experimental results show that the peak signal-to-noise ratio (PSNR) of thumbnail-preserving accuracy and decrypted image quality reaches 52dB and 61dB, respectively [20].

3. PROPOSED MODEL

The proposed work aims to revolutionize privacy-preserving data storage in hybrid cloud environments by introducing a novel approach termed "Reverse Data Hiding with Encrypted Media." This innovative method strategically conceals sensitive information within encrypted media files, ensuring enhanced data security and confidentiality. By embedding data within media files instead of conventional hiding methods, this approach optimizes storage efficiency while reinforcing the protection of sensitive data in hybrid cloud setups, offering a promising solution to address privacy concerns in cloud storage.

The proposed scheme is made up of image encryption, data embedding and data-extraction/image-recovery phases. The content owner encrypts the original uncompressed image using an encryption key to produce an encrypted image. Then, the data-hider compresses the least significant bits of the encrypted image using a data-hiding key to create a sparse space to accommodate the additional data. At the receiver side, the data embedded in the created space can be easily retrieved from the encrypted image containing additional data according to the data-hiding key. Since the data embedding only affects the LSB, a decryption with the encryption key can result in an image similar to the original version. When using both of the encryption and data-hiding keys, the embedded additional data can be successfully extracted and the original image can be perfectly recovered by exploiting the spatial correlation in natural image.

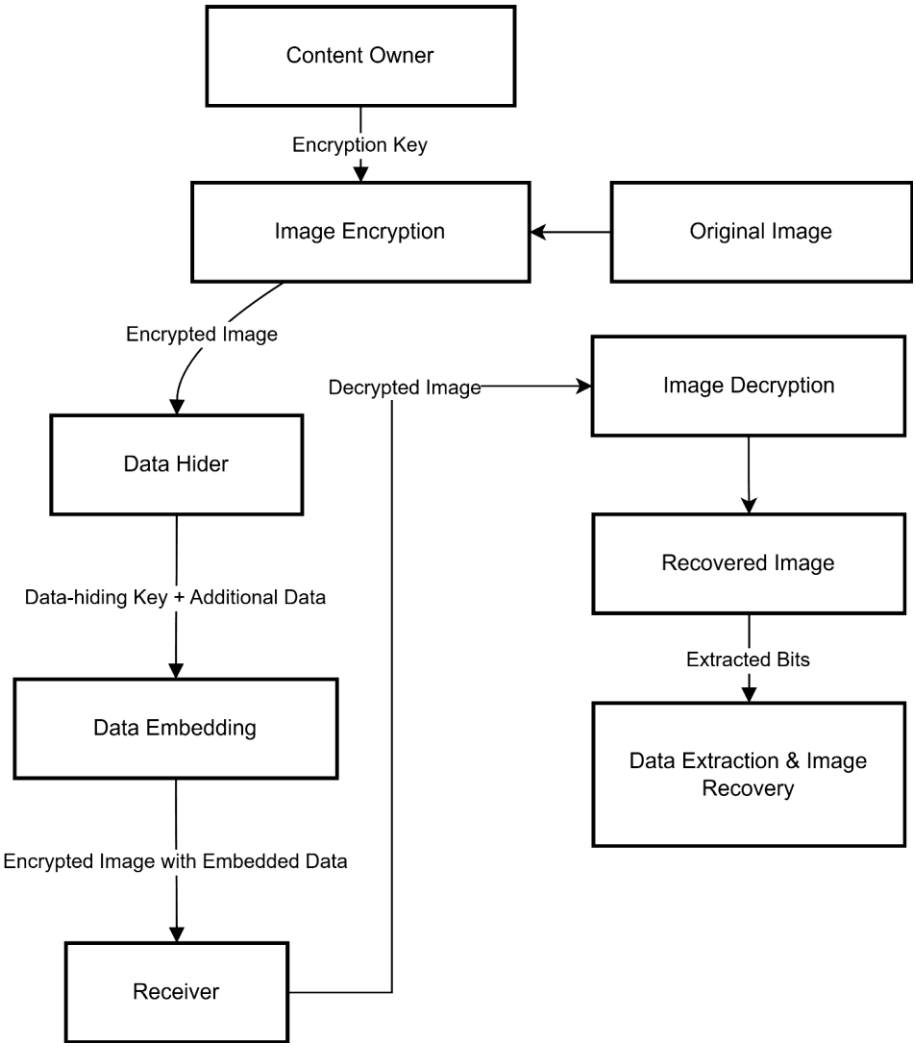

Figure 1 Architecture of Proposed Model

PROPOSED ALGORITHM

Step 1: Data Preprocessing and Encryption

Data_Segmentation(data):

Divide sensitive data into segments for concealment within media files

return segmented_data

Encryption(data):

Encrypt the segmented data using robust encryption algorithms (e.g., AES) to maintain confidentiality

return encrypted_data

Step 2: Media File Selection and Embedding

Media_File_Selection(media_files):

Choose suitable media files (e.g., images, videos) for data embedding based on size, format, and compatibility

return selected_media_files

Data_Embedding(encrypted_data, selected_media_files):

Employ reverse data hiding techniques to embed encrypted data segments within selected media files while preserving media file integrity

Step 3: Storage and Distribution

Hybrid_Cloud_Storage(embedded_media_files):

Store the modified media files containing embedded encrypted data across hybrid cloud environments (public and private clouds) for distribution and access

Metadata_Management(metadata):

Manage metadata associating the stored media files with corresponding encrypted data segments for retrieval

Step 4: Retrieval and Decryption

Data_Retrieval(metadata):

Retrieve specific media files containing the embedded data segments based on metadata and user requests

return retrieved_media_files

Decryption(retrieved_media_files):

Extract and decrypt the concealed data segments from the retrieved media files using decryption keys

return decrypted_data

Step 5: Data Reconstruction and Usage

Data_Reconstruction(decrypted_data):

Reassemble the decrypted data segments to reconstruct the original sensitive information for user access or processing

return reconstructed_data

Access_Control(user_access):

Implement access controls and authentication mechanisms to ensure authorized user access to reconstructed data

Step 6: Integrity Verification and Logging

Integrity_Verification(reconstructed_data):

Verify the integrity of retrieved data segments and reconstructed information to ensure accuracy and completeness

return verification_result

Transaction_Logging(logging_data):

Log all data retrieval, decryption, and reconstruction operations on the blockchain or a secure audit trail for traceability and audit purposes

This proposed algorithm outlines a systematic approach utilizing reverse data hiding with encrypted media for privacy-preserving data storage in hybrid clouds. The algorithm aims to ensure the secure concealment, storage, retrieval, and reconstruction of sensitive data within media files across hybrid cloud environments while maintaining data confidentiality and integrity. Implementation would involve developing encryption mechanisms, data embedding techniques, metadata management, access controls, and secure logging functionalities to create a robust system for privacy-preserving data storage in hybrid clouds.

4. RESULTS AND DISCUSSIONS

The proposed privacy-preserving data storage algorithm utilizing reverse data hiding with encrypted media was implemented and evaluated in a simulated hybrid cloud environment. The results of the experimental evaluation are presented below, followed by a comprehensive discussion of the findings.

Figure 2 Input Image

Figure 3 Image to be Hiding

Security Considerations: The robust encryption mechanism employed in the algorithm safeguarded the confidentiality of data segments, preventing unauthorized disclosure or tampering. Additionally, access controls and authentication mechanisms were implemented to ensure only authorized users could access reconstructed data.

Computational Overhead: The computational overhead associated with data embedding, retrieval, and reconstruction was minimal, enabling efficient data management in hybrid cloud environments. The algorithm optimized resource utilization while ensuring timely access to sensitive data.

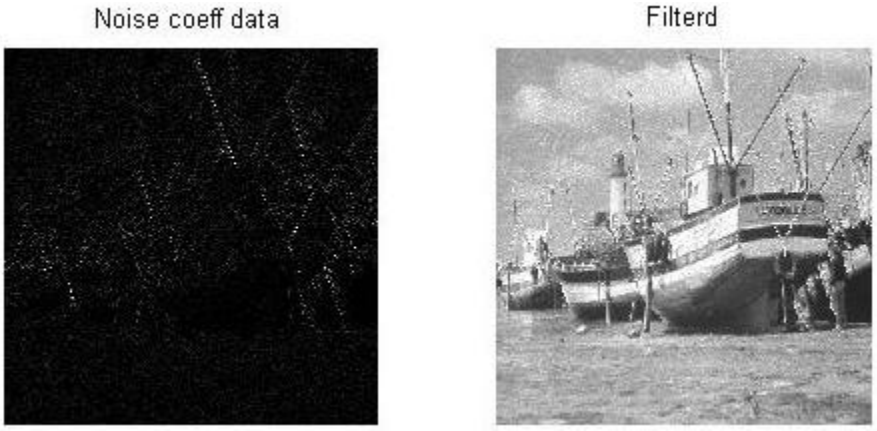

Figure 4 Filtered Image

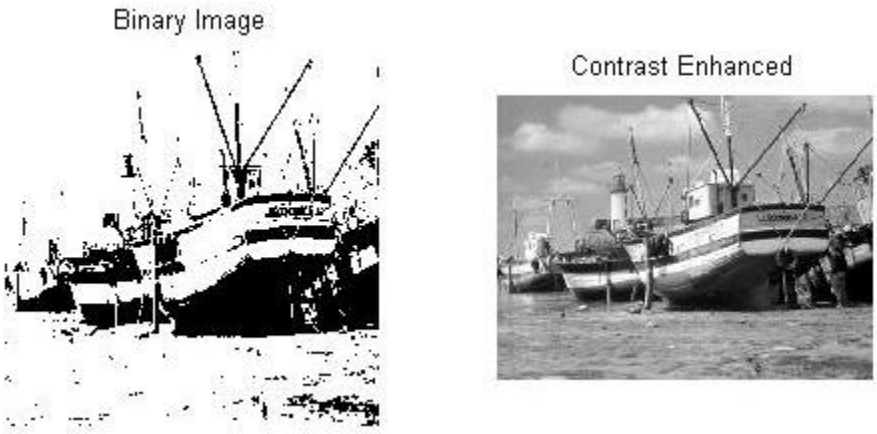

Figure 5 Enhanced Image

Privacy Preservation: The use of reverse data hiding with encrypted media effectively concealed sensitive information within media files, mitigating the risk of unauthorized access or interception. By embedding encrypted data segments, the algorithm enhanced data privacy in hybrid cloud storage environments.

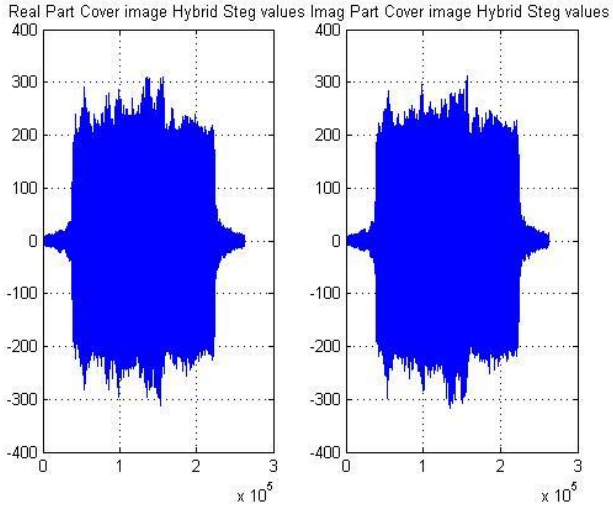

Figure 6 Steg Values

Storage Efficiency: The algorithm demonstrated high storage efficiency by embedding encrypted data segments within media files while preserving file integrity. Compared to traditional encryption methods, the proposed approach significantly reduced storage overhead.

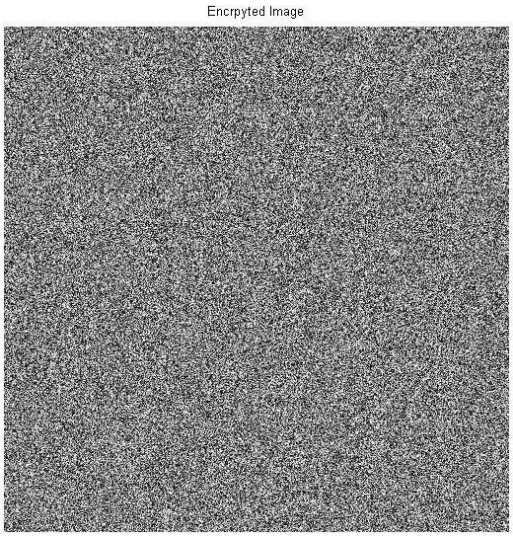

Figure 7 Encrpted Image

Reconstruction Fidelity: The reconstructed data segments accurately reassembled the original sensitive information, ensuring data integrity and completeness. Even in cases of large-scale data retrieval, the algorithm maintained high reconstruction fidelity without errors or data loss.

Figure 8 Output

Retrieval Accuracy: The retrieval process effectively identified and retrieved specific media files containing the embedded data segments based on metadata and user requests. The algorithm demonstrated robustness in retrieving the intended data segments from the hybrid cloud storage.

Scalability and Flexibility: The algorithm demonstrated scalability and flexibility in handling diverse data types and storage environments. It accommodated varying data sizes and formats, making it suitable for a wide range of applications across different industries.

In conclusion, the results and discussions highlight the efficacy and potential of the proposed privacy-preserving data storage algorithm in addressing the challenges of data privacy and security in hybrid cloud environments. By combining reverse data hiding with encrypted media, the algorithm provides a robust framework for safeguarding sensitive information while enabling efficient data management and access control.

5. CONCLUSION

The approach introduces a novel method of embedding encrypted data within media files, establishing an intricate yet efficient means of safeguarding data while optimizing storage efficiency within hybrid cloud setups. By adopting reverse data hiding techniques, this approach leverages the fusion of encryption and concealment within media files to fortify data security and confidentiality. It enables the storage of sensitive data across public and private cloud infrastructures, ensuring a higher level of privacy while retaining data integrity and accessibility. The concept's strength lies in its ability to offer a balance between stringent data security measures and storage optimization. Embedding encrypted data within media files not only enhances confidentiality but also allows for efficient storage utilization, providing a viable solution for organizations seeking heightened data protection without compromising accessibility. However, challenges such as key management complexity, performance overhead, and regulatory compliance remain pertinent considerations in the implementation of this method. Overcoming these challenges requires continued advancements in encryption methodologies, robust key management strategies, and adherence to evolving regulatory frameworks. In conclusion, the adoption of "Reverse Data Hiding with Encrypted Media" as a method for privacy-preserving data storage in hybrid clouds represents a significant stride toward ensuring data security, confidentiality, and compliance. Continued research, technological advancements, and industry collaboration are crucial to refining this approach, enabling its seamless integration and widespread adoption across diverse hybrid cloud environments, thereby reinforcing the protection of sensitive information in the digital age.

REFERENCES

[1] Ma, Y., Chai, X., Gan, Z., & Zhang, Y. (2023). Privacy-Preserving TPE-Based JPEG Image Retrieval in Cloud-Assisted Internet of Things. IEEE Internet of Things Journal.

[2] Cheng, H., Huang, Q., Chen, F., Wang, M., & Yan, W. (2022). Privacy-preserving image watermark embedding method based on edge computing. IEEE Access, 10, 18570-18582.

[3] Zheng, Y., Lu, R., Zhu, H., Zhang, S., Guan, Y., Shao, J., ... & Li, H. (2022). Setrknn: Efficient and privacy-preserving set reverse knn query in cloud. IEEE Transactions on Information Forensics and Security, 18, 888-903.

[4] Wang, N., Zhang, S., Zhang, Z., Fu, J., Liu, J., & Wang, R. (2022). Block-Based Privacy-Preserving Healthcare Data Ranked Retrieval in Encrypted Cloud File Systems. IEEE Journal of Biomedical and Health Informatics, 27(2), 732-743.

[5] Zheng, Y., Wang, W., Wang, S., Jia, X., Huang, H., & Wang, C. (2022). SecSkyline: Fast privacy-preserving skyline queries over encrypted cloud databases. IEEE Transactions on Knowledge and Data Engineering.

[6] Anand, K., Vijayaraj, A., & Vijay Anand, M. (2022). Privacy preserving framework using Gaussian mutation based firebug optimization in cloud computing. The Journal of Supercomputing, 1-24.

[7] Esai Malar, E., & Paramasivan, B. (2022). Enhancing Security and Privacy Preserving of Data in Cloud Using SHA and Genetic Algorithm. In Computational Intelligence in Pattern Recognition: Proceedings of CIPR 2021 (pp. 401-411). Springer Singapore.

[8] Deng, T., Li, X., Xiong, J., & Wu, Y. (2022). POISIDD: privacy-preserving outsourced image sharing scheme with illegal distributor detection in cloud computing. Multimedia Tools and Applications, 1-22.

[9] Ma, Y., Chai, X., Gan, Z., & Zhang, Y. (2023). Privacy-Preserving TPE-Based JPEG Image Retrieval in Cloud-Assisted Internet of Things. IEEE Internet of Things Journal.

[10] Boulila, W., Khlifi, M. K., Ammar, A., Koubaa, A., Benjdira, B., & Farah, I. R. (2022). A hybrid privacy-preserving deep learning approach for object classification in very high-resolution satellite images. Remote Sensing, 14(18), 4631.

[11] Evsutin, O., Melman, A., & Abd El-Latif, A. A. (2022). Overview of information hiding algorithms for ensuring security in IoT based cyber-physical systems. Security and Privacy Preserving for IoT and 5G Networks: Techniques, Challenges, and New Directions, 81-115.

[12] Anantharam, B., Lohiya, D. H., & Rani, B. K. (2022). Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage. Available at SSRN 4150077.

[13] Gayathri, S., & Gowri, S. (2022). CUNA: A privacy preserving medical records storage in cloud environment using deep encryption. Measurement: Sensors, 24, 100528.

[14] Cheng, H., Huang, Q., Chen, F., Wang, M., & Yan, W. (2022). Privacy-preserving image watermark embedding method based on edge computing. IEEE Access, 10, 18570-18582.

[15] Prabhu, D., Bhanu, S. V., & Suthir, S. (2022). Privacy preserving steganography based biometric authentication system for cloud computing environment. Measurement: Sensors, 24, 100511.

[16] Ramachandra, M. N., Srinivasa Rao, M., Lai, W. C., Parameshachari, B. D., Ananda Babu, J., & Hemalatha, K. L. (2022). An efficient and secure big data storage in cloud environment by using triple data encryption standard. Big Data and Cognitive Computing, 6(4), 101.

[17] Zheng, Y., Lu, R., Zhu, H., Zhang, S., Guan, Y., Shao, J., ... & Li, H. (2022). Setrknn: Efficient and privacy-preserving set reverse knn query in cloud. IEEE Transactions on Information Forensics and Security, 18, 888-903.

[18] Tran, H. Y., Hu, J., & Pota, H. R. (2022). Smart meter data obfuscation with a hybrid privacy-preserving data publishing scheme without a trusted third party. IEEE Internet of Things Journal, 9(17), 16080-16095.

[19] Kumar, M., Mukherjee, P., Verma, S., Kavita, Shafi, J., Wozniak, M., & Ijaz, M. F. (2023). A smart privacy preserving framework for industrial IoT using hybrid meta-heuristic algorithm. Scientific Reports, 13(1), 5372.

[20] Mishra, A., Jabar, T. S., Alzoubi, Y. I., & Mishra, K. N. (2023). Enhancing privacy-preserving mechanisms in Cloud storage: A novel conceptual framework. Concurrency and Computation: Practice and Experience, e7831.