International Journal of Research, Education, and Innovation (IJREI)
Volume 1, Issue 4, November. 2024, pp.1-5

Watermarking Approaches for Strengthening Cloud Data Security: A Review

[1]Ghorpade Mahesh Sanjay, [2]Mr. Jeetendra Singh Yadav

[1]M. Tech., Scholar, maheshghorpade89@gmail.com, CSE Department RKDFCE, Bhopal, India

[2]Assis. Prof., jeetendra2201@gmail.com, RKDFCE, Bhopal, India

Abstract- *Cloud computing has revolutionized data storage and management, offering scalable solutions to businesses and individuals. However, with the increasing reliance on cloud services, data security remains a critical concern. Traditional security measures like encryption and access controls are often insufficient to protect sensitive data from unauthorized access or tampering. Watermarking techniques have emerged as a promising solution to address these challenges, providing an additional layer of protection to cloud data. This paper presents a comprehensive review of watermarking approaches for enhancing cloud data security. It explores various types of watermarking techniques, including fragile, robust, and semi-fragile watermarking, highlighting their applications, advantages, and limitations in cloud environments. The paper also discusses the integration of watermarking with other security mechanisms, such as encryption and access control, to provide multi-faceted protection. Furthermore, it examines the challenges faced in implementing watermarking techniques in cloud computing, such as computational overhead, scalability, and resilience against attacks. Finally, future research directions and potential improvements in watermarking for cloud data security are discussed, emphasizing the need for more efficient, secure, and adaptable watermarking solutions. This review aims to provide a comprehensive understanding of the current state-of-the-art in watermarking techniques and their role in strengthening the security of cloud-based data storage and transmission.*

Keyword: Cloud computing, data security, watermarking techniques, fragile watermarking, robust watermarking, semi-fragile watermarking, encryption, access control, multi-faceted protection, scalability

1. INTRODUCTION

The Cloud computing has become a cornerstone of modern digital infrastructure, enabling organizations and individuals to store, manage, and process vast amounts of data with flexibility, scalability, and cost efficiency. However, as data is increasingly migrated to the cloud, concerns regarding the security, integrity, and confidentiality of cloud-stored information have also grown. Cloud environments, by nature, expose data to various risks, such as unauthorized access, data tampering, and malicious attacks, making data protection a primary challenge for cloud service providers and users alike.

While traditional security measures such as encryption, access controls, and authentication are essential in safeguarding cloud data, these techniques often focus on confidentiality and access restriction but do not always guarantee data integrity or traceability. To address these gaps, watermarking has emerged as a promising security technique in the cloud computing domain. Watermarking involves embedding a unique, invisible marker (or watermark) within the data, which can be used for data authentication, ownership verification, and tamper detection. Unlike encryption, watermarking does not alter the original content of the data but adds an extra layer of security by ensuring that the authenticity and integrity of the data can be verified at any point.

This paper provides an in-depth review of watermarking approaches that strengthen cloud data security. The primary objective of this paper is to explore various watermarking techniques, including

fragile, robust, and semi-fragile watermarking, and examine their effectiveness in protecting data stored and transmitted over cloud environments. Additionally, the integration of watermarking with other security mechanisms, such as encryption and access control, is discussed to provide a comprehensive security framework for cloud data. The paper also addresses the challenges in implementing watermarking in the cloud, such as computational overhead, scalability issues, and vulnerabilities to attacks. Finally, we outline future research directions that could help overcome these challenges and improve the applicability and performance of watermarking techniques in cloud computing environments.

By investigating the potential of watermarking for enhancing cloud data security, this paper aims to contribute to the development of more robust and adaptable security strategies for cloud-based systems.

II. LITERATURE SURVEY

S.K. Sahoo et al. (2023) study explores the various cloud computing services and examines how watermarking techniques can enhance security. It discusses how watermarking can improve the protection of data stored in the cloud, ensuring greater security for cloud-based information. Cloud computing distributes data across numerous virtual servers, enabling users from various locations to connect with cloud service providers. This model eliminates the need for users to upgrade their systems or establish complex infrastructure to access cloud services [1].

Neha Khajanchi et al. (2019) studies on cloud computing offers a flexible data outsourcing solution that alleviates users from the challenges of local storage management. However, a major concern is ensuring secure and reliable data archiving amidst potentially unreliable service providers. This paper addresses the application of watermarking technology for copyright protection within cloud computing environments. It employs GLCM (Gray-Level Co-occurrence Matrix) and PCA (Principal Component Analysis) algorithms to extract features from the original image and generate a semi-blind watermarking image. The integration of digital watermarking with cloud computing can significantly enhance the robustness and security of the system, ensuring the protection of users' data [2].

Amrit Anil et al. (2020) paper explores the advantages of cloud computing and cloud storage, highlighting their cost flexibility and security features. It also examines data security and the associated threats. Additionally, the paper discusses watermarking and how digital watermarking can be employed to enhance data security. Knowledge has the potential to provide significant leverage, particularly when used with malicious intent. With the rise of the internet, data production has reached unprecedented levels, surpassing the total number of humans who have ever lived. Given this vast volume of data, it is crucial to ensure its security, as any stolen or misused data can have widespread repercussions. Cloud computing has become a key solution for managing this data influx, offering both scalability and enhanced security measures to protect against leaks. Nevertheless, achieving complete security remains challenging due to the rapid evolution of technology and the increasingly sophisticated methods used by hackers to gain unauthorized access. The best approach to mitigating data breaches involves continually updating existing security policies and incorporating new security techniques [3].

Alaa Abdulsalam Alarood et al. (2022) studies on the effectiveness of the watermarking technique by applying it to digital images. It measures the correlation coefficient between the watermarked and original images, as well as various metrics such as Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), and Mean Squared Error (MSE). The implementation of both invisible watermarking using the Least Significant Bit (LSB) algorithm and visible watermarking is discussed. The research further examines various security issues related to image watermarking and assesses the impact of multiple attacks on the quality of watermarked images. The experiments demonstrate that the proposed embedding process, particularly with the LSB algorithm, enhances embedding efficiency by avoiding the need to modify all bits, thus improving the overall effectiveness of the watermarking technique. The internet revolution has dramatically transformed multimedia applications, enhancing the speed and accuracy of data and image transfers. However, these advancements have also made it easier for valuable information to be modified or misused through hacking. To combat these issues,

digital watermarking has been proposed as a solution to protect multimedia data copyrights. By embedding a watermark—whether in the form of an image, text, or other content—within the digital data, copyright and confidentiality can be safeguarded, allowing secure transmission without revealing the content to unauthorized third parties. This research presents a method for hiding data, specifically a text file, by first encrypting it using the Keyword Mixed Transposition technique to produce ciphertext. This encrypted data is then embedded into an image using a Low-High coefficient wavelet transform. The resulting image maintains high quality while allowing the full recovery and decoding of the embedded message without needing the original image [4].

Shakun Gupta et al. (2020) study introduces the use of the Kalman filter in conjunction with SVD-DCT-DWT techniques to improve the PSNR and MSE values of the extracted watermarked images. The Kalman filter enhances the overall performance of the watermarking process, ensuring better quality and security of the watermarked data in cloud computing environments. Cloud computing is a widely adopted technology with numerous benefits, but it faces significant challenges, particularly in security and privacy. This work addresses these concerns by implementing a watermarking technique to enhance data security. The proposed watermarking approach integrates Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) within the cloud architecture. To evaluate the robustness of the watermarked data, various attacks—such as sharpened attack, contrast attack, and salt & pepper attack—were applied. The performance of the watermarking technique was assessed using metrics like Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) [5].

Padmini Devi B et al. (2023) study on approach combines watermarking with proxy re-encryption to facilitate the secure exchange of multimedia content. In this method, a private key is encrypted using a specific encryption algorithm that requires a key, and this encrypted key is then merged with the user's private key. The resulting encrypted information is embedded into an image using the Least Significant Bit (LSB) technique. Once the confidential data is embedded, the image is further secured using Elliptic Curve Cryptography (ECC) encryption.While this approach enhances security, copyright protection remains a complex issue due to the rapid increase in internet usage and advancements in digital technology. Despite the implementation of advanced techniques, protecting intellectual property in the digital realm continues to pose significant challenges [6].

III. METHODOLOGY

The methodology of this review paper involves a systematic approach to analyzing and synthesizing various watermarking techniques used to enhance data security in cloud computing environments. The first step in the methodology was to conduct a comprehensive literature search across major academic databases such as IEEE Xplore, SpringerLink, and ScienceDirect. The search focused on keywords like "watermarking in cloud computing," "data security," "copyright protection," and "robust watermarking." Studies published between 2019 and 2023 were prioritized to include the most recent advancements in watermarking applications within cloud environments.

The selected studies were carefully chosen based on their relevance to cloud data security, specifically those that explored watermarking techniques for digital image protection, semi-blind watermarking, and watermarking combined with encryption methods. Each study was then categorized based on the type of watermarking technique employed, such as fragile, robust, and semi-fragile watermarking, allowing for a comparative analysis of different approaches. In fragile watermarking, the focus was on detecting any unauthorized changes or tampering of data, while robust watermarking techniques aimed to preserve the watermark's integrity despite common data modifications like compression or noise addition. Semi-fragile watermarking provided a balanced approach, combining aspects of both fragile and robust methods to ensure data integrity while allowing for some controlled alterations.

To assess the effectiveness of these watermarking techniques, the study employed several evaluation metrics, including security strength, data integrity, scalability, computational efficiency, and resilience to attacks. Security strength was measured by the watermark's ability to resist unauthorized removal or modification, while data integrity was evaluated by comparing the quality of watermarked data before and after embedding, using metrics like Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR).

Scalability was considered in the context of cloud environments, where the ability to manage large-scale data efficiently is crucial. Computational efficiency was assessed based on the processing time and storage overhead introduced by the watermarking process, and resilience to attacks was evaluated by testing the watermarked data against various threats such as compression, cropping, and malicious tampering.

Additionally, the review examined how watermarking techniques can be integrated with other cloud security mechanisms, such as encryption, access control, and data integrity verification, to provide a holistic security solution. Hybrid approaches, combining watermarking with encryption techniques, were given particular attention for their potential to enhance the overall security framework of cloud data. The paper also addressed the challenges and limitations associated with watermarking in cloud environments, including scalability issues in large cloud infrastructures, resistance to sophisticated attacks, and the computational overhead introduced by watermarking processes. Finally, the review identified gaps in the current research and suggested future directions, such as the development of adaptive watermarking algorithms and the integration of AI-driven watermarking solutions to improve efficiency and security in cloud computing environments.

IV. CONCLUSION

In conclusion, this review highlights the significant role of watermarking techniques in enhancing data security within cloud computing environments. The study demonstrates that watermarking offers a robust solution to safeguard data integrity, protect against unauthorized modifications, and ensure copyright protection in cloud-based storage systems. By examining various watermarking methods, such as fragile, robust, and semi-fragile techniques, this paper provides insights into how these approaches can be effectively implemented to address different security challenges in cloud environments.

The review also emphasizes the importance of integrating watermarking with other cloud security mechanisms, such as encryption and access control, to create a more comprehensive and resilient security framework. While watermarking has shown promise in improving data security, the study also identifies several challenges, including scalability issues, resistance to advanced attacks, and the potential computational overhead associated with watermarking processes. These challenges highlight the need for continued research and innovation in watermarking techniques to make them more efficient and adaptable to the evolving demands of cloud computing.

REFRENCES

[1] S.K. Sahoo, Mohammed Arif, P. Das,"Improving Cloud Data Security With Watermarking In Cloud Computing", 2023 IJCRT, Volume 11, Issue 5 May 2023, ISSN: 2320-2882.

[2] Neha Khajanchi, Prof. Vishakha Nagrale," To Apply Watermarking Technique in Cloud Computing To Enhance Cloud Data Security", Volume 4, Issue 7, July 2019 IJSDR.

[3] Amrit Anil; Vinod Kumar Shukla; Ved Prakash Mishra, "Enhancing Data Security Using Digital Watermarking", ISBN:978-1-7281-4098-8, 2020, IEEE, DOI: 10.1109/ICIEM48762.2020.9160090

[4] ALAA ABDULSALAM ALAROOD, "IMPROVE THE EFFICIENCY FOR EMBEDDING IN LSB METHOD BASED DIGITAL IMAGE WATERMARKING", August 2022. Vol.100. No 15, ISSN: 1992-8645, Journal of Theoretical and Applied Information Technology.

[5] Shakun Gupta , Harsimran Singh, "To Propose A Novel Technique for Watermarking In Cloud Computing", IJEDR - INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, Vol.3, Issue 2, page no.504-509, May 2015, Available :https://rjwave.org/IJEDR/papers/IJEDR1502094.pdf.

[6] Padmini Devi B; Deepak S; Abimanyu N K; Harish Kumar S, "Review On Prevention of Data Leakage in Cloud Server by Utilizing Watermarking and Double Encryption Techniques", ISSN: 2469-5556, 2023, IEEE, DOI: 10.1109/ICACCS57279.2023.10112767.

[7] Nagaram Ramesh, B. Nagaveni, P. Satyavathi, "An Efficient Technique to provide Security for Data Owners Cloud Computing", ISSN: 2278-0181, Vol. 1 Issue 5, July – 2012, International Journal of Engineering Research & Technology (IJERT).

[8] Sarvesh Kumar, Surendra Kumar, Nikhil Ranjan, Shivam Tiwari, T. Rajesh Kumar, Dinesh Goyal, Gajanand Sharma, Varsha Arya, Marjan Kuchaki Rafsanjani, "Digital Watermarking-Based Cryptosystem for Cloud Resource Provisioning", International Journal of Cloud Applications and Computing (IJCAC) 12(1), DOI: 10.4018/IJCAC.311033.

[9] Ching-Chun Chang; Chang-Tsun Li; Yun-Qing Shi, "Privacy-Aware Reversible Watermarking in Cloud Computing Environments", IEEE Access (Volume: 6), ISSN: 2169-3536, 2018, DOI: 10.1109/ACCESS.2018.2880904.

[10] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu, "Data Security and Privacy in Cloud Computing" Volume 10, Issue 7, July 2014, International Journal of Distributed Sensor Networks, DOI: https://doi.org/10.1155/2014/190903.

[11] Riya Naik; Manisha Naik Gaonkar, "Data Leakage Detection in cloud using Watermarking Technique", ISBN:978-1-5386-8260-9, 2019, IEEE, DOI: 10.1109/ICCCI.2019.8821894.

[12] Ashwani Kumar, "A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy preserving", Volume 81, pages 21417–21448, (2022), Springer.

[13] Swati Singh & Sarita Soni, "Security of Data with 3DES & Watermarking Algorithm", Volume: 4 Issue: 1, ISSN: 2454-4248, 2018, International Journal on Future Revolution in Computer Science & Communication Engineering.

[14]Samarth.K.N, Poornapragna.M.S, Sambhav Kumar.P.Jain, Nagarathna, "A Novel Technique Of Hiding An Audio Message In An Image", International Conference on Electronics and Communication Engineering, 28th April-2013, Bengaluru, ISBN: 978- 93-83060-04-7.

[15]Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade , "Image Steganography using Karhunen-Loève Transform and Least Bit Substitution", International Journal of Computer Applications ,Volume 79 – No9, October 2013, (0975 – 8887).

[16] K.Sakthisudan, P.Prabhu and P.thangaraj, "Secure Audio Steganography for hiding Secret Information", International Conference on recent trends in Computational methods, Communication and Controls (ICON3C 2012).

[17] Pritam Kumari, Chetna Kumar, Preeyanshi and jaya Bhushan, " Data Security Using Image steganography And Weighing Its Techniques", International Journal Of Scientific & Technology Research, Volume 2 ,Issue 11,November 2013. ISSN 2277-8616.

[18] Budda Lavanya, Yangala, Srinivasa Rao, " Data Hiding In Audio By Using Image Steganography Technique," International Journal Of Emerging Trends & Technology In Computer Science, Volume. 2, Issue 6, Nov-Dec 2013. ISSN: 2278-6856.

[19]Ankit Chadha, Neha Satam, Rakshak Sood, Dattatray Bade," An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution", International Journal of Computer Applications Volume 77– No.13, September 2013, ISSN:0975 – 8887.

[20] M.I.Khalil," Image Steganography: Hiding Short Audio Messages within Digital Images", JCS&T, Vol .11 No 2, October 2011.

[21] R.A.Jain, Hrushikesh B.Surve, Amit A.Sonar, Swpanil N.Salunke, "Secret Communication through Image and Audio for Defense", International Journal of Science and Modern Engineering (IJISME), Volume-1, Issue-5, April 2013, ISSN: 2319-6386.

[22]Samarth.K.N, Poornapragna.M.S, Sambhav Kumar.P.Jain, Nagarathna, "A Novel Technique Of Hiding An Audio Message In An Image", International Conference on Electronics and Communication Engineering, 28th April-2013, Bengaluru, ISBN: 978- 93-83060-04-7.