WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Secured Cloud Data Sharing: Privacy-Preserving Storage Optimization with Data Confidentiality

Mrinal [a]***, Ekta*** [b]

[a] *Assistant Professor, Department of Computer Science and Engineering, MERI College of Engineering and Technology, Haryana, India*
[b] *Assistant Professor, Department of Computer Science and Engineering, MERI College of Engineering and Technology, Haryana, India*

DOI: https://doi.org/10.55248/gengpi.4.823.51935

ABSTRACT

The present research presents an innovative access control system with the aim of enhancing privacy and optimizing cloud storage operations. The main aim of this framework is to provide cloud service providers an economically viable approach to ensuring the security, integrity, availability, and privacy of data, while also maintaining customer trust. The solution being presented focuses on implementing a strong authentication system that ensures the security of data both during its storage and transit inside cloud environments. The main goal of this framework is to enhance cost efficiency in storage while ensuring the preservation of data security and integrity.

The recommended methodology involves the compression of high-resolution photographs, leading to an estimated decrease of around 60% in the amount of data storage. The data that is in a fragmented state is then subjected to encryption using a proprietary private key, therefore forming a security framework consisting of two tiers. The process of decrypting and reconstructing data back to its original format is exclusively limited to those who have been granted authorized access. Furthermore, a distinct signature is produced in order to authenticate the integrity of the data. If there are any attempts made by unauthorized organizations to change the data, the audit process is designed to detect any instances of compromised data.

When data is sent to the cloud by users, a digital signature is formed via the use of asymmetric keys and the user's private key for the purpose of generating such digital signature. The use of this model not only decreases expenses related to data storage by using effective data compression methods, but also offers a well-defined data access protocol that prioritizes the utmost significance of safeguarding data privacy.

The experimental phase produced findings that indicate the superiority of the proposed scheme in comparison to current systems across several benchmarks. The use of a framework that optimizes storage while emphasizing access control centered on privacy may effectively assure the safe storage and sharing of data, particularly in collaborative cloud computing settings.

Keywords: *Digital Media, Data Compression, Data Privacy, Data Security, Cloud Storage, Digital Signature*

1. INTRODUCTION

The advent of cloud computing has significantly transformed the realm of company data storage and sharing methodologies. This particular technical innovation has facilitated enhanced efficiency in the sharing of data, while also providing cost-effective and simplified solutions. Nevertheless, in addition to these advantages, the ease of cloud computing also gives rise to noteworthy apprehensions pertaining to the privacy and security of data. As enterprises transition their data to cloud environments, they are faced with the task of maintaining data security while still enabling authorized access. The challenge of securely exchanging data with other entities, including other businesses, third-party providers, and customers, while maintaining control, has emerged as a critical concern for modern-day enterprises.

Traditional access control methods, such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), possess some drawbacks when it comes to ensuring safe data flow inside cloud platforms. The aforementioned models exhibit a lack of adaptability and provide challenges in terms of management, thereby increasing the probability of mistakes and vulnerabilities that undermine the security of data. In order to overcome these challenges, it is necessary to establish a highly efficient infrastructure that is specifically designed for the purpose of data storage and access control. The presented model presents a versatile and adaptable method for implementing access control, guaranteeing that just authorized entities possess exclusive privileges to data while preserving its secrecy.

Numerous risks and issues pertaining to cloud computing have been discovered for the purpose of mitigation. These include:

The act of gaining access to data without proper authorization. The act of gaining access to data in cloud settings without proper authorization has substantial consequences and presents a substantial risk to both people and companies. Instances of such invasions transpire when unauthorized entities gain entry to data kept in the cloud by many methods, including but not limited to weak passwords, manipulation of individuals through psychological tactics, unaddressed vulnerabilities in the cloud architecture, and compromised authentication credentials. The repercussions of illegal access include a wide spectrum of negative outcomes, including but not limited to personal identity theft, financial detriment, intrusions into corporate data, theft of intellectual property, damage to reputation, and potential legal ramifications. In order to mitigate the risk of unauthorized data breaches, it is essential to implement robust security protocols, including two-factor authentication, severe access restrictions, encryption methodologies, and regular security audits. Furthermore, it is essential to provide comprehensive training to staff about the identification and mitigation of social engineering assaults, as well as to maintain ongoing surveillance of cloud infrastructure.

The occurrence of data breaches presents substantial hazards to the suggested paradigm. The increasing use of cloud computing for storing and sharing information is accompanied by a corresponding increase in the potential for illegal access by hackers. Robust security measures, including encryption, stringent access restrictions, and regular security audits, are used to mitigate the risk of data breaches.

Insider threats, which include trusted individuals inside businesses such as employees, contractors, and suppliers, revealing sensitive data to unauthorized parties, are a significant area of concern. The implementation of access controls and monitoring processes is crucial for effectively addressing internal threats.

Cloud computing offers organizations the advantage of flexible and easily available storage resources; nevertheless, it is important to note that the expenses connected with this technology may be significant. Cloud storage companies often determine their pricing structure by considering factors such as the amount of data stored, the frequency of access, and the rate of data transfer. Nevertheless, the task of calculating and managing storage expenses may provide challenges, particularly in situations when demand experiences fluctuations. Cost management measures include utilization analysis, the use of cost optimization tools provided by vendors, and the use of data compression techniques.

One potential concern about the suggested paradigm is the potential absence of transparency, which might restrict the ability to observe and understand the access and exploitation of data. Transparency may be achieved by the use of audit trails, archiving, and monitoring systems.

It is important to consider and address these challenges and requirements in order for the suggested framework to thrive within the dynamic environment of cloud computing. Organizations may effectively safeguard data accessibility by using stringent access restriction procedures and robust security measures. The establishment of a key distribution system to generate and distribute security keys among users is an essential element that contributes to the enhancement of data security resilience. This complete architecture facilitates the use of cloud storage and file sharing by enterprises, ensuring the preservation of data integrity and confidentiality.

Cloud computing poses a variety of security concerns as a result of the need to rely on third-party service providers for data storage and management. This situation gives rise to problems pertaining to the management of data, weaknesses in security, and restricted visibility. The shared security obligations between cloud providers and users underscore the need of using encryption techniques for both storage and transmission purposes. Furthermore, the potential for data breaches arising from the consolidation of various clients' data underscores the need of implementing a comprehensive cloud security approach that encompasses encryption protocols and individualized authentication credentials.

In conclusion, with the implementation of the suggested all-encompassing framework, enterprises may successfully embrace the advantages associated with cloud storage and sharing, such as scalability, flexibility, and cost-efficiency, while simultaneously safeguarding the privacy and reliability of their data.

2. LITERATURE SURVEY

In a recent research, Kharya et al. (year) introduced an innovative cloud computing model that utilizes Convolutional Neural Networks (CNN) to address a range of challenges, including data protection, backup, and storage strategies. Cloud service providers enforce storage restrictions on customers, so requiring users to take into account the capacity of data storage while accumulating data.

This study presents a novel methodology for implementing Data Access Revocation via the use of a Mix-and-Slice strategy. As seen in Figure 3.1, the system architecture comprises a data owner, two storage providers, and several end users, who are customers of the data owner. The presence of vulnerabilities in man-in-the-middle attacks is recognized due to the untrustworthy nature of the system [1].

This particular arrangement gives rise to concerns about the reliability of data storage providers in terms of their trustworthiness, inquisitiveness, and vulnerability to external breaches. Nevertheless, the customer communication route has been deemed dependable. In order to protect the secrecy of data, the data owner use symmetric encryption to divide the original data into k parts. The aforementioned parts are then distributed to at least two other cloud storage providers, hence enhancing the redundancy of the data. The distribution of the encryption key, a crucial component for the decryption of data, is conducted in a secure manner to a specified number of authorized users, therefore guaranteeing limited access and safeguarding the confidentiality of the data. The accurate decryption keys enable partial decryption even in cases when only a portion of the fragments is available. Data stored outside may be accessed by many end users via the process of downloading pieces from storage providers and then decrypting them using the appropriate key.

The SecACS Architecture entails the responsibility of data storage and ensuring the integrity of cloud computing is with the Cloud Service Provider (CSP). The Trusted Key Generation Center (TKGC) and the data proprietor play essential responsibilities within the context of the Confidentiality, Integrity, and Availability (CIA) Security Policy (CSP). The TKGC is responsible for generating public parameters and private keys for the system, whilst the data owner has the responsibility of outsourcing and revising the data. Users engage with the Cloud Service Provider (CSP) by submitting audit inquiries and verifying provided evidence. The secret key is sent across a secure channel. In summary, the use of SecACS facilitates the establishment of a secure channel for the transmission of data by means of creating and distributing a confidential key between the entity possessing the data and the recipients. The process of transmitting data units and identifiers to the cloud enables the evaluation of data correctness by generating proofs and validating them via user input [2].

In this paper, the author emphasizes the significance of the Cloud-edge-collaborative storage (CECS) structure as an effective approach for managing Internet of Things (IoT) data in a secure manner. The proposed system involves the preprocessing of data using peripheral servers before its storage on a cloud server, therefore enabling the real-time analysis of data produced by Internet of Things (IoT) devices. Nevertheless, the author admits the existence of possible weaknesses in the security measures of CECS, namely those that heavily depend on the integrity of peripheral servers. In order to address this particular risk, the author presents a proposed technique that deviates from traditional secure CECS designs in two notable ways.

The suggested methodology allows users to produce and maintain their own public and private keys, eliminating the need for external servers in the administration of keys. This upgrade effectively enhances control measures pertaining to data security. Furthermore, the proposed solution integrates the use of searchable public-key encryption methods, hence enhancing the robustness, efficacy, and flexibility of data retrieval processes. This invention aims to enhance cloud data security, streamline safe data sharing and searching processes, and eliminate any vulnerabilities inside the system.

3. PROPOSED SYSTEM

A complete framework has been established to solve the issues associated with lowering data storage costs, ensuring privacy via data access rules, and certifying data integrity in the context of data sharing. The paradigm under consideration, as seen in figures 1, 2 and 3, has three fundamental processes: Ownership, User, and Third-Party Auditor (TPA).

Costs Associated with Storage

One of the essential aspects of our methodology is to the minimization of storage costs. Our solution aims to address the financial implications of keeping substantial amounts of data in cloud settings by proposing a streamlined data storage strategy that ensures the preservation of data security and privacy. The proposed approach integrates data compression, data fragmentation, and data encryption techniques, leveraging the private key of the data owner.

In order to achieve efficient reduction of file sizes, our methodology proposes the compression of high-resolution photographs prior to their storage in the cloud. Empirical evidence indicates that the compression of high-resolution photographs may provide a substantial reduction in data size, reaching up to sixty percent. This module utilizes the DCT (Discrete Cosine Transform) method, known for its computational efficiency and segmented structure, enabling the generation of numerous DCTs for both rows and columns. Furthermore, the power integration features of the system contribute to its enhanced efficacy.

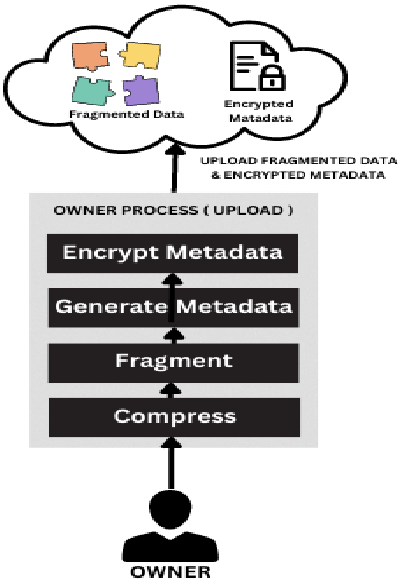


Fig. 1 – Process of Owner

Enhancing Privacy via Access Control

The incorporation of access control measures that promote privacy becomes an essential supplementary element inside our concept. These procedures are designed to enforce access control and data integrity, therefore deterring illegal access and modification. The implemented model incorporates an access control system that allows users to establish data access rules, so guaranteeing that only those with proper authorization may access the data. In addition, we propose the fragmentation of the compressed data into numerous parts in order to optimize storage consumption. The data that is fragmented is then subjected to encryption using the private key of the owner, so introducing an extra level of protection. This mechanism guarantees that only those with proper authorization has the ability to decode and restore the data to its initial form. An picture may be acquired by a user subsequent to receiving authorization from the owner to access it. However, it is necessary to have a certain sequence of pieces in order to rebuild the picture file. In the course of the fragmentation procedure, fragment particulars are recorded and subjected to encryption measures in order to ensure security. The act of decrypting this log file grants access to the aforementioned fragment data.

The module known as Data Defragmentation is tasked with the responsibility of rebuilding pictures from pieces that have been previously saved. When a user with proper authorization asks access to a picture, this particular component efficiently detects the necessary fragmented portions by using the data present in the log file. Subsequently, these portions are systematically organized in the appropriate sequence to provide the user with a cohesive and comprehensive depiction. The decryption of these pieces is performed by using the public key of the data owner, who first supplied the material.

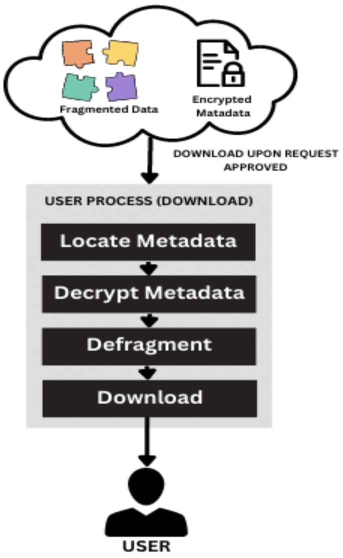


Fig. 2 – Process of User

Data Correction and Verification

The process of verifying data and ensuring its integrity is of utmost importance in academic research and other data-driven fields. It involves a systematic approach to confirm the accuracy, reliability, and consistency of collected data, as well as the implementation of measures to prevent any unauthorized alteration or corruption. Verification of data include thorough scrutiny and cross-checking of

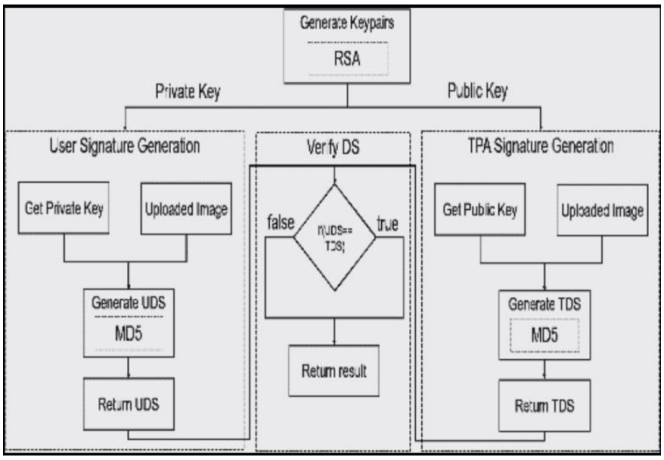


Fig. 3 – Model of Data Correction and Verification

The proposed methodology significantly enhances the efficiency of dynamic operations and guarantees the integrity of data in cloud-based systems, consequently speeding the process of data audits conducted by auditors. Auditors are granted restricted access, limited to read-only privileges, which facilitates the process of conducting audits on a larger scale. A signature generation procedure is implemented in which user traits and system time are included, therefore guaranteeing the uniqueness of signatures, minimizing storage expenses, and preserving the timeliness of data.

Within the context of our architectural framework, the Trusted Third Party (TPA) employs a process whereby it autonomously forms a signature by including all relevant user qualities. This procedure serves to guarantee the authenticity and accuracy of the associated data. The system does not store multiple instances of data and maintains the confidentiality of the private key throughout the decryption process. The Trusted Platform Agent (TPA) continually produces signatures, which are updated whenever users submit or modify data, in order to maintain data freshness. The aforementioned technology enhances user reaction time inside the cloud environment while also preserving the effectiveness of data storage by means of bulk processing.

The present idea outlines the integration of an access control system that utilizes asymmetric credentials. The generation of a digital signature occurs when a person employs their private key with the purpose of submitting data to the cloud. The validation of this digital signature may be performed by a third-party auditor via the use of the corresponding public key. This process serves to guarantee the integrity of the data and enables streamlined auditing and verification operations.

4. CNN TRAIN AND TEST MODEL

The successful application of picture compression may be achieved by using a specific subset of the Kaggle dataset, such as ImageNet. The use of a labeled dataset is not necessary for this assignment since it does not entail object identification. The main goal is to decrease the physical dimensions of the picture by over fifty percent while maintaining its aesthetic integrity.

The Discrete Cosine Transform (DCT) is a member of the discrete cosine transform family of lossy compression methods. The Discrete Cosine Transform (DCT) has significant effectiveness in compressing images when operating inside the Fourier-related transform domain. In the present study, a modified Quality Factor was used in conjunction with a variation of the Discrete Cosine Transform (DCT) method. The implementation of this adjustment was crucial in order to effectively regulate and manage the quality of the images. The use of a certain Quality Factor during the process of picture compression aids in the preservation of image quality without causing any degradation.

A Comparative Analysis of the Techniques of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT)

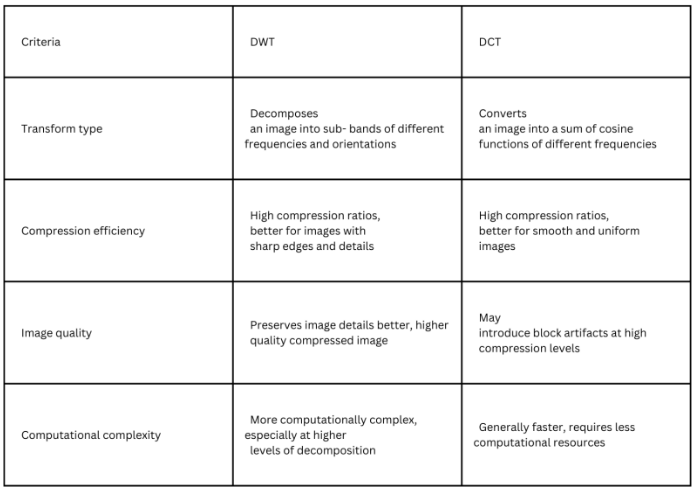
The Discrete Wavelet Transform (DWT) procedure is a mathematical algorithm used for signal and image processing. It involves decomposing The process involves dividing a picture into sub-bands that exhibit distinct frequencies and orientations. The picture is expressed as a combination of cosine functions at different frequencies.

The use of this format is favored for photos that include well-defined borders and precise features, owing to its ability to achieve greater compression ratios.

The preservation of picture details is enhanced, leading to a compressed image of superior quality. The computational complexity of the system increases substantially, particularly when operating at higher degrees of decomposition. The Discrete Cosine Transform (DCT) methodology is a widely used technique in signal processing and data compression. The process involves transforming a picture into a representation consisting of the summation of cosine functions with varying frequencies. - This method is particularly advantageous for generating smooth and consistent images, as it offers larger compression ratios. However, excessive compression levels may lead to the occurrence of block anomalies. The discrete wavelet transform (DWT) is generally considered to be less efficient and more computationally demanding compared to other methods.

The choice between Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) is contingent upon the unique demands of the application and the intrinsic properties of the picture.

Table 1 – DWT and DCT Comparative Analysis



Criteria	DWT	DCT
Transform type	Decomposes an image into sub- bands of different frequencies and orientations	Converts an image into a sum of cosine functions of different frequencies
Compression efficiency	High compression ratios, better for images with sharp edges and details	High compression ratios, better for smooth and uniform images
Image quality	Preserves image details better, higher quality compressed image	May introduce block artifacts at high compression levels
Computational complexity	More computationally complex, especially at higher levels of decomposition	Generally faster, requires less computational resources

Figure 4 illustrates the comparative sizes, measured in megabytes (MB) and kilobytes (KB), of five unique photos before and after compression. Significantly, after to compression, the size of "Image 1" decreased from 1 MB to 250 KB. The graph illustrates a general trend where bigger original pictures tend to exhibit lower compression rates, leading to a relatively lesser decrease in size compared to their original dimensions.

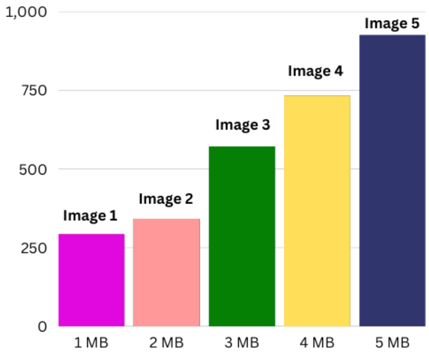


Fig. 4 – The disparity in storage capacity between the original picture and the compressed image.

The visual representation in Figure 5 shows a series of pictures accompanied by their corresponding Peak Signal-to-Noise Ratio (PSNR) values.

The Peak Signal-to-Noise Ratio (PSNR) is a widely used statistic in the field of image processing for assessing the quality of a picture by measuring its faithfulness to the original source. The picture labeled as "Camera Man" achieved a peak signal-to-noise ratio (PSNR) of 37.04 when subjected to the discrete cosine transform (DCT) in the first row. Conversely, in the second row, the PSNR saw a little improvement, reaching 37.37, when the image underwent the discrete wavelet transform (DWT). In a similar vein, the picture labeled as "Rice" in the second set of rows had a peak signal-to-noise ratio (PSNR) value of 39.04 when subjected to discrete cosine transform (DCT) processing. However, when subjected to discrete wavelet transform (DWT) processing, the PSNR value decreased to 37.7.

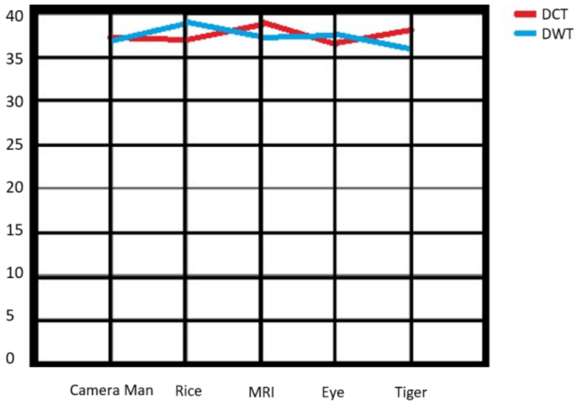


Fig. 5 – Images that have been compressed by DCT and DWT, along with their PSNR values

In Figure 6, a comparison is shown between the auditing model that has been presented and the SecACS model. This visual representation presents a comparison of the computational efficiency between the method suggested in this study and the SecACS algorithm. Furthermore, it is essential to acknowledge that the computational duration of the auditing method exhibits a straight correlation with the quantity of audit questions.

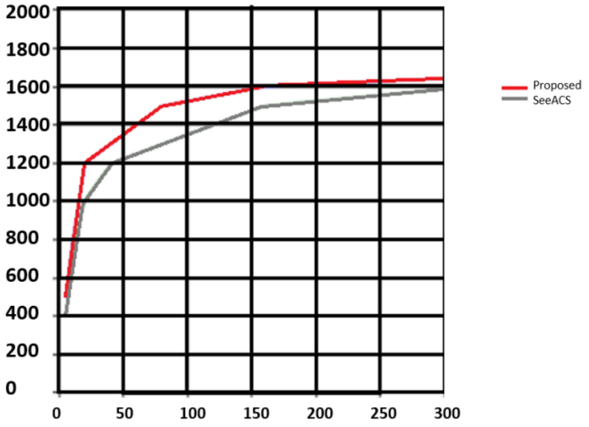


Fig. 6 – A look at the planned inspection plan and SecACS

5. CONCLUSION

The suggested architecture for decentralized data access control presents a novel approach that facilitates safe data sharing among authorized entities, while also empowering the data owner with the capability to withdraw access privileges when necessary. The attainment of this objective is accomplished by using a strategic approach to the use of encryption and data fragmentation techniques, which, when integrated, provide a multifaceted security framework. In order to rebuild the original file, it is necessary to decode each fragment for illegal access to the contents. This security measure involves the fragmentation of a singular file into several smaller files, followed by the encryption of each individual fragment prior to its storage in a cloud environment. The use of a multi-authority access control system efficiently ensures the protection of sensitive data saved and exchanged in cloud environments within the framework.

This framework offers a comprehensive solution to address problems related to data safety and privacy, demonstrating its potential applicability across various remote storage systems. The platform's capacity to promote regulated data exchange, uphold ownership-based access management, and provide several layers of protection makes it a compelling option for businesses aiming to enhance data governance and secrecy.

The result of this study presents a decentralized data access control framework that offers a unique and innovative way to ensuring the safe sharing and management of data access. By using encryption and data fragmentation techniques, the framework effectively deters unlawful access and empowers data owners with enhanced control over their shared data. Enhancing the security of sensitive data housed in cloud environments fosters trust and confidence among users and stakeholders. Ensuring data integrity and privacy throughout its lifespan is of paramount importance in the digital realm. This framework effectively addresses these issues in a comprehensive manner.

In the realm of prospective advancements, it is vital to consider future developments.

There are many possible avenues for enhancing and refining the suggested framework in the future, hence creating further chances for improvement.

This study aims to develop strategies for effectively handling bigger datasets while ensuring optimal performance and maintaining robust security measures.

Developing interfaces that are user-friendly and controls that are intuitive is crucial in order to facilitate broad adoption and effective administration.

Interoperability refers to the assessment of the compatibility between integration processes and pre-existing data storage and management systems.

This study aims to investigate sophisticated encryption algorithms in order to enhance data security in response to emerging threats.

This study aims to explore systems that provide the real-time change of access restrictions in order to effectively address changing requirements.

The potential integration of blockchain technology should be considered as a means to augment data integrity, audit trails, and access transparency.

This study aims to design and implement automated auditing systems to facilitate the ongoing monitoring of data access and consumption.

By exploring these options, the suggested framework has the potential to enhance its effectiveness in safeguarding data security, privacy, and access control within the dynamic environment of remote storage systems.

References

[1] Katarzyna KAPUSTA, Han QIU, and Gerard MEMMI LTCI, Telecom ParisTech, Paris, France “Secure Data Sharing with Fast Access Revocation through Untrusted Clouds” 978-1-7281-1542-9/19/$31.00 ©2019 IEEE.

[2] Li Li, Jiayong Liub “SecACS: Enabling lightweight secure auditable cloud storage with data dynamics” 2214-2126/© 2020 Elsevier Ltd. All rights reserved.

[3] Reyhaneh Rabaninejad, Seyyed Mahdi Sedaghat, Mohamoud Ahmadian Attari, Mohammad Reza Aref “An ID-Based Privacy-Preserving Integrity Verification of Shared Data Over Untrusted Cloud” K. N. Toosi University of Technology Department of Electrical Engineering Tehran, Iran, 978-1-7281-5937- 9/20/$31.00 ©2020 IEEE

[4] Premlata Singh, Sushil Kr. Saroj “A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage” Department of Computer Science & Engineering, Madan Mohan Malaviya University of Technology Gorakhpur, India 978-1-7281-5197- 7/20/$31.00 ©2020 IEEE

[5] Jian Wang, Kehua Wu, Chunxiao Ye, Xiaofeng Xia, Fei Ouyang ∗Colleage of Computer Science, Chongqing University, Chongqing, China “Improving Security Data Access Control for Multi-Authority Cloud Storage” 978-1-7281-4328-6/19/$31.00 ©2019 IEEE

[6] Aritra Dutta, Rajesh Bose, Swamendu Kuma Chakraborty, Sandip Roy, Haraprasad Mondal, Computational science Brainware University, Kolkata India "Data Security Mechanism for Green Cloud", IEEE 2021

[7] Ding ManJiang 1, Cao Kai 1, Wang ZengXi 2, Zhu LiPeng 3, 1. State Grid Jiangsu Tendering Co., Ltd, Nanjing, China 2. Jiangsu Electric Power Information Technology Co., Ltd, Nanjing, China 3. Global Energy Interconnection Research Institute Co., Ltd, Beijing, China, "Design of a Cloud Storage Security ncryption Algorithm for Power Bidding System", IEEE 2020

[8] YANG Zhen, WANG Wenyu, HUANG Yongfeng, and LI Xing, Department of Electronic Engineering, Tsinghua University, Beijing 100084, China “Privacy- Preserving Public Auditing Scheme for Data Confidentiality and Accountability in Cloud Storage” 2019 Chinese Institute of Electronics. DOI:10.1049/cje.2018.02.017 ©2019 IEEE

[9] Fei Chen, Fengming Meng, Tao Xiang, Hua Dai, Jianqiang Li, Jing Qin “Towards Usable Cloud Storage Auditing” 1045-9219 (c) 2020 IEEE

[10] C.Jenifer Kamalin1, Dr.T.Arul Raj2, Dr.G.MuthuLakshmi3 1Research Scholar, 2, 3Assistant Professor 1,3Department of Computer Science & Engineering, Manonmaniam Sundaranar University, Abishekapatti, Tirunelveli – 627 012 2Department of Computer Science, Sri Paramakalyani College, Alwarkurichi, Tenkasi – 627 412, “Comparative Analysis for Dct, Dwt Image Compression Performed with Huffman, Run Length and Lzw Encoding”, NTERNATIONAL JOURNAL OF SPECIAL EDUCATION Vol.37, No.3, 2022

[11] SI HAN, KE HAN, AND SHOUYI ZHANG Department of Science and Technology, China University of Political Science and Law, 102249 China “A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era” 2169- 3536 2019 IEEE.

[12] Leyou Zhang, Yilei Cui , and Yi Mu , Senior Member, IEEE “Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing” 1937-9234 © 2019 IEEE

[13] T. A. Mohanaprakash, Dr.J.Andrews Department of CSE, Sathyabama Institute of Science and Technology, Chennai 600119, Tamilnadu, India “Novel privacy preserving system for Cloud Data security using Signature Hashing Algorithm” 978-1-7281-1576- 4/19/$31.00 ©2019 IEEE

[14] YE TAO, PENG XU, and HAI JIN, National Engineering Research Center for Big Data Technology and System, Services Computing Technology and System Lab “Secure Data Sharing and Search for Cloud-Edge-Collaborative Storage” 10.1109/ACCESS.2019.2962600, IEEE Access

[15] Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Tengfei Yang, School of Cyber Engineering, Xidian University, Xi'an 710071, China “Privacy-Preserving Data Sharing Framework for High-Accurate Outsourced Computation” 978-1-5386-8088-9/19/$31.00 ©2019 IEEE

[16] Wenxiu Ding, Member, IEEE, Rui Hu, Zheng Yan, Senior Member, IEEE, Xinren Qian, Robert H. Deng, Fellow, IEEE, Laurence T. Yang, Senior Member, IEEE, and Mianxiong Dong, Member, IEEE “An Extended Framework of Privacy-Preserving Computation with Flexible Access Control” 1932-4537 (c) 2019 IEEE

[17] HAN YU, XIUQING LU, AND ZHENKUAN PAN, College of Computer Science and Technology, Qingdao University, Qingdao 266071, China, “An Authorized Public Auditing Scheme for Dynamic Big Data Storage in Cloud Computing” r 10.1109/ACCESS. 2020 IEEE

[18] Nikolaos Doukas, Oleksandr P. Markovskyi, Nikolaos G. Bardis Department of Mathematics and Engineering Science, Hellenic Military Academy, Vari – 16673, Greece “Hash function design for cloud storage data auditing” 0304-3975/© 2019 Elsevier

[19] Nureni Ayofe Azeez, Charles Van der Vyver School of Computer Science and Information Systems, Faculty of Natural and Agricultural Sciences, Vaal Triangle Campus, North-West University, South Africa. “Security and privacy issues in e-health cloud-based system: A comprehensive content analysis” 1110-8665/2018 Production and hosting by Elsevie

[20] Jianghong Wei , Wenfen Liu, and Xuexian Hu “Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage” IEEE SYSTEMS JOURNAL, VOL. 12, NO. 2, JUNE 2018

[21] Zhan Qin, Jian Weng, Yong Cui, Kui Ren, “Privacy- preserving Image Processing in the Cloud” 10.1109/MCC.2018. IEEE

[22] Kaiping Xue, Senior Member, IEEE, Weikeng Chen, Wei Li, Jianan Hong, Peilin Hong "Combining Data Owner-side and Cloud-side Access Control for Encrypted Cloud Storage" 1556-6013 (c) 2018 IEEE

[23] Jianting Ning, Zhenfu Cao, Senior Member, IEEE, Xiaolei Dong, Kaitai Liang, Member, IEEE, Lifei Wei, and Kim-Kwang Raymond Choo, Senior Member, IEEE "CryptCloud+: Secure and Expressive Data Access Control for Cloud Storage" 1939-1374 (c) 2017 IEEE

[24] Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou Department of ECE Illinois Institute of Technology , Department of ECE Worcester Polytechnic Institute "Ensuring Data Storage Security in Cloud Computing" 978-1-4244-3876-1/09/$25.00 ©2009 IEEE

[25] Cong Wang, Student Member, IEEE, Qian Wang, Student Member, IEEE, Kui Ren, Senior Member, IEEE, Ning Cao, and Wenjing Lou, Senior Member, IEEE, "Toward Secure and Dependable Storage Services in Cloud Computing" 1939-1374/12/$31.00 2012 IEEE

[26] Syam Kumar P, Subramanian R Department of Computer Science, School of Engineering & Technology Pondicherry University, Puducherry-605014, India,"An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 6, No 1, November 2011

[27] CONG WANG1 (Member, IEEE), BINGSHENG ZHANG2 (Member, IEEE), KUI REN2 (Senior Member, IEEE), AND JANET M. ROVEDA3 (Senior Member, IEEE) Department of Computer Science, City University of Hong Kong, Hong Kong "Privacy- Assured Outsourcing of Image Reconstruction Service in Cloud" IEEE TRANSACTIONS ON CLOUD COMPUTING VOL:1 NO:1 YEAR 2013

[28] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2, FEBRUARY 2013

[29] Kan Yang, Student Member, IEEE, Xiaohua Jia, Senior Member, IEEE, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 1045-9219/12/$31.00 © 2012 IEEE Boyang Wang, Student Member, IEEE, Baochun Li, Senior Member, IEEE, and Hui Li, Member, IEEE "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud", IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 2, NO. 1, JANUARY- MARCH 2014

[30] HUAQUN WANG1, 2 1 Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, "Anonymous Data Sharing Scheme in Public Cloud and Its Application in E-health Record" 2169-3536 (c) 2018 IEEE

[31] R.Swathi, T.Subha, Associate Professor, Department of Information Technology, Sri Sairam Engineering College, Chennai, swathi.marthandan@gmail.com, subharajan@gmail.com, "ENHANCING DATA STORAGE SECURITY IN CLOUD USING CERTIFICATELESS PUBLIC AUDITING" 978-1- 5090-6221-8/17/$31.00 c 2017 IEEE

[32] Nelmiawati Department of Informatics Engineering Politeknik Negeri Batam Batam, Indonesia mia@polibatam.ac.id, Wahyudi Arifandi Department of Informatics Engineering Politeknik Negeri Batam Batam, Indonesia wahyudi.arifandi@gmail.com,"A Seamless Secret Sharing Scheme Implementation for Securing Data in Public Cloud Storage Service" 978-1- 5386-8066-7/18/$31.00 ©2018 IEEE

[33] Salunke M. D, Kumbharkar P. B; Kumar, P. (2021). A Proposed Methodology to Mitigate the Ransomware Attack. https://doi.org/10.3233/apc210173.

[34] M.D.Salunke, Kumbharkar P. B; SharmaYogesh Kumar. (2020). Proposed Methodology to Prevent a Ransomware Attack. International Journal of Recent Technology and Engineering (IJRTE), 9(1), 2723–2725.

[35] Subhash G. Rathod, R N khobragade, Vilas Thakare, Sushama L. Pawar. (2022). Security for Shared Data Over Public Cloud for Maintaining Privacy. Mathematical Statistician and Engineering Applications, 71(4), 7167–7173. Retrieved from https://www.philstat.org/index.php/MSEA/article/view/1336

[36] Rathod, S., Khobragade, R. N., Thakare, V. M., Walse, K. H., &amp;Pawar,

[37] S. (2022, September). Lightweight Auditable Secure Cloud Storage With Privacy Enabled Data Storage Optimization. In 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-6). IEEE.

[38] Rathod, S., Khobragade, R. N., Thakare, V. M., Walse,

[39] K. H., Pawar, S. (2022, September). Model for Efficient Data Storage on Public Cloud. In 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) (pp. 1-5). IEEE.

[40] Subhash Gulabrao Rathod, Dr.K.H.Walse, Dr. R N khobragade, Dr. Vilas Thakare , &amp;Sushama L. Pawar. (2022). PRESERVING PRIVACY &amp; MAINTAINING SECURITY FOR SHARED DATA OVER PUBLIC CLOUD: A SURVEY. International Journal Of Advance Research And Innovative Ideas In Education, 8(3), 4971-4976.

[41] Dhanwanth, B. ., Saravanakumar, R. ., Tamilselvi, T. ., & Revathi, K. . (2023). A Smart Remote Monitoring System for Prenatal Care in Rural Areas. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3), 30–36. https://doi.org/10.17762/ijritcc.v11i3.6196

[42] Kanna, D. R. K. ., Muda, I. ., & Ramachandran, D. S. . (2022). Handwritten Tamil Word Pre-Processing and Segmentation Based on NLP Using Deep Learning Techniques. Research Journal of Computer Systems and Engineering, 3(1), 35–42. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/ article/view/39

[43] Subhash rathod, mangesh d. Salunkeet et. Al. (2023). Ensuring optimized storage with data confidentiality and privacy- preserving for secure data sharing model over international journal of intelligent systems and applications in engineering ijisae, 2023, 11(3), 35–44.