International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Ensuring Optimized Storage with Data Confidentiality and Privacy-Preserving for Secure Data Sharing Model Over Cloud

Subhash Rathod[1]*, Mangesh D. Salunke[2], Meghna Yashwante [3], Manisha Bhende [4], Sudhir R. Rangari[5], Vaibhav D. Rewaskar[6]

Submitted: 19/04/2023 **Revised**: 21/06/2023 **Accepted**: 04/07/2023

Abstract: This paper proposes privacy-preserving access control model for optimized storage over cloud. The main goal is to provide data security, privacy, integrity, and availability at a lower cost to cloud service providers while ensuring that users feel confident in trusting them. To achieve this, a secure authenticity scheme is proposed to protect data during storage and transfer over the cloud. The framework focuses on storage cost optimization while maintaining data security and authenticity. The proposed scheme compresses high-resolution images to reduce the storage size of the data by 60%. The data is then fragmented into multiple chunks, and these chunks are encrypted using the owner's private key, providing two layers of security. Only users with authority to the data can decrypt and reconstruct it into its original format. A signature is generated to check the integrity of data. If unauthorized users attempt to update data, the auditing process can identify the compromised data. Asymmetric keys are used, and when a user uploads data to the cloud, a digital signature is created with the user's private key. By implementing the suggested model, not only can the expenses associated with data storage be diminished through efficient data compression techniques, but it also introduces a well-defined data access protocol that prioritizes the preservation of data privacy. Experimental execution concludes that the proposed scheme has good performance over existing systems with a variety of aspects. The optimized storage and privacy-preserving access control model can be used to ensure secure data storage and sharing in collaborative cloud computing environments.

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

1. Introduction

The advent of cloud computing has transformed the manner in which enterprises store and exchange data. With the emergence of this technology, the process of data sharing has undergone a significant revolution, rendering it simpler, swifter, and economically advantageous compared to previous methods. However, the convenience of cloud computing comes with a price, as it also raises significant concerns regarding data privacy and security. As data moves to the cloud, organizations must address the challenge of maintaining control over their data while still providing authorized access to it. One of the biggest issues facing organizations today is how to securely share data with other organizations, third-party vendors, or customers, while maintaining control over it. Traditional access control models based on Role-Based Access Control (RBAC) or Attribute-Based Access Control (ABAC) have their limitations when it comes to securely sharing data over the cloud. RBAC and ABAC models can be inflexible and complex to manage, which can lead to errors and vulnerabilities that can compromise the privacy of the data. To address these challenges, an optimized storage and access control model for data sharing is proposed. The proposed model provides a flexible and scalable approach to access control, ensuring that the data is only accessible by authorized parties while maintaining privacy. There are several issues and vulnerabilities in cloud computing that we are considering to mitigate which are as follows:

Unauthorised Access to Data: The potential ramifications of unauthorized data access in cloud environments are severe, posing a grave threat to both individuals and organizations. It occurs when someone gains access to cloud-based data without permission or authorization, and can be caused by various factors such as weak passwords, social engineering attacks, unpatched vulnerabilities in cloud infrastructure, and compromised credentials. The impact of unauthorized access to cloud data can be severe. For individuals, it can result in identity theft, financial loss, and loss of privacy. For organizations, the impact can be even greater, with potential consequences including data breaches, loss of intellectual property, damage to reputation, and legal liability.

In order to minimize the potential vulnerability of unauthorized data breaches in cloud environments, it is crucial to enforce robust security protocols. These measures

[1]*Marathwada Mitra Mandal's Institute of Technology, Pune*
ORCID ID : 0000-0003-2528-9202
[2] *Marathwada Mitra Mandal's Institute of Technology, Pune*
ORCID ID : 0000-0001-8691-8311
[3] *Marathwada Mitra Mandal's Institute of Technology, Pune*
ORCID ID : 0000-0002-4081-0265
[4]DPU, Dr. D. Y. Patil Schoolof Science& Technology, Tathwade, Pune
ORCID ID : 0000-0003-2407-8091

** Corresponding Author Email: subhashrathod@gmail.com, salunkemangesh019@gmail.com*

include the adoption of two-factor authentication, stringent access controls, encryption techniques, as well as conducting routine security evaluations. Additionally, it is essential to educate employees on how to recognize and prevent social engineering attacks, and to monitor cloud infrastructure for signs of unauthorized access or unusual activity.

Data breaches: One of the most significant threats to the model is the risk of data breaches. As data is stored and shared over cloud computing, there is a higher risk of cybercriminals gaining unauthorized access to the data. Organizations must implement robust security measures to prevent data breaches, such as encryption, secure access controls, and regular security audits.

Insider threats: Another significant threat to the proposed model is insider threats. Insider threats occur when trusted individuals within an organization, such as employees, contractors, or vendors, intentionally or unintentionally expose sensitive information to unauthorized parties. Organizations must have strict access controls and monitoring procedures in place to prevent insider threats.

Storage Cost: A noteworthy benefit offered by cloud computing is its capacity to furnish instantly available computing resources and storage capabilities that can be flexibly adjusted to meet fluctuating demands. However, the issue of storage cost can be a major concern for businesses that use cloud storage services. Cloud storage providers typically charge for storage on a per-gigabyte basis, with additional charges for data transfer, data access, and other services. The cost of cloud storage can vary widely depending on the provider, the amount of data stored, the level of redundancy required, and other factors. One of the challenges with cloud storage cost is predicting and managing it effectively. While cloud storage offers scalability and flexibility, it also means that the cost can be difficult to estimate, especially if storage needs change frequently. To address this issue, businesses can employ a number of strategies, such as analysing usage patterns to identify areas where cost savings can be achieved, leveraging cost optimization tools provided by the cloud provider, and compressing the data to reduce storage size.

Lack of transparency: The proposed model may also face a lack of transparency, which can make it challenging to determine how the data is being accessed and used. Organizations must ensure that the model provides clear visibility into who is accessing the data and how it is being used. This can be achieved through audit trails, logging, and monitoring tools.

Issues and Parameters Considered

Cloud computing introduces several security challenges and issues the utilization of cloud technology for data storage and access involves entrusting a third-party provider, which raises concerns regarding limited visibility and control over data, as well as security risks. The responsibility for cloud security risks is shared by both the cloud provider and the customer, with the provider securing the cloud infrastructure and the customer ensuring their data's safety. Nonetheless, utilizing file sharing services from third-party vendors may put data confidentiality at risk by exposing it to external IT environments. To mitigate these risks, it's recommended to encrypt files during storage and transfer. Moreover, since multiple customers' data is stored on the same server, the possibility of data breaches through third-party access should be considered. Therefore, it is critical to invest in a comprehensive cloud security strategy that includes encrypting sensitive data and securing unique credentials.

The proposed framework aims to address these security concerns and should work in a malicious environment. Implementing access restriction protocols is essential to ensure that only authorized users can have access to data. To ensure security, two conditions must be met: To ensure the robustness of data security, it is imperative to establish a reliable key distribution module responsible for generating and disseminating security keys to all users. Both the data owner and the data users must securely store these keys to prevent unauthorized access. By implementing such a comprehensive framework, organizations can leverage the benefits of cloud storage and file sharing services, such as flexibility, scalability, and cost savings, while simultaneously safeguarding the confidentiality and integrity of their data.

2. Literature Survey

1) In a recent study, Kharya et al. proposed a CNN-based Cloud computing has many challenges such as data security, data backup, data storage techniques, availability. One limitation in cloud storage is user can acquire limited amount of storage as decided by the cloud service provider. Cloud service provider also has to take care of data storage space while backing up their data.

2) Data Access Revocation using Mix & Slice approach

The system presented here aims to provide secure data transmission and confidentiality with the added feature of data access revocation. Figure 3.1 depicts the system architecture, which consists of a data owner, two storage providers, and multiple end users (who are clients of the data owner). However, there is a risk of a man-in-the-middle attack as the system is untrusted. [1]

3) In this scenario, the reliability of the storage providers is in question due to concerns about their honesty, curiosity, or vulnerability to external attacks. However, there is trust in the communication channel between users. In order to guarantee the privacy of sensitive data, a data owner employs a symmetric encryption method to convert the original data into a collection of k fragments. These fragments are subsequently distributed among at least two

distinct cloud storage providers, thereby enhancing data redundancy. The encryption key, crucial for decrypting the data, is securely shared among N authorized users, ensuring controlled access and maintaining data confidentiality. Even if only a portion of the set is accessible, the fragments can be decrypted using the accurate key. Several end-users can retrieve the data stored externally by downloading it from both cloud storage providers and decrypting the fragments utilizing the appropriate key.

4) SecACS Framework

In cloud computing, the responsibility of storing and ensuring data integrity lies with the Cloud Service Provider (CSP). The CSP consists of two key components: the Trusted Key Generation Center (TKGC) and the data owner. The TKGC generates public parameters and secret keys for the system, while the data owner handles the task of outsourcing and updating the data. Data users interact with the CSP by sending audit queries and verifying the provided proofs. The secret key is securely transmitted through a trusted channel. In summary, SecACS offers a concise overview of these processes. To establish a secure solution, a confidential key is generated and securely shared between the data owner and users through a communication channel with high levels of security. Following this, the data owner transfers data blocks along with their corresponding tags to the cloud. Users can then perform audits on the data's correctness by utilizing the tags and specific data blocks to generate proofs. These proofs are subsequently validated by the users to ensure the integrity of the data. [2].

5) Sharing Data Securely and Cloud Based Collaborative Storage

According to the author's perspective, the Cloud-edge-collaborative storage (CECS) framework presents a practical solution for effectively managing data generated by the Internet of Things (IoT). This innovative framework enables real-time processing of IoT data by utilizing edge servers, followed by storing the processed data on a cloud server. However, the author acknowledges that while CECS is advantageous for IoT data processing, it is susceptible to potential information leakage. Current secure CECS plans heavily rely on the trustworthiness of all edge servers. Regrettably, if any one of these servers becomes compromised, it could result in the exposure of all data stored in the cloud. To address this issue, the author proposes an alternative approach that enhances existing secure CECS plans in two key ways.

6) Firstly, instead of depending on edge servers for private key management, the suggested approach empowers users to create and manage their own public and private keys. This shift provides a higher level of control over data security. Secondly, the proposed plan incorporates searchable public-key encryption techniques, thereby augmenting the security, efficiency, and flexibility of data searching processes. Through this new approach, the author aims to ensure the security of cloud data, facilitate secure data sharing and searching, and eliminate single points of failure within the system.

3. Proposed System

We designed data sharing framework that can ensure low data storage cost, Data access control that will provide data privacy and data verification of stored data. As shown in figure 3.1, 3.2 and 3.3 proposed model contains three process. Owner, User and TPA process

Storage Cost Optimization

One of the main features of our proposed model is the storage cost optimization technique. We recognize that storing large amounts of data on the cloud can be expensive, and we propose a solution to optimize the storage of data while ensuring data security and privacy. The proposed solution involves compressing data to reduce its size, dividing the data into multiple fragments, and encrypting the data using owner's private key.

To reduce the size of the data, we propose compressing high-resolution images before storing them on the cloud. Our experiments show that compressing high-resolution images can reduce the size of the data by up to 60%. This module reduces storage size by half taking pictures as input and compressing them using the DCT (Discrete Cosine Transform) algorithm. DCT is preferred due to its ease of computation and its segmented nature, which allows for the creation of various DCTs for rows and columns. Additionally, it possesses characteristics of power integration, further enhancing its usefulness.

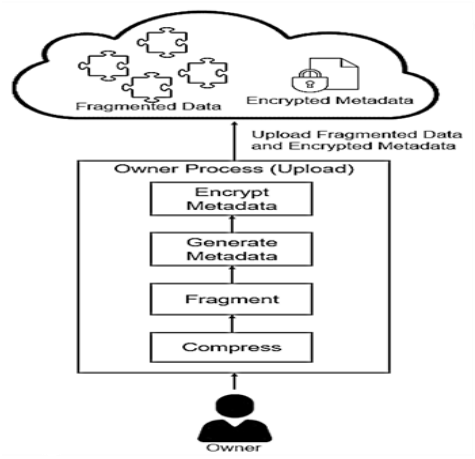

Fig. 3.1 Owner Process

Privacy-Preserving Access Control

The other main feature of our proposed model is privacy-preserving access control. Access control mechanisms ensure that only authorized users can access and modify data, protecting it from unauthorized access and modification. In our proposed model, we use an access control mechanism that allows users to specify access control on who can access data. This mechanism ensures that only authorized users can access, data. We also propose fragmenting the compressed data into multiple chunks to maximize the use of available storage space. The fragmented data is then encrypted using the owner's private key, providing two layers of security. This ensures that only users with authority to the data can decrypt and reconstruct it into its original format. After the owner approves the user's download request, the user can proceed to download the image. However, in order to reconstruct the image file, a specific sequence of fragments is required. These fragment details are gathered and stored in a log file during the fragmentation phase, which is encrypted for security purposes. To access this information, the encrypted log file is first decrypted using a log decryption process and subsequently passed to the data defragmentation module.

To reconstruct image into original form from encrypted fragmented chunks, it needs to convert into readable format by decrypting them. These decrypted chunks and decrypted log file will then be input to data defragmentation module in order to reconstruct data into its original form. Here public key of data owner who originally uploaded data is used to decrypt the fragments.

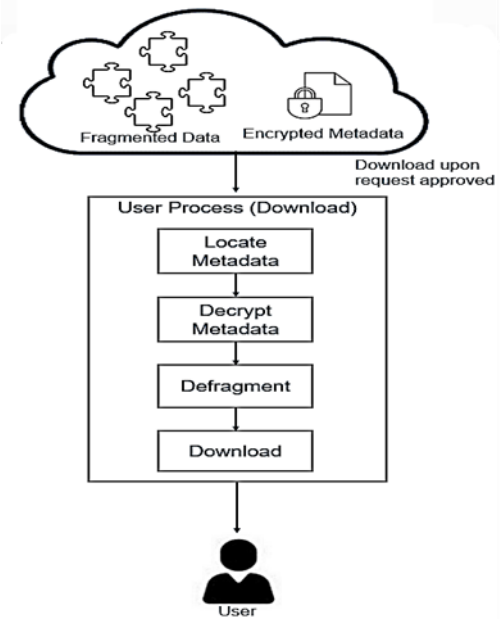

Fig. 3.2 User Process

The task of reformation images from previously stored fragments by the owner on the cloud, falls under the purview of the Data Defragmentation module. When an authorized user seeks access to an image, this component promptly identifies the fragmented segments by utilizing the details supplied in the log file. Subsequently, it consolidates these

segments in the appropriate order to ensure a coherent and complete image is presented to the user.

Data Correctness and Verification

Our approach enables auditors to conduct data audits more efficiently, as it supports dynamic operations and ensures data accuracy in cloud-based systems. During operations, auditors have read-only privileges, and batch auditing is supported. Our method involves generating a signature with the user's data, which includes the current system time to enhance the probability of generating a unique signature. This reduces storage expenses while maintaining data freshness.

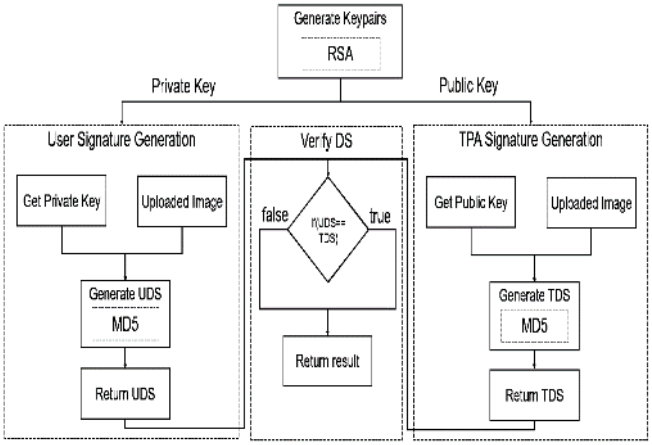

Fig. 3.3 Data Correctness and Verification Model

To achieve our objective, we have established an efficient system within our proposed architecture. As shown in fig. 3.3 TPA generates its own signature, utilizing all user characteristics. The system avoids storing data copies and does not disclose the private key during decryption to safeguard data accuracy. The TPA generates its signature at all times, and when a user saves or modifies data, their signature is updated, ensuring constant data freshness. The system operates in batch processing and supports the user's response time on the cloud without compromising data storage.

Our proposal suggests the utilization of asymmetric keys for implementing an access control mechanism. When a user decides to upload data to the cloud, a digital signature is generated using the user's private key. In the event that a third-party auditor needs to verify the integrity of the user's data, they can create a digital signature using the corresponding public key. This approach guarantees the preservation of data privacy for the user while enabling efficient auditing and verification processes to ensure the integrity of the data..

4. Cnn Train and Test Model:

To implement image compression, a dataset such as ImageNet (a subset of Kaggle dataset) can be used. The availability of label dataset is not required as object detection is not involved. The primary objective is to reduce the image's physical size by more than 50% while maintaining the visual quality of the image.

The DCT (Discrete Cosine Transform) is a commonly used lossy compression method that belongs to a family of discrete cosine transforms. It is a Fourier-related transform that offers high efficiency in image compression. In our implementation, we utilized a modified version of the DCT algorithm with a Quality Factor. This modification was necessary to control the quality of the compressed image, as compressing an image with a specific Quality Factor ensures that the image quality is not lost.

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

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

Table 1.1 Comparative Analysis of DCT and DWT

In general, the DWT and DCT techniques possess distinct strengths and weaknesses. The selection of either method relies upon the specific demands of the application and the inherent characteristics of the image undergoing compression.

In Figure 4.1, there is data presented regarding the original size and compressed sizes of five distinct images, measured in megabytes (MB) and kilobytes (KB) respectively. The original size of "Image 1" is noted as 1 MB, and after compression, it has been reduced to 250 KB. Observing the figure, it becomes evident that larger original images tend to exhibit relatively lower compression rates, leading to a smaller reduction in size compared to their original dimensions.[38,40]

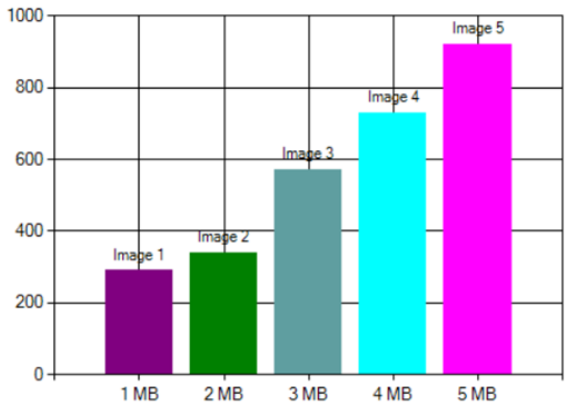

Fig. 4.1 Storage size difference between original image and compressed image

The figure 4.2 showcases different images and their corresponding PSNR values, which are used to measure the quality of the images based on their fidelity to the original source. In the first row, the image named "Camera Man" has a PSNR value of 37.04 for DCT, while in the second row, the same image has a slightly higher PSNR value of 37.37 for DWT. Moving on to the second set of rows, the image labeled "Rice" has a PSNR value of 39.04 for DCT, whereas in the next row, the PSNR value decreases to 37.7 for DWT for the same image [34-35].

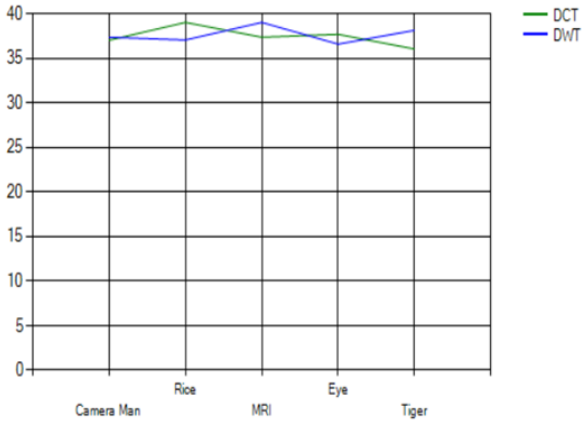

Fig 4.2 Images compressed by DCT and DWT and their respective PSNR Values

In figure 4.3 a comparison is presented between the proposed auditing model [36] and the SecACS model. The above depiction clearly illustrates that the proposed scheme demonstrates a reduced computational time in comparison to SecACS. Moreover, it is worth noting that increase in the computational time for the auditing process is directly proportional to increase in number of audit queries.[37,39]

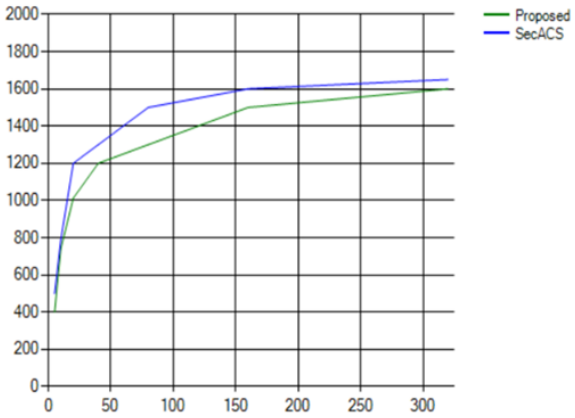

Fig. 4.3 Analysis of proposed auditing scheme and SecACS

5. Conclusion

The proposed framework for decentralized data access control allows authorized parties to share data while giving the data owner the ability to revoke access at any time. Our approach provides multi-layer security through a combination of data fragmentation and encryption. By dividing a single file into smaller pieces and encrypting them before storing them in the cloud, unauthorized access to the data requires the decryption of each fragment in order to reconstruct the original file. This multi-authority access control system offers a robust solution for protecting sensitive data shared in the cloud. Overall, our proposed framework is a promising solution that can be used in any remote storage system to ensure data security and privacy.

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 Elsevier

[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

[30] 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

[31] 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

[32] 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

[33] 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

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

[35] 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.

[36] 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

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

[38] 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.

[39] Rathod, S., Khobragade, R. N., Thakare, V. M., Walse, 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 , &Sushama L. Pawar. (2022). PRESERVING PRIVACY & 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