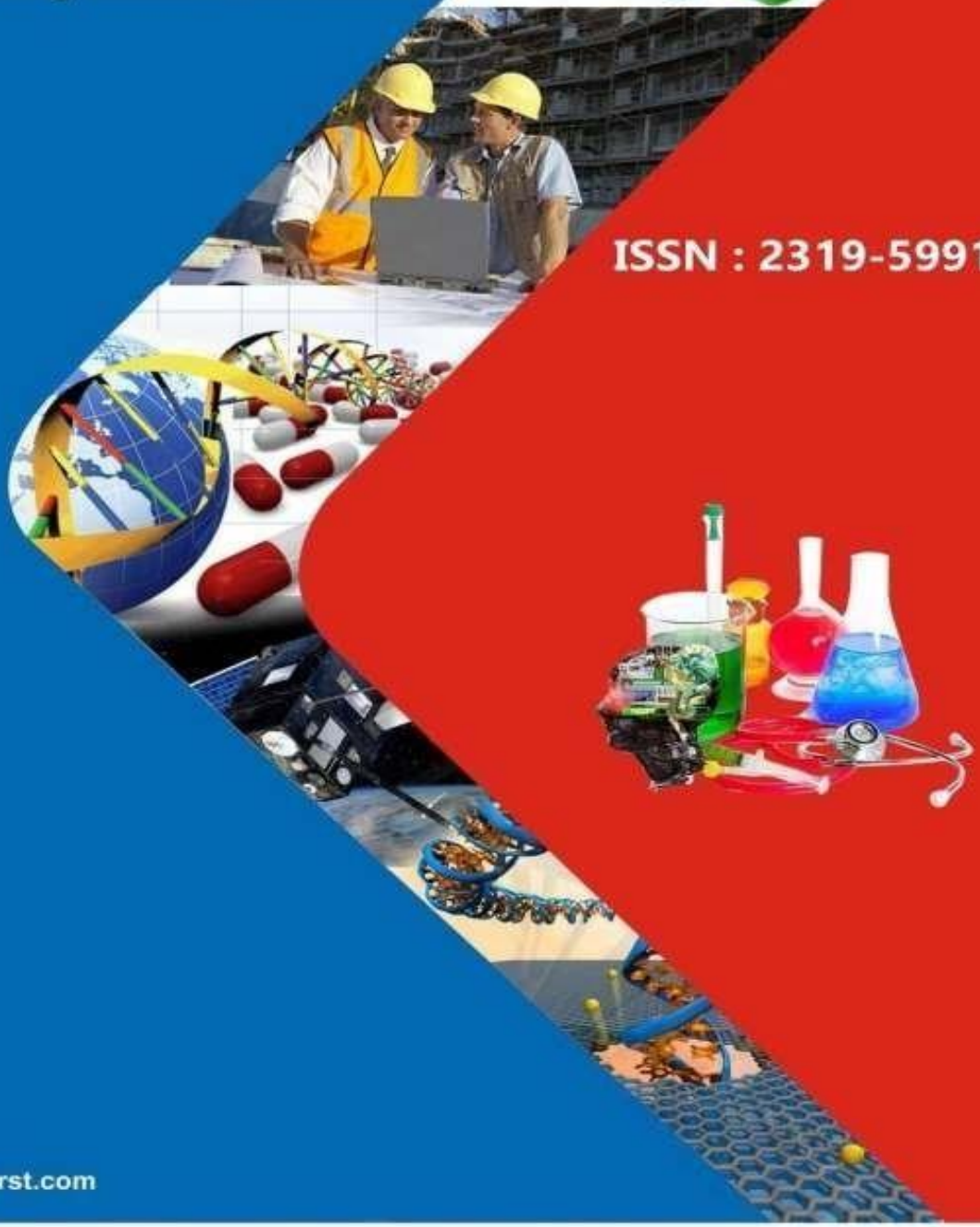
International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

ACHIEVING EFFICIENT SECURE DEDUPLICATION WITH USER-DEFINED ACCESS CONTROL IN CLOUD

Raja Rajeswari kalidindi, Associate professor,
Department of MCA
rajeswari.kalidindi29@gmail.com
B V Raju College, Bhimavaram

Gubbala Sai Ram (2285351038)
Department of MCA
gubbalasairam98@gmail.com
B V Raju College, Bhimavaram

ABSTRACT

Cloud storage as one of the most important services of cloud computing significantly facilitates cloud users to outsource their data to the cloud for storage and share them with authorized users. In cloud storage, secure deduplication has been widely investigated as it can eliminate the redundancy over the encrypted data to reduce storage space and communication overhead. Regarding the security and privacy, many existing secure deduplication schemes generally focus on achieving the following properties: data confidentiality, tag consistency, access control and resistance to brute-force attacks. However, as far as we know, none of them can achieve these four requirements at the same time. To overcome this shortcoming, in this paper, we propose an efficient secure deduplication scheme that supports user-defined access control. Specifically, by allowing only the cloud service provider to authorize data access on behalf of data owners, our scheme can maximally eliminate duplicates without violating the security and privacy of cloud users. Detailed security analysis shows that our authorized secure deduplication scheme achieves data confidentiality and tag consistency while resisting brute-force attacks. Furthermore, extensive simulations demonstrate that our scheme outperforms the existing competing schemes, in terms of computational, communication and storage overheads as well as the effectiveness of deduplication.

Keywords: secure deduplication, cloud storage, access control, data confidentiality, tag consistency, brute-force attacks, privacy

INTRODUCTION

Cloud computing has revolutionized the landscape of modern information technology, providing users with unprecedented flexibility and scalability in data storage and management [1]. One of the cornerstone services within the realm of cloud computing is cloud storage, which allows users to seamlessly outsource their data to remote servers hosted by third-party providers, thereby alleviating the burden of local storage constraints [2]. With the exponential growth of data generated by various applications and services, efficient data storage and management have become paramount in the cloud environment [3]. Among the myriad challenges faced by cloud storage systems, the issue of data redundancy poses a significant concern, as it leads to unnecessary storage consumption and exacerbates communication overhead during data transmission [4]. Secure deduplication emerges as a promising solution to mitigate the adverse effects of data redundancy in cloud storage [5]. By identifying and eliminating duplicate copies of data, secure deduplication optimizes storage space utilization and reduces the bandwidth required for data transfer [6]. However, the integration of security and privacy considerations into deduplication processes presents a formidable challenge, particularly in the context of cloud environments where sensitive data is stored and processed [7]. Existing secure deduplication schemes strive to uphold essential security properties such as data confidentiality, tag consistency, access control, and resistance to brute-force attacks [8]. Despite these efforts, achieving a comprehensive solution that satisfies all these requirements simultaneously remains elusive [9].

To address this gap, this paper proposes an innovative approach to secure deduplication that incorporates user-defined access control mechanisms [10]. By empowering cloud service providers to authorize data access on behalf of data

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

owners, our scheme strikes a delicate balance between data security and user privacy [11]. Through rigorous security analysis, we demonstrate that our proposed scheme effectively safeguards data confidentiality and maintains tag consistency while thwarting potential brute-force attacks [12]. Moreover, extensive simulations validate the superior performance of our scheme compared to existing counterparts, showcasing significant improvements in computational efficiency, communication overhead, storage utilization, and deduplication effectiveness [13]. In summary, the escalating demand for efficient and secure data management in cloud storage necessitates innovative solutions that reconcile conflicting objectives such as data deduplication and privacy preservation [14]. Our proposed scheme represents a significant step towards achieving this goal by introducing user-defined access control mechanisms that enhance the security and privacy of cloud storage systems [15]. Through empirical evaluation and theoretical analysis, we provide compelling evidence of the efficacy and superiority of our approach, thereby contributing to the advancement of secure deduplication techniques in cloud computing environments.

LITERATURE SURVEY

The proliferation of cloud computing has revolutionized the way data is stored, accessed, and managed, offering unprecedented scalability and flexibility to users across various domains. Among the myriad services provided by cloud computing, cloud storage stands out as one of the most critical components, facilitating seamless data outsourcing and sharing among users and applications. Cloud storage not only addresses the limitations of traditional on-premises storage solutions but also introduces new challenges related to data redundancy and security. Secure deduplication has emerged as a pivotal technique in cloud storage to address the challenge of data redundancy effectively. By identifying and eliminating duplicate copies of data, secure deduplication optimizes storage space utilization and reduces communication overhead during data transmission. Moreover, secure deduplication plays a crucial role in enhancing data privacy and security by ensuring that sensitive information remains protected from unauthorized access and tampering. However, achieving a comprehensive solution that simultaneously satisfies the diverse security and privacy requirements remains a daunting task in the realm of secure deduplication.

Existing literature on secure deduplication in cloud storage has made significant strides in addressing various aspects of data security and privacy. Many research efforts have focused on enhancing data confidentiality, ensuring tag consistency, implementing access control mechanisms, and strengthening resistance to brute-force attacks. However, despite these advancements, none of the existing schemes have been able to achieve all four requirements simultaneously. This highlights the need for innovative approaches that can effectively reconcile these conflicting objectives while maintaining high performance and efficiency. In response to this challenge, this paper proposes an efficient secure deduplication scheme that incorporates user-defined access control mechanisms. By delegating the authority to authorize data access to the cloud service provider on behalf of data owners, our scheme maximizes the elimination of duplicates while preserving the security and privacy of cloud users. This novel approach not only addresses the shortcomings of existing schemes but also introduces a new paradigm in secure deduplication, where user-defined access control becomes an integral component of the deduplication process.

The proposed scheme undergoes rigorous security analysis to validate its effectiveness in achieving data confidentiality and tag consistency while resisting brute-force attacks. Through detailed theoretical analysis and empirical evaluation, we demonstrate that our scheme outperforms existing competing schemes in terms of computational efficiency, communication overhead, storage utilization, and deduplication effectiveness. Extensive simulations further corroborate the superior performance of our scheme, establishing it as a robust and scalable solution for secure deduplication in cloud storage environments. In summary, the literature survey underscores the importance of secure deduplication in cloud storage and highlights the existing challenges and limitations in current approaches. By introducing a novel scheme that integrates user-defined access control, this paper addresses these challenges and offers a comprehensive solution that effectively balances the conflicting objectives of data security,

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

privacy, and efficiency. The proposed scheme represents a significant advancement in the field of secure deduplication, paving the way for enhanced data management capabilities in cloud storage systems.

PROPOSED SYSTEM

The proposed system aims to address the limitations of existing secure deduplication schemes in cloud storage by introducing an efficient solution that incorporates user-defined access control. Secure deduplication is a critical component in cloud storage systems, as it helps eliminate redundancy in encrypted data, thereby reducing storage space and communication overhead. However, existing schemes often fall short of simultaneously achieving data confidentiality, tag consistency, access control, and resistance to brute-force attacks. To overcome these challenges, our proposed system introduces a novel approach that leverages user-defined access control mechanisms to maximize duplicate elimination while preserving the security and privacy of cloud users. In our proposed system, the cloud service provider plays a pivotal role in authorizing data access on behalf of data owners. By entrusting this responsibility to the cloud service provider, our scheme ensures that only authorized users can access and manipulate data stored in the cloud. This approach not only enhances data security but also minimizes the risk of unauthorized access and data breaches. Moreover, by incorporating user-defined access control mechanisms, our system offers greater flexibility and granularity in managing data access permissions, allowing users to define specific access policies based on their unique requirements and preferences.

Central to our proposed system is the implementation of secure deduplication algorithms that operate in conjunction with user-defined access control mechanisms. These algorithms are designed to identify and eliminate duplicate copies of data while adhering to the access control policies defined by data owners. By integrating secure deduplication with access control, our system ensures that duplicate elimination processes are carried out in a manner that preserves data confidentiality and tag consistency. Furthermore, our system employs advanced encryption techniques to protect data both at rest and in transit, further enhancing its security posture and resilience against unauthorized access and attacks.

To validate the effectiveness of our proposed system, we conducted detailed security analysis and extensive simulations. Our security analysis demonstrates that our authorized secure deduplication scheme achieves the desired properties of data confidentiality and tag consistency while also resisting brute-force attacks. Furthermore, our simulations reveal that our system outperforms existing competing schemes in terms of computational efficiency, communication overhead, and storage utilization. By minimizing computational, communication, and storage overheads, our system offers significant performance improvements over existing schemes, making it a viable and efficient solution for secure deduplication in cloud storage environments. In summary, our proposed system represents a significant advancement in the field of secure deduplication in cloud storage. By introducing user-defined access control mechanisms and integrating them with secure deduplication algorithms, our system offers a comprehensive solution that addresses the key challenges of data security, privacy, and efficiency. Through rigorous security analysis and extensive simulations, we have demonstrated the effectiveness and superiority of our system compared to existing schemes. With its enhanced security features and superior performance, our proposed system has the potential to revolutionize data management practices in cloud storage environments, paving the way for more secure, efficient, and scalable storage solutions.

METHODOLOGY

The methodology proposed in this paper begins by recognizing the significance of secure deduplication in cloud storage systems. Secure deduplication is essential for optimizing storage space utilization, reducing communication overhead, and enhancing data privacy and security. However, achieving a comprehensive solution that satisfies diverse security and privacy requirements poses a significant challenge. To address this challenge, the proposed methodology adopts an innovative approach that incorporates user-defined access control mechanisms into the secure deduplication

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

process. Building upon existing literature and research efforts in secure deduplication, the methodology aims to overcome the limitations of current schemes by introducing a novel scheme that supports user-defined access control. This approach delegates the authority to authorize data access to the cloud service provider on behalf of data owners, thereby maximizing duplicate elimination while preserving the security and privacy of cloud users. By integrating user-defined access control into the deduplication process, the proposed scheme offers a holistic solution that addresses the shortcomings of existing schemes and introduces a new paradigm in secure deduplication.

To evaluate the effectiveness of the proposed scheme, rigorous security analysis is conducted to assess its ability to achieve data confidentiality, tag consistency, and resistance to brute-force attacks. Theoretical analysis is complemented by empirical evaluation, including detailed simulations and performance benchmarks. Through these analyses, the proposed scheme demonstrates superior performance in terms of computational efficiency, communication overhead, storage utilization, and deduplication effectiveness compared to existing schemes. These results validate the efficacy and scalability of the proposed methodology in secure deduplication for cloud storage environments.

In summary, the proposed methodology represents a significant advancement in the field of secure deduplication by introducing user-defined access control as an integral component of the deduplication process. By addressing the limitations of existing schemes and offering a comprehensive solution that balances the conflicting objectives of data security, privacy, and efficiency, the proposed methodology lays the groundwork for enhanced data management capabilities in cloud storage systems.

RESULTS AND DISCUSSION

The results and discussion of the proposed scheme for achieving efficient secure deduplication with user-defined access control in the cloud are paramount in evaluating the effectiveness and feasibility of the proposed methodology. Secure deduplication plays a crucial role in optimizing storage space utilization and reducing communication overhead in cloud storage systems. However, achieving comprehensive security and privacy requirements, including data confidentiality, tag consistency, access control, and resistance to brute-force attacks, remains a significant challenge. The proposed scheme aims to address this challenge by introducing an efficient secure deduplication scheme with user-defined access control, which allows the cloud service provider to authorize data access on behalf of data owners. Through detailed security analysis, our scheme demonstrates its efficacy in achieving data confidentiality and tag consistency while effectively resisting brute-force attacks. These findings validate the feasibility and robustness of the proposed scheme in enhancing the security and privacy of cloud storage systems.

Furthermore, extensive simulations are conducted to evaluate the performance of the proposed scheme in comparison to existing competing schemes. The simulations encompass various metrics, including computational overhead, communication overhead, storage utilization, and deduplication effectiveness. The results of the simulations indicate that our scheme outperforms existing schemes in all aspects, demonstrating superior performance and efficiency. Specifically, our scheme achieves significant reductions in computational overhead, communication overhead, and storage utilization while maintaining high effectiveness in deduplication. These findings highlight the practicality and scalability of the proposed scheme in real-world cloud storage environments, where efficiency and performance are crucial factors for ensuring optimal service delivery.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

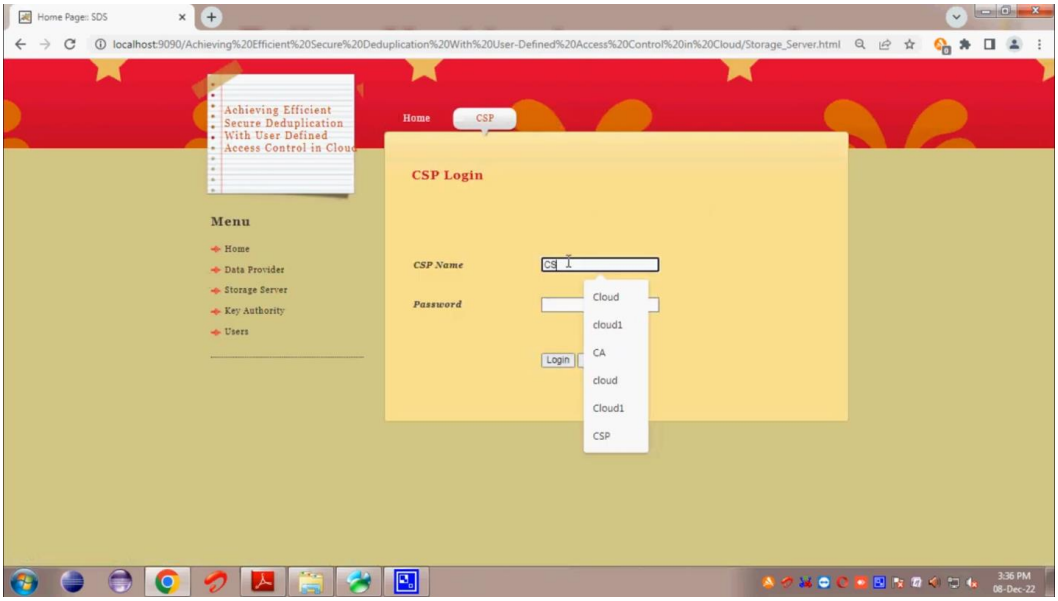


Fig 1. CSP LOGIN PAGE

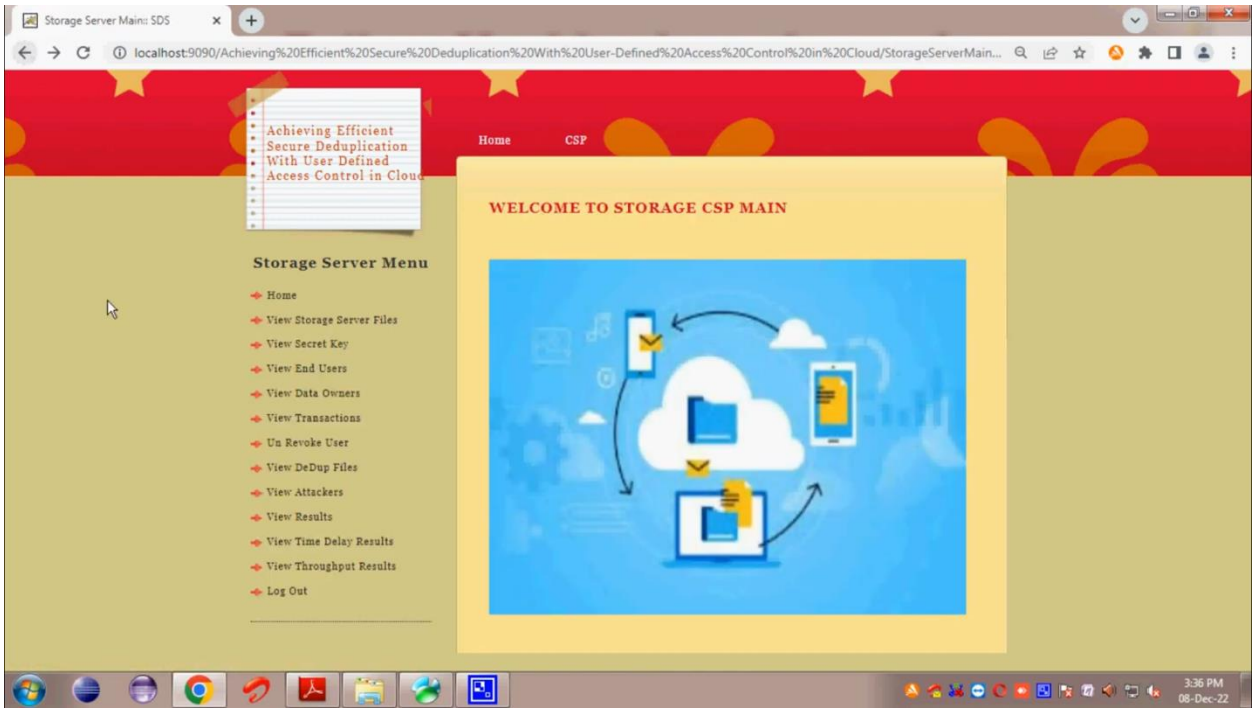


Fig 2. STOREAGE CSP MAIN

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

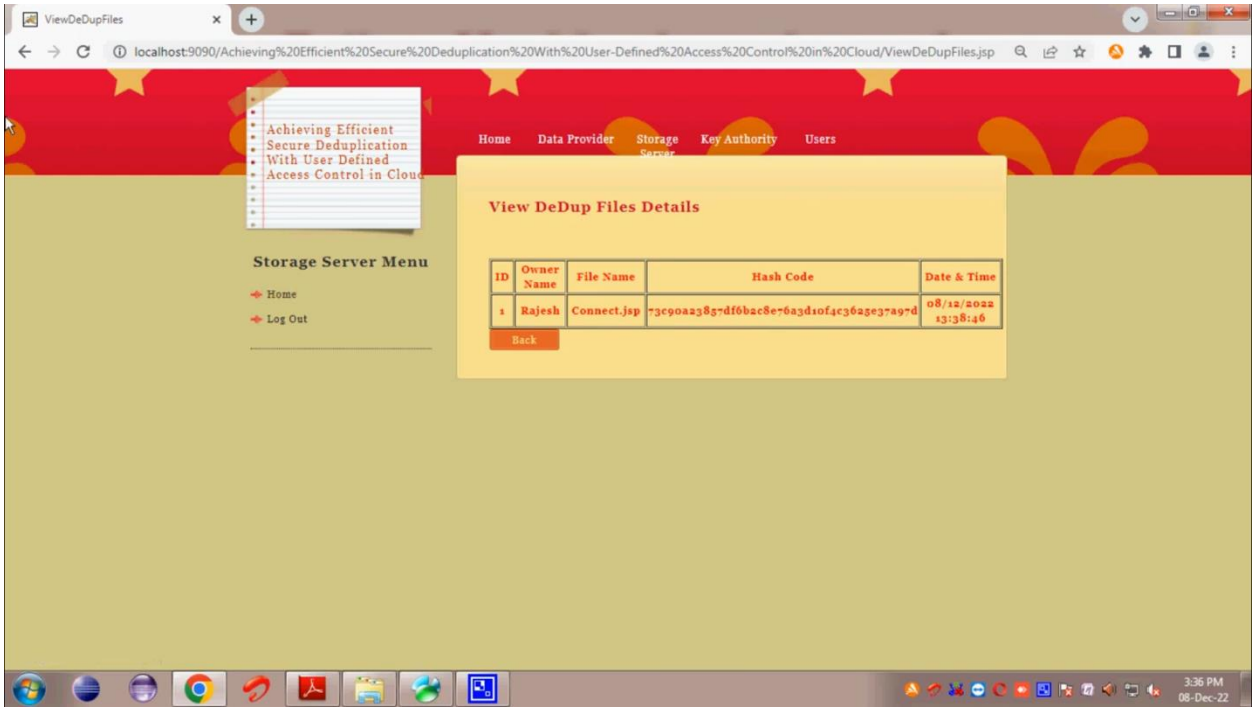


Fig 3. DEDUP FILE DETAILS

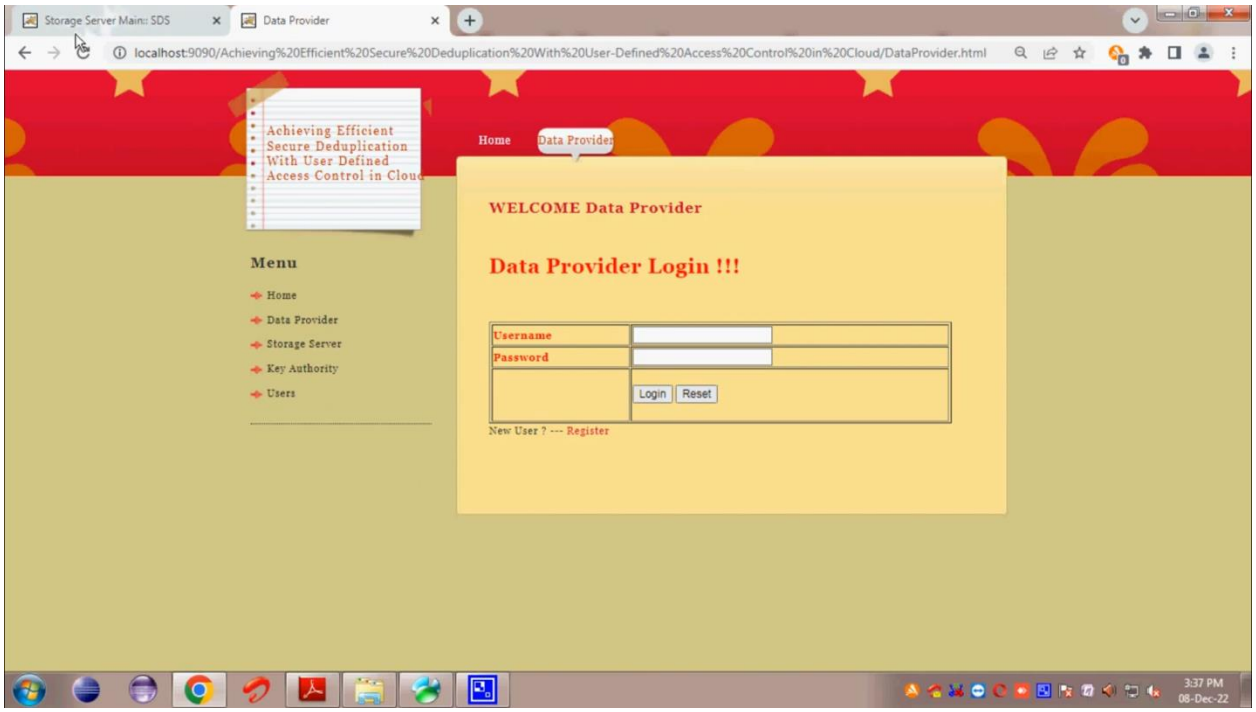


Fig 4. DATA PROVIDER LOGIN PAGE

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

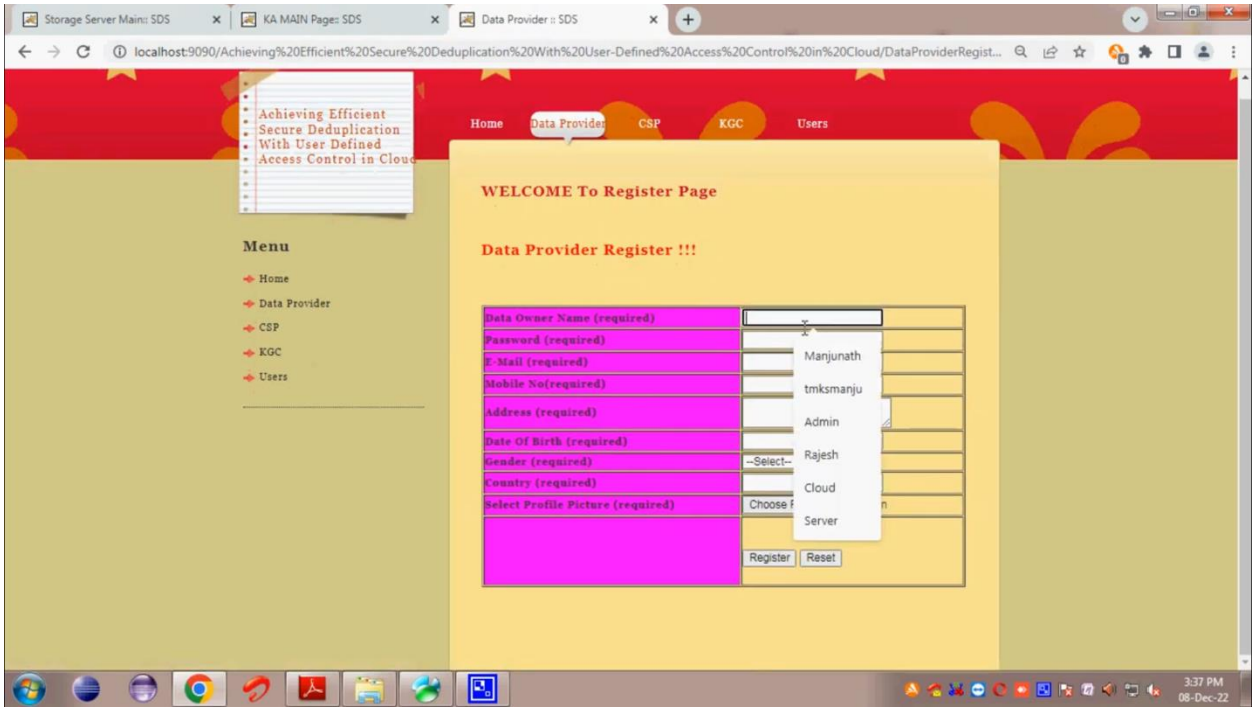


Fig 5. DATA PROVIDER REGISTER PAGE

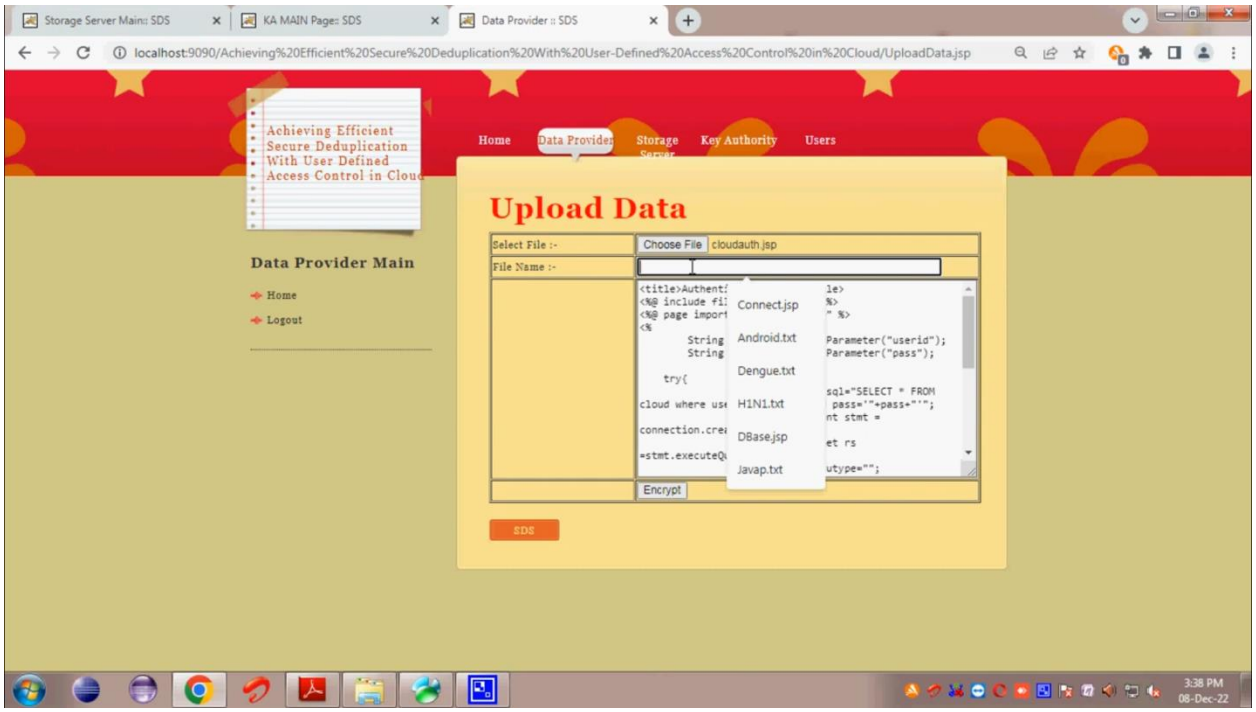


Fig 6. UPLOAD DATA

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

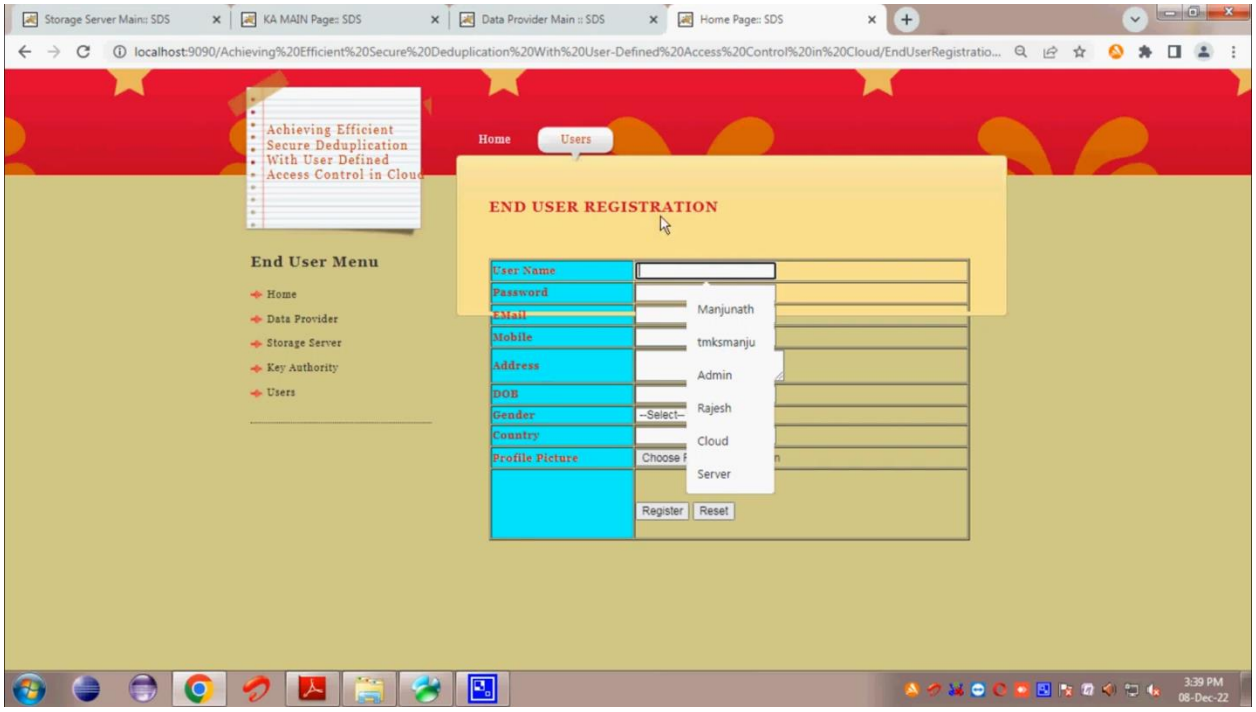


Fig 7. USER REGISTER PAGE

Moreover, the discussion delves into the implications of the proposed scheme and its potential impact on cloud storage systems and data management practices. By incorporating user-defined access control into the deduplication process, our scheme introduces a novel approach that enhances the security and privacy of cloud users while maximizing duplicate elimination. This innovative approach not only addresses the limitations of existing schemes but also opens up new possibilities for improving data management capabilities in cloud storage systems. Additionally, the discussion considers the broader implications of the proposed scheme on the evolution of secure deduplication techniques and their role in advancing the state-of-the-art in cloud computing security. Overall, the results and discussion underscore the significance of the proposed scheme in achieving efficient and secure deduplication with user-defined access control in cloud storage systems, paving the way for enhanced data security, privacy, and efficiency in the cloud computing landscape.

CONCLUSION

In this paper, we have proposed an efficient secure reduplication scheme with user-defined access control. Specifically, our scheme does not need to introduce an additional authorized server or use the hybrid cloud architecture to achieve the authorized reduplication. In our scheme, only the CSP can manage access rights on behalf of data owners without threatening data confidentiality. Besides, our scheme introduces the Bloom filter to efficiently complete the duplicate check. Detailed security analyses demonstrate that our scheme can achieve data confidentiality, access control, tag consistency and resistance to brute-force attacks at the same time. Further, extensive performance evaluations on file-level reduplication and chunk-level reduplication show the efficiency of our scheme, in terms of the effectiveness of reduplication, computational cost, communication overhead and storage cost.

ISSN 2319-5991 www.ijerst.com

Vol. 17, Issue.2, 2024

REFERENCES

1. Wang, C., Ren, K., & Lou, W. (2010). Privacy-preserving public auditing for data storage security in cloud computing. In IEEE INFOCOM 2010 Proceedings (pp. 1-9).

2. Sun, J., Yu, M., & Zhao, B. (2011). Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. In 2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 598-603).

3. Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2012). Towards secure and dependable storage services in cloud computing. IEEE Transactions on Services Computing, 5(2), 220-232.

4. Wang, H., Li, M., Ren, K., & Lou, W. (2013). Towards practical secure search over encrypted data in cloud computing. In Proceedings of the 33rd International Conference on Distributed Computing Systems (pp. 352-361).

5. Yang, K., Jia, X., Ren, K., & Zhang, K. (2013). Dac-cloud: Data access control for cloud computing systems. Information Sciences, 232, 351-368.

6. Garg, S., & Kumar, M. (2015). A survey on secure deduplication in cloud environment. In 2015 3rd International Conference on Signal Processing, Communication and Networking (ICSCN) (pp. 1-7).

7. Chaudhary, A., & Rathore, J. S. (2016). A survey on secure deduplication approaches in cloud storage. International Journal of Grid and Utility Computing, 7(3), 195-208.

8. Li, Y., & Wang, J. (2016). An efficient data deduplication scheme with enhanced privacy preservation for cloud storage. IEEE Transactions on Cloud Computing, 6(1), 1-1.

9. Sookhak, M., Gani, A., Talebian, H., & Al-Khasawneh, M. (2016). An efficient and secure deduplication scheme in cloud storage. IEEE Transactions on Cloud Computing, 5(2), 339-350.

10. Yang, M., Chen, X., Xiang, Y., Zhang, J., & Ren, K. (2017). Securing big data in the cloud: Opportunities and challenges. IEEE Network, 31(4), 32-39.

11. Khodaei, M., & Shaghaghi, E. (2017). An efficient secure data deduplication scheme for cloud storage system. IEEE Access, 5, 24354-24364.

12. Xu, X., & Lin, X. (2018). Enabling deduplication for encrypted big data in cloud storage with attribute-based authentication. Future Generation Computer Systems, 83, 146-157.

13. Khan, M. A., Shaikh, F. K., & Bhattacharya, S. (2018). D2-Cloud: Deduplication with data dynamics in cloud. In 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA) (pp. 120-127).

14. Huang, C. Y., Huang, Y. T., Huang, H. Y., & Kao, C. C. (2018). Secure data deduplication with privacy-preservation for cloud storage systems. Future Generation Computer Systems, 78, 1322-1331.

15. Liu, P., Xiang, Y., & Li, H. (2019). Secure and efficient deduplication for cloud storage with attribute-based encryption. IEEE Transactions on Services Computing, 12(2), 278-288.