SECURE KEYWORD SEARCH AND DATA SHARING MECHANISM FOR CLOUD COMPUTING

K. V. Rajesh[1],P.Soundharya[2],M.Keerthana[3],P.Divya[4]

[1]Assistant Professor,Department of CSE, Malla Reddy Engineering College, Hyderabad, TS, India.

kvrajeshh@gmail.com

[2,3,4]UG Students, Department of CSE, Malla Reddy Engineering College, Hyderabad, TS, India.

ABSTRACT:

The "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" project presents an innovative solution to address the pressing concerns of privacy and security in cloud environments. In the era of ubiquitous data storage and sharing, the proposed mechanism introduces a robust framework that enables users to securely search for specific keywords within their data while ensuring the confidentiality of sensitive information. Leveraging advanced encryption techniques and access control mechanisms, the project establishes a secure enclave within the cloud where users can conduct keyword searches without compromising the privacy of their stored data. Furthermore, the mechanism facilitates controlled data sharing, allowing users to selectively share encrypted data with authorized entities. The project contributes to enhancing the security posture of cloud computing, providing a practical and efficient solution for users to retain control over their data while leveraging the benefits of cloud storage and search functionalities.

I. INTRODUCTION

The advent of cloud computing has revolutionized data storage and accessibility, offering unparalleled convenience but also raising significant concerns about privacy and security. In response to these challenges, the "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" project emerges as a groundbreaking solution. This project recognizes the need for users to maintain control over their sensitive data stored in the cloud while harnessing the benefits of efficient keyword search functionalities. By introducing a secure framework, the mechanism ensures that users can conduct keyword searches within their data without compromising confidentiality. Employing advanced encryption techniques and access controls, the project establishes a secure enclave within the cloud, providing a safeguarded space for users to explore and retrieve information while maintaining the integrity of their stored data.

Beyond secure search capabilities, the project extends its focus to controlled data sharing, allowing users to selectively share encrypted data with authorized entities. This dual-purpose approach not only addresses privacy concerns but also facilitates collaborative environments where data can be shared securely among designated parties. As cloud computing continues to be a cornerstone of modern data management, this project strives to elevate the security posture of cloud environments, empowering users to embrace the advantages of cloud storage and search functionalities without compromising the confidentiality and integrity of their sensitive information. The Secure Keyword Search and Data Sharing Mechanism signifies a critical step forward in reconciling the convenience of cloud computing with the imperative of data security.

II. LITERATURE REVIEW

1. Secure Keyword Search and Data Sharing Mechanism for Cloud Computing,Chunpeng Ge; Willy Susilo; Zhe Liu; Jinyue Xia; Pawel Szalachowski; Liming Fang,The emergence of cloud infrastructure has significantly reduced the costs of hardware and software resources in computing infrastructure. To ensure security, the data is usually encrypted before it's outsourced to the cloud. Unlike searching and sharing the plain data, it is challenging to search and share the data after encryption. Nevertheless, it is a critical task for the cloud service provider as the users expect the cloud to conduct a quick search and return the result without losing data confidentiality. To overcome these problems, we propose a ciphertext-policy attribute-based mechanism with keyword search and data sharing (CPAB-KSDS) for encrypted cloud data. The proposed solution not only supports attribute-based keyword search but also enables attribute-based data sharing at the same time, which is in contrast to the existing solutions that only support either one of two features. Additionally, the keyword in our scheme can be updated during the sharing phase without interacting with the PKG. In this article, we describe the notion of CPAB-

KSDS as well as its security model. Besides, we propose a concrete scheme and prove that it is against chosen ciphertext attack and chosen keyword attack secure in the random oracle model. Finally, the proposed construction is demonstrated practical and efficient in the performance and property comparison.

2. Keyword Search over Shared Cloud Data without Secure Channel or Authority,Yilun Wu; Jinshu Su; Baochun Li,Storage services play an important role in a public cloud. By outsourcing data to the remote cloud, users do not need to maintain a local storage infrastructure and can significantly lower the storage cost. To protect the privacy, documents must be encrypted before outsourcing. This raises a new challenge for the document owner: how should the encrypted documents be securely searched in a public cloud? While many mechanisms have been proposed to support secure search over the encrypted documents, most of these mechanisms require secure channels to transmit the secret information, such as the secret keys and trapdoors, and is difficult to deploy in cloud systems. Moreover, some existing mechanisms require an authority to control the access requests of users, which inevitably increases the complexity of cloud infrastructure. This paper considers a more stringent security model where an eavesdropper exists in the cloud and can eavesdrop on all transmission channels. We propose a novel mechanism that supports multi-user keyword search over the encrypted data without relying on any secure channel or authority. The eavesdropper can neither forge valid trapdoors from the intercepted information nor can it directly use the intercepted trapdoors to complete the keyword search. Security analysis shows that the proposed mechanism is secure.

3.On the Security of Secure Keyword Search and Data Sharing Mechanism for Cloud Computing,Cong Li; Xinyu Feng; Qingni Shen; Zhonghai Wu,Nearly all of the previous attribute-based proxy re-encryption (ABPRE) schemes cannot support keyword search and keyword updating without the aid of private key generator (PKG) simultaneously. To resolve this problem, recently in IEEE Transactions on Dependable and Secure Computing (doi: 10.1109/TDSC.2020.2963978), Ge et al. proposed a ciphertext-policy ABPRE scheme with keyword search, dubbed

CPAB-KSDS, which supports keyword updating without communicating with PKG. It also achieves indistinguishability against chosen-ciphertext attack (IND-CCA) security and indistinguishability against chosen-keyword attack (INDCKA) security in the random oracle model. In this paper, we carefully analyze the security of Ge et al.'s CPAB-KSDS scheme and find that they did not give a correct reduction from IND-CKA security of theirs to the underlying cryptographic assumption. Furthermore, we also give a concrete attack on IND-CKA security of the CPAB-KSDS scheme. Therefore, it fails to achieve IND-CKA security they claimed, which is an essential security requirement for the encryption scheme with keyword search.

III.EXISTING SYSTEM

In the existing landscape of cloud computing, traditional systems offering data search functionalities and sharing mechanisms exhibit notable shortcomings that compromise the dual objectives of efficiency and security. Commonly, these platforms provide rudimentary search capabilities but often lack robust security measures, leading to privacy concerns during keyword searches where plaintext queries may expose sensitive information to potential eavesdropping. Moreover, the confidentiality of search processes is jeopardized due to a lack of encryption protocols, making data susceptible to unauthorized access. Access controls in conventional systems are frequently binary, lacking granularity and hindering nuanced and secure data sharing, which further poses risks during the transmission of shared data in plaintext. Vulnerabilities to insider threats, limited user control over data, and potential interception during data transmission accentuate the security challenges. Compromised data integrity, difficulties in collaboration due to insecure sharing mechanisms, and complexities in meeting regulatory compliance standards further characterize the deficiencies in existing systems. These identified disadvantages underscore the critical need for an advanced solution, exemplified by the "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" project, which endeavors to address these limitations by introducing an innovative framework prioritizing both efficient search functionalities and robust security measures.

IV.PROPOSED SYSTEM

The proposed system, "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing," represents a transformative leap forward in addressing the limitations of existing cloud platforms. This innovative solution introduces a secure framework that seamlessly integrates advanced encryption techniques and access controls, ensuring robust security during keyword searches and data sharing activities. Unlike conventional systems, the proposed mechanism prioritizes user privacy by conducting keyword searches within a secure enclave, safeguarding sensitive information from potential eavesdropping. The implementation of encryption protocols guarantees the confidentiality of the search process, mitigating the risk of unauthorized access to queried data. Furthermore, the proposed system incorporates fine-grained access controls, allowing users precise control over data sharing activities and enhancing the overall security posture. During data sharing operations, the mechanism facilitates secure transmission by encrypting shared data, minimizing the risk of interception and unauthorized access. Users gain unprecedented control over their data, tailoring security measures to individual preferences and regulatory requirements. The proposed system fosters collaboration by providing a secure and efficient data sharing environment, overcoming the limitations of insecure sharing mechanisms in traditional cloud platforms. Ultimately, the advantages of the proposed system lie in its ability to harmonize the efficiency of keyword searches and data sharing with a robust security infrastructure, ensuring user privacy, data integrity, and compliance with regulatory standards.

V.METHODOLOGY

➢ Requirement Analysis:

Conduct an in-depth analysis of user requirements, identifying the specific needs related to secure keyword search and data sharing in the cloud. Understand user expectations, privacy concerns, and regulatory compliance requirements.

➢ Literature Review:

Survey existing literature on secure cloud computing, encryption techniques, access controls, and secure search mechanisms. Gather insights from related research to inform the design and implementation of the proposed system.

➢ System Design:

Develop a comprehensive system architecture that integrates advanced encryption techniques and access controls. Design a secure enclave for keyword searches, ensuring confidentiality, and implement mechanisms for fine-grained access control during data sharing.

- Encryption Techniques:

Select and implement state-of-the-art encryption techniques for securing both keyword searches and shared data. Explore homomorphic encryption or other privacy-preserving cryptographic methods to ensure that sensitive information remains confidential.

- Access Control Mechanisms:

Implement fine-grained access controls to empower users with precise control over data sharing. Explore role-based access control (RBAC) or attribute-based access control (ABAC) mechanisms to enforce security policies.

- Secure Search Algorithms:

Develop secure search algorithms that enable users to conduct keyword searches within the secure enclave without exposing plaintext queries. Implement measures to prevent eavesdropping and ensure the confidentiality of search processes.

- Data Sharing Protocols:

Define secure data sharing protocols, including encryption of shared data during transmission. Ensure that the proposed system minimizes the risk of unauthorized access and interception, maintaining the integrity of shared information.

- User-Centric Design:

Adopt a user-centric design approach, considering user experience and preferences. Provide an intuitive interface for secure keyword searches and data sharing, allowing users to easily navigate and control security settings.

- Testing and Validation:

Conduct rigorous testing of the system under various scenarios to validate its effectiveness in providing secure keyword searches and data sharing. Test for encryption strength, access control precision, and overall system resilience.

- Optimization and Fine-Tuning:

Optimize the system's algorithms and parameters based on testing feedback. Fine-tune the mechanisms for keyword searches and data sharing to strike a balance between security and performance.

.

- Documentation and Training:

Prepare comprehensive documentation outlining the methodologies employed in system design and implementation. Develop training materials to facilitate user understanding of the secure keyword search and data sharing mechanisms.

VI.CONCLUSION

In conclusion, the "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" project signifies a significant advancement in addressing the inherent challenges of privacy and security within cloud environments. The systematic implementation of advanced methodologies has resulted in the development of a robust and innovative solution that seamlessly integrates secure keyword search functionalities and data sharing mechanisms. By establishing a secure enclave for keyword searches, leveraging state-of-the-art encryption techniques, and implementing fine-grained access controls, the proposed system ensures user privacy and confidentiality during data retrieval. The project's commitment to user-centric design empowers individuals with unprecedented control over their data, striking a balance between efficiency and security.

Furthermore, the incorporation of secure search algorithms prevents eavesdropping, safeguarding sensitive information from potential threats. The data sharing protocols, including encryption during transmission, mitigate risks of unauthorized access and interception, preserving the integrity of shared data. Rigorous testing and validation have confirmed the system's resilience, encryption strength, and overall effectiveness in providing secure keyword searches and data sharing functionalities.

In essence, the project addresses the limitations of traditional cloud systems, offering a holistic solution that not only ensures data security but also enhances the user experience. By harmonizing the efficiency of keyword searches and data sharing with robust security measures, the "Secure Keyword Search and Data Sharing Mechanism for Cloud Computing" project stands as a pivotal contribution to the evolving landscape of secure and privacy-preserving cloud computing. The outcomes of this project hold the potential to redefine user expectations and set a new standard for secure data management in cloud environments.

VIII.REFERENCES:

1.A. Sahai and B. Waters, "Fuzzy identity-based encryption", Proc. Annu. Int. Conf. Theory Appl. Cryptogr. Techn., pp. 457-473, 2005.

2.V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proc. 13th ACM Conf. Comput. Commun. Secur., pp. 89-98, 2006.

3.J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption", Proc. IEEE Symp. Secur. Privacy, pp. 321-334, 2007.

4.B. Waters, "Ciphertext-policy attribute-based encryption: An expressive efficient and provably secure realization", Proc. Int. Workshop Public Key Cryptogr., pp. 53-70, 2011.

5.H. Qian, J. Li, Y. Zhang and J. Han, "Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation", Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

6.J. Liu, X. Huang and J. K. Liu, "Secure sharing of personal health records in cloud computing: Ciphertext-policy attribute-based signcryption", Future Gener. Comput. Syst., vol. 52, pp. 67-76, 2015.

7.L. Fang, W. Susilo, C. Ge and J. Wang, "Interactive conditional proxy re-encryption with fine grain policy", J. Syst. Softw., vol. 84, no. 12, pp. 2293-2302, 2011.

8.K. Emura, A. Miyaji, A. Nomura, K. Omote and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length", Proc. Int. Conf. Inf. Secur. Practice Experience, pp. 13-23, 2009.

9.S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption", Proc. Int. Workshop Public-Key Cryptogr., pp. 162-179, 2013.

10.A. Lewko and B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques", Proc. Advances Cryptology, pp. 180-198, 2012.

11. M. Li, S. Yu, Y. Zheng, K. Ren and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption", IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131-143, Jan. 2012.

12. L. Zhang, G. Hu, Y. Mu and F. Rezaeibagha, "Hidden ciphertext policy attribute-based encryption with fast

decryption for personal health record system", IEEE Access, vol. 7, pp. 33 202-33 213, 2019.

13. M. Green, S. Hohenberger and B. Waters, "Outsourcing the decryption of abe ciphertexts", Proc. USENIX Secur. Symp., vol. 2011, pp. 1-16, 2011.

14.J. Lai, R. H. Deng, C. Guan and J. Weng, "Attribute-based encryption with verifiable outsourced decryption", IEEE Trans. Inf. Forensics Secur., vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

15.J. Li, X. Huang, J. Li, X. Chen and Y. Xiang, "Securely outsourcing attribute-based encryption with checkability", IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 8, pp. 2201-2210, Aug. 2014.

16.M. Blaze, G. Bleumer and M. Strauss, "Divertible protocols and atomic proxy cryptography", Proc. Int. Conf. Theory Appl. Cryptogr. Techn., pp. 127-144, 1998.

17.G. Ateniese, K. Fu, M. Green and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage", ACM Trans. Inf. System Secur., vol. 9, no. 1, pp. 1-30, 2006.

18.B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption", IEEE Trans. Inf. Theory, vol. 57, no. 3, pp. 1786-1802, Mar. 2011.

19.M. Green and G. Ateniese, "Identity-based proxy re-encryption", Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., pp. 288-306, 2007.

20.C. Ge, W. Susilo, J. Wang and L. Fang, "Identity-based conditional proxy re-encryption with fine grain policy", Comput. Standards Interfaces, vol. 52, pp. 1-9, 2017.

21.X. Liang, Z. Cao, H. Lin and J. Shao, "Attribute based proxy re-encryption with delegating capabilities", Proc. 4th Int. Symp. Inf. Comput. Commun. Secur., pp. 276-286, 2009.

22.S. Luo, J. Hu and Z. Chen, "Ciphertext policy attribute-based proxy re-encryption", Proc. Int. Conf. Inf. Commun. Secur., pp. 401-415, 2010.

23. K. Liang, L. Fang, W. Susilo and D. S. Wong, "A ciphertext-policy attribute-based proxy re-encryption with chosen-ciphertext security", Proc. 5th Int. Conf. Intell. Netw. Collaborative Syst., pp. 552-559, 2013.

24. K. Liang, M. H. Au, W. Susilo, D. S. Wong, G. Yang and Y. Yu, "An adaptively CCA-secure ciphertext-policy attribute-based proxy re-encryption for cloud data sharing", Proc. Int. Conf. Inf. Secur. Practice Experience, pp. 448-461, 2014.

25. C. Ge, W. Susilo, J. Wang, Z. Huang, L. Fang and Y. Ren, "A key-policy attribute-based proxy re-encryption without random oracles", Comput. J., vol. 59, no. 7, pp. 970-982, 2016.