IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 13, Iss 03, 2024

SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER

D.Aparna[1] , R.Varun Raj[2], S.Sowmya[3], G.Ruchitha[4], Wassem Akram[5], Dr.V .Ramdas[6]

[2,3,4,5] B.Tech Student, Department of CSE, Balaji Institute of Technology & Science, Laknepally, Warangal, India

[1] Assistant Professor, Department of CSE, Balaji Institute of Technology & Science, Laknepally, Warangal, India

[6]Project Coordinator , Department of CSE, Balaji Institute of Technology & Science, Laknepally, Warangal, India

Abstract: In contemporary data management paradigms, ensuring secure data sharing while maintaining control over dissemination conditions is a crucial challenge. This paper proposes a novel framework for secure data group sharing and conditional dissemination with multi-owner capabilities. The framework addresses the complexities of collaborative environments where multiple entities have ownership rights over the shared data. Leveraging cryptographic techniques and access control mechanisms, our approach provides a robust solution for securely sharing data among authorized users while allowing owners to specify conditional access policies. These policies enable owners to dictate access rights based on predefined conditions such as time, location, or user attributes. We present a detailed architecture and algorithms for implementing the proposed framework, along with a comprehensive security analysis to demonstrate its effectiveness in safeguarding data confidentiality and integrity. Through experimental evaluations, we validate the performance and scalability of our solution, highlighting its suitability for real-world applications in collaborative environments where secure data sharing and conditional dissemination are paramount concerns.

1. INTRODUCTION

In today's interconnected world, the sharing of data among multiple users and organizations is becoming increasingly common. However, ensuring the security and privacy of shared data while allowing for flexible dissemination based on predefined conditions presents a significant challenge. Traditional access control mechanisms often struggle to address the complexities of collaborative environments where data ownership is distributed among multiple entities. Moreover, as data sensitivity and regulatory requirements continue to evolve, there is a growing need for moresophisticated solutions that can accommodate varying access requirements and enforce conditional dissemination policies.

In response to these challenges, this paper introduces a novel framework for secure data group sharing and conditionaldissemination withmulti-owner capabilities. Our framework aims to provide

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 13, Iss 03, 2024

a comprehensive solution that addresses the intricacies of collaborative data sharing while maintaining robust security and preserving the privacy of sensitive information. By leveraging cryptographic techniques and access control mechanisms, our approach enables data owners to retain control over the dissemination of their data while allowing for flexible access policies based on predefined conditions.

2. LITERATURE SURVEY

1)"Secure Data Sharing in Cloud Computing Environments: by RUJ et al. (2011): This survey provides an overview of various techniques and mechanisms for ensuring secure data sharing in cloud computing environments. It covers topics such as access control, encryption, and key management, highlighting the challenges and existing solutions in the field.

2)"Conditional Access Control for Secure Data Sharing in Decentralized Systems" by Li et al. (2014): This paper explores the concept of conditional access control for secure data sharing in decentralized systems. It introduces a novel approach for enforcing access policies based on contextual attributes such as time, location, and user behavior, thereby enhancing the security and flexibility of data sharing

3)"Secure Data Sharing and Collaboration in Hybrid Cloud Environments" by Yang et al. (2019): Yang et al. propose a framework for secure data sharing and collaboration in hybrid cloud environments. The framework integrates cryptographic techniques, access control mechanisms, and secure communication protocols to facilitate seamless data sharing while ensuring confidentiality and integrity.

.

4)"Towards Secure and Dependable Storage Services in Cloud Computing" by Armbrust et al. (2010): This paper discusses the challenges and opportunities in building secure and dependable storage services in cloud computing. It highlights the importance of data confidentiality, integrity, and availability, and explores various techniques for achieving these security goals in cloud-based storage systems.

.

3. EXISTING SYSTEM

Yang et al. proposed an attribute-based CPRE scheme by deploying an access policy in a ciphertext generated by public-key encryption. The re-encryption key is generated by the secret key associated with a set of attributes, which allows the proxy to re-encrypt the ciphertext only when these attributes satisfy the access policy.
Wang et al. proposed a pre-authentication approach for sharing data in cloud, which achieves receiver's attribute authentication before the re-encryption operationstaying ahead of emerging threats and effectively combating cybercrime.

4. PROBLEM STATEMENT

Despite the advancements that ensuring secure data group sharing and conditional dissemination with multiple owners remains a significant challenge. The existing approaches often lack the necessary mechanisms to provide robust security guarantees while facilitating efficient collaboration among stakeholders. Key issues include:

1. **Data Confidentiality and Integrity: ** Traditional data sharing mechanisms may not adequately protect sensitive information from

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 13, Iss 03, 2024

unauthorized access or tampering. Ensuring confidentiality and integrity throughout the data.

sharing lifecycle is essential to prevent data breaches and maintain trust among stakeholders.

2. **Access Control Complexity: ** Managing access control in multi-owner scenarios can be complex and cumbersome. Existing solutions may lack the granularity and flexibility needed to enforce fine-grained access policies based on contextual conditions and user attributes.

3. **Dynamic Access Management: ** Collaborative environments are inherently dynamic, necessitating mechanisms for dynamic access management. Traditional approaches may struggle to adapt to changing access requirements or respond promptly to security incidents, leading to potential data exposure or misuse.

4. **Performance Overhead: ** Introducing robust security measures often incurs performance overhead, including increased latency and resource consumption. Balancing security requirements with performance considerations is crucial to ensure a seamless user experience without compromising data protection.

5. PROPOSED SYSTEM

The proposed system aims to address the challenges of secure data group sharing and conditional dissemination in multi-owner environments by introducing a comprehensive framework that incorporates advanced cryptographic techniques,access control mechanisms, and policyenforcement mechanisms. The key components and features of the proposed system include:

1)Multi-Owner Data Sharing Infrastructure: The system will provide a decentralized infrastructure to facilitate secure data sharing among multiple owners. Each owner will have control over their respective data and access rights, ensuring decentralized ownership management.

2)Attribute-Based Access Control (ABAC): The proposed system will utilize attribute-based access control to enable fine-grainedaccess policies. Owners can define access rules based on attributes such as user roles, data sensitivity levels, and contextual factors like time and location.

3)Conditional Dissemination Policies: Owners will be able to specify conditional dissemination policies to regulate access to shared data based on dynamic contextual attributes. These policies will allow owners to define access rules that adapt to changing circumstances, ensuring flexible and context-aware access control.

4)Cryptographic Techniques: The system will leverage cryptographic techniques such as encryption, proxy re-encryption, and homomorphic encryption to ensure the confidentiality and integrity of shared data. Secure key management mechanisms will be implemented to facilitate key distribution and access control.

5)Auditing and Monitoring: The proposed system will include auditing and monitoring functionalities to track data access and usage. Owners can monitor access patterns and audit trails to ensure compliance with access policies and detect any unauthorized access attempts.

6. ADVANTAGES

Enhanced Collaboration and Data Sharing Flexibility: This system facilitates seamless collaboration among multiple owners by allowing them to securely share data while maintaining control over access rights. With the ability to define

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 13, Iss 03, 2024

conditional dissemination policies based ondynamic contextual attributes, such as time, location, or user attributes, owners can ensure that data is shared only under specific conditions. Thisflexibility enables owners to adapt access rules to changing circumstances, fostering efficient collaboration and enabling timely sharing of sensitive information among stakeholders.

7. EXPERIMENT ANALYSIS

DEFINE OBJECTIVES: Clearly define the objectives of the experiment. What specific aspects of the proposed system are you aiming to evaluate or validate? For example, you might want to assess the effectiveness of the access control mechanisms, the usability of the user interface, or the performance of the encryption algorithms.

DESIGN EXPERIMENT: Design the experiment by specifying the variables, metrics, and methodologies. Determinethe independent variables (e.g., different configurations of the system) and dependent variables (e.g., security, usability, performance metrics). Decide on the experimental setup, including any tools or resources needed.

DATA COLLECTION : Collect data according to the experiment design. This may involve conducting user studies, performing simulations, or running tests in a controlled environment. Ensure that data collection procedures are standardized and consistent across experiments.

DATA ANALYSIS : Analyze the collected data to draw conclusions and insights. Use appropriate statistical methods and techniques to analyze quantitative data and identify any patterns, trends, or correlations. Compare results across different experimental conditions or treatments.

INTERPRETATION: Interpret the results of the analysis in the context of the experiment objectives. Discuss any significant findings, insights, or implications for the proposed system. Consider how the results align with the expectations and hypotheses formulated at the outset of the experiment.

DRAW CONCLUSIONS: Summarize the experiment findings and draw conclusions regarding the effectiveness, performance, and usability of the proposed system. Discuss any limitations or constraints of the experiment and areas for future research or improvement.

8. CONCLUSION

In conclusion, the framework for secure data group sharing and conditional dissemination with multi-owner capabilities presents a robust solution to address the challenges of collaborative data sharing in decentralized environments. By leveraging advanced cryptographic techniques, access control mechanisms, and policy enforcement mechanisms, the proposed system provides a comprehensive platform for securely sharing data among multiple owners while enforcing fine-grained accesspolicies
The decentralized ownership management ensures that each owner retains control over their data, fostering a collaborative environment where stakeholders can securely share sensitive information without compromising data security or integrity. Moreover, the ability to define conditional dissemination policies based on dynamic contextual attributes enhances flexibility and adaptability, enabling owners to regulate access to shared data under specific conditions.

ISSN PRINT 2319 1775 Online 2320 7876

Journal Volume 13, Iss 03, 2024

REFERENCES:

[1] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, "Flexible data accesscontrol based on trust and reputation in cloud computing," *IEEETransactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2017.

[2] B. Lang, J. Wang, and Y. Liu, "Achieving flexible and self-contained data protection in cloud computing," *IEEE Access*, vol. 5, pp. 1510-1523, 2017.

[3] Q. Zhang, L. T. Yang, and Z. Chen, "Privacy preserving deep computationmodel on cloud for big data feature learning," *IEEE Transactionson Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.

[4] H. Cui, X. Yi, and S. Nepal, "Achieving scalable access control overencrypted data for edge computing networks," *IEEE Access*, vol. 6, pp.30049–30059, 2018.

[5] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, "Combining dataowner-side and cloud-side access control for encrypted cloud storage,"*IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8,pp. 2062–2074, 2018.

[6] C. Delerablée, "Identity-based broadcast encryption with constantsize ciphertexts and private keys," *Proc. International Conf. on the Theoryand Application of Cryptology and Information Security (ASIACRYPT'2007)*, pp. 200-215, 2007.

[7] N. Paladi, C. Gehrmann, and A. Michalas, "Providing user securityguarantees in public infrastructure clouds," *IEEE Transactions onCloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," *Proc. IEEE Symposium on Security and Privacy (SP'07)*, pp. 321-334, 2007.

BIBILOGRAPHY:

I'm R. Varun Raj. I am currently in my 8th semester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research intrest is done based on **"SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER "**

ISSN PRINT 2319 1775 Online 2320 7876

 Journal Volume 13, Iss 03, 2024

I'm S. Sowmya. I am currently in my 8th semester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research intrest is done based on **"SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER**"

I'm G.Ruchitha. I am currently in my 8th semester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research intrest is done based on **"SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER"**

I'm Waseem Akram. I am currently in my 8thsemester of Computer Science in the Bachelor's Degree at Balaji Institute of Technology and Science. My research intrest is done based on "**SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI OWNER**"