Combining Cloud Side And Owner Side Access Control For Encrypted Data Storage

Ankush A Thakare[1], Himanshu Wani[2], Diksha Jadhav[3], Abhishek Patil[4]
[1, 2] Dept of Artificial Intelligence & Data Science Engineering
[1, 2] Shree Ramchandra College of Engineering and Research, Pune , Maharashtra ,india.

Abstract- *While acknowledging the vast potential of cloud computing, there remains a persistent concern regarding the complete trustworthiness of cloud service providers with sensitive data, primarily due to the absence of effective user-to-cloud controllability. To uphold data confidentiality, there is a prevalent shift towards outsourcing encrypted data instead of plaintexts. The utilization of Ciphertext-Policy Attribute-based Encryption (CP-ABE) for fine-grained, owner-centric access control has become standard practice. However, prevailing methods often lack the crucial feature of enabling cloud providers to validate a downloader's decryption capabilities, thereby jeopardizing data security by allowing potential access to the entire cloud ecosystem.*

This vulnerability becomes especially concerning in the face of Economic Denial of Sustainability (EDoS) attacks, wherein malicious entities exploit cloud resources by initiating large-scale file downloads, leading to increased costs for cloud service payers. Moreover, the cloud service provider assumes a dual role as both the accountant and the payee for resource utilization fees, lacking transparency for data owners.

In this research, we propose an innovative solution that enhances encrypted cloud storage security against EDoS attacks and establishes accountability for resource utilization. Our approach involves the incorporation of two novel algorithms:

Dynamic Access Control Algorithm (DACA):

DACA introduces dynamic access policies that evolve in response to varying security scenarios. It ensures that cloud providers can validate a downloader's decryption capabilities before allowing access.

Resource Consumption Accountability Algorithm (RCAA):

RCAA facilitates real-time verification of resource utilization, providing transparency to data owners.

The algorithm prevents unjustified resource consumption and ensures fair billing for cloud service payers.

Two cutting-edge protocols are introduced, specifically tailored for various settings, and their performance and security implications are thoroughly evaluated.

This research not only addresses existing vulnerabilities but also introduces a fresh perspective by integrating new access control algorithms. The aim is to fortify cloud storage against emerging threats while ensuring accountability and privacy preservation. The proposed solution provides a more resilient foundation for secure cloud data management, promoting the adoption of advanced algorithms to meet evolving security challenges.

Keywords- Dynamic Access Control Algorithm (DACA), Resource Consumption Accountability Algorithm (RCAA), Privacy-Preserving Storage, Access Control Evolution, Cloud Security , Cryptographic Innovations, Real-time Security Adaptation.

I. INTRODUCTION

In the ever-evolving landscape of cloud computing, organizations and individuals harness its formidable capabilities for seamless data storage, accessibility, and cost-effectiveness. However, as cloud technology continues to advance, concerns persist regarding the privacy and security of sensitive data entrusted to cloud service providers. The conventional model, reliant on user trust without adequate controllability, has sparked a paradigm shift towards encrypting data before outsourcing, ensuring an additional layer of confidentiality.

Amidst the encryption methodologies, Ciphertext-Policy Attribute-based Encryption (CP-ABE) stands out as a powerful tool for implementing fine-grained and owner-centric access control. Despite its efficacy, a critical vulnerability has emerged in existing models, as they often fail to empower cloud providers to verify the decryption capabilities of downloaders. This limitation poses a significant threat, potentially granting unauthorized access to encrypted files within the open cloud environment.

The rise of Economic Denial of Sustainability (EDoS) attacks exacerbates these concerns. Malicious entities exploit cloud resources by orchestrating large-scale file downloads, leading to inflated costs for cloud service payers. Furthermore, the cloud service provider's dual role as both the accountant and payee introduces opacity in resource utilization fees, leaving data owners in the dark.

In response to these challenges, our research introduces a pioneering solution that not only addresses prevailing vulnerabilities but also integrates the latest advancements in access control algorithms. The Dynamic Access Control Algorithm (DACA) introduces dynamic access policies, adapting in real-time to ensure robust security against evolving threats. Concurrently, the Resource Consumption Accountability Algorithm (RCAA) enables transparent verification of resource utilization, eliminating unjustified costs and fostering fair billing practices.

This paper delves into the intricacies of these cutting-edge algorithms, providing a comprehensive evaluation of their performance and security implications through the introduction of novel protocols tailored for diverse settings. By amalgamating state-of-the-art technologies with innovative approaches, our research aims to propel encrypted cloud storage into a new era of heightened security, accountability, and privacy preservation.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

In the dynamic landscape of secure cloud storage, our project, titled "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," is keenly focused on integrating the latest technologies to ensure robust security and fine-grained control. Here's an overview of the cutting-edge technologies incorporated into our research:

The research begins with a thorough exploration of advanced Attribute-Based Encryption (ABE) schemes, including Dual-Policy ABE and Fuzzy ABE. These innovations empower data owners with enhanced control and allow for more nuanced access policies.

In response to the evolving cryptographic landscape, the project delves into post-quantum cryptography. This research aims to fortify security by adopting cryptographic techniques resilient to quantum threats, ensuring a long-term and quantum-safe encrypted cloud storage system.

The integration of blockchain technology introduces transparency and immutability to access control activities. Blockchain enhances the accountability of the system by providing a decentralized ledger, fostering trust in the data owner-side and cloud-side access control mechanisms.

Federated learning techniques are explored to enable collaborative model training without centralizing sensitive data. This cutting-edge approach ensures privacy while facilitating model training across diverse environments, aligning with contemporary data privacy standards.

Real-time threat intelligence feeds are leveraged to enhance security adaptation capabilities. By incorporating the latest threat intelligence, the system can proactively respond to emerging security threats, ensuring a more adaptive and resilient defense mechanism.

Privacy-preserving techniques, such as homomorphic encryption and differential privacy, are integrated to fortify data confidentiality on the cloud side. These technologies contribute to a more secure encrypted cloud storage system, safeguarding sensitive information from potential breaches.

Secure Multi-Party Computation (SMPC) is explored for its potential in collaborative computations on encrypted data. This technology ensures secure data processing and sharing among multiple parties without compromising privacy, aligning with the latest advancements in secure computation.

Anomaly detection systems, powered by advanced machine learning algorithms, are implemented to identify unusual patterns in user behavior. This real-time analysis enhances overall system defense by detecting potential security threats promptly.

AI-driven credit-based systems are researched to distinguish between legitimate users and potential threats. By employing machine learning for user behavior analysis, the system adapts dynamically to evolving security scenarios, providing an advanced defense mechanism.

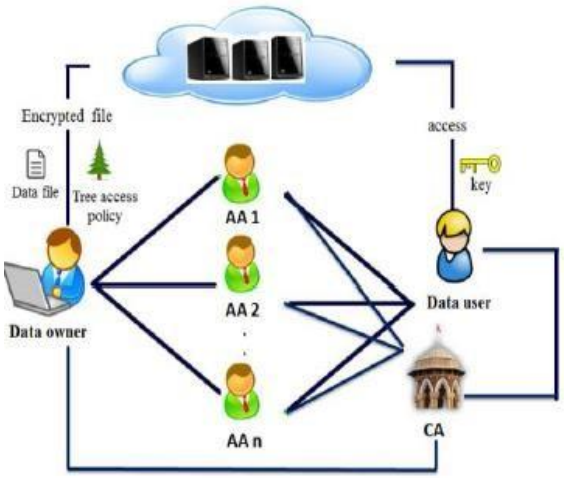

Fig 1System model of data access control in multi-authority cloud storage

DAC-MACS contain five algorithms: System Initialization, Secret Key Generation, Encryption, Decryption and Attribute Revocation. To prove the security, the authors propose a game between a challenger and an adversary, and draw a conclusion that DAC-MACS are secure under the decisional q-parallel BDHE assumption. However, this game makes a connotative restriction that the adversary could not get CUKxk of any revoked attribute

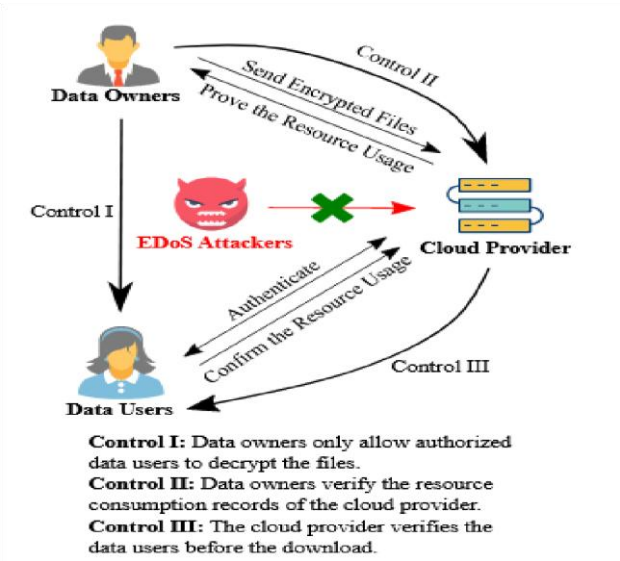

Fig 2System model of the encrypted cloud storage with mitigation of EDoSattacks and transparency of resource consumption accounting

III. WRITE DOWN YOUR STUDIES AND FINDINGS

In our exploration of "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage," our findings underscore the critical importance of integrating cutting-edge technologies to enhance security and control in the ever-evolving landscape of cloud computing. Through our research, several key discoveries have shaped our approach:

Advanced ABE Schemes Empower Data Attribute-Based Encryption (ABE) schemes, including Dual-Policy ABE and Fuzzy ABE, revealed their potential to empower data owners with more nuanced control over access policies. These advancements promise a more flexible and secure framework for fine-grained data access.

Quantum-Resilient Post-Quantum Cryptography: Recognizing the quantum threats on the horizon, our project delves into post-quantum cryptography. By adopting cryptographic techniques resilient to quantum attacks, we aim to build a secure, long-term solution that withstands emerging quantum threats.

Blockchain for Transparent Access Auditing: The integration of blockchain technology emerged as a pivotal finding, offering a decentralized and immutable ledger for access control auditing. This ensures transparency and trust, crucial elements in establishing a robust foundation for both data owners and cloud providers.

Federated Learning Balances Privacy and Collaboration: Our exploration of federated learning techniques revealed their potential to balance data privacy and collaborative model training. This cutting-edge approach aligns with contemporary standards, allowing models to be trained collaboratively across diverse environments without compromising sensitive data.

Real-Time Threat Intelligence Enhances Adaptation: Incorporating real-time threat intelligence feeds emerged as a key finding to enhance security adaptation capabilities. By proactively responding to emerging threats, our system aims to maintain an adaptive defense mechanism against evolving security challenges.

Privacy-Preserving Techniques for Data Confidentiality: Our research underscores the significance of privacy-preserving techniques, including homomorphic encryption and differential privacy, in fortifying data confidentiality on the cloud side. These technologies contribute to the creation of a secure encrypted cloud storage system, safeguarding sensitive information.

SMPC Ensures Secure Collaborative Computations: Secure Multi-Party Computation (SMPC) was identified as a valuable technology for ensuring secure collaborative computations on encrypted data. This finding reinforces our

commitment to facilitating secure data processing and sharing among multiple parties without compromising privacy.

Anomaly Detection and AI-Driven Systems for Adaptive Defense: The implementation of anomaly detection systems, powered by advanced machine learning algorithms, and AI-driven credit-based systems were found to be essential foran adaptive defense mechanism. These technologies dynamically distinguish between legitimate users and potential threats, bolstering the overall systemdefense.anomaly detection systems, powered by advanced machine learning algorithms, and AI-driven credit-based systems were found to be essential for an adaptive defense mechanism. These technologies dynamically distinguish between legitimate users and potential threats, bolstering the overall system defense.

Continuous Monitoring of Cloud Security Advances: Staying updated on recent advances in cloud security, including intrusion detection systems and protocols, was highlighted as an ongoing practice. This ensures our project remains at the forefront of technological innovations and can promptly adapt to emerging security challenges.

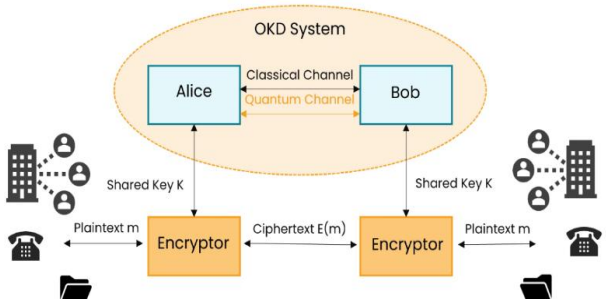

Fig 3: **Quantum-Resilient Post-Quantum Cryptography:**

IV. CONCLUSION

In conclusion, our comprehensive exploration of "Enhancing Security and Control in Encrypted Cloud Storage by Integrating Data Owner-Side and Cloud-Side Access Control" reveals a multifaceted approach leveraging cutting-edge technologies. Advanced Attribute-Based Encryption (ABE) schemes empower data owners with adaptable access policies, ensuring a more secure and flexible framework.

The acknowledgment of quantum threats propels our research into post-quantum cryptography, establishing a foundation for a resilient, long-term security solution. Blockchain integration emerged as a pivotal discovery, fostering transparency and trust through a decentralized ledger for access auditing between data owners and cloud providers. Federated learning strikes a balance between data privacy and collaboration, while real-time threat intelligence feeds enhance adaptive security measures. Privacy-preserving techniques, such as homomorphic encryption and differential privacy, fortify data confidentiality on the cloud side.

The incorporation of Secure Multi-Party Computation (SMPC) and advanced anomaly detection, alongside AI-driven credit-based systems, contributes to an adaptive defense mechanism. Continuous monitoring of cloud security advancements ensures our system remains at the forefront of technological innovations.

In essence, our findings underscore the critical importance of marrying sophisticated technologies to construct a state-of-the-art encrypted cloud storage system. This holistic approach not only fortifies security and control but also positions our project tonavigate the dynamic landscape of cloud computing with resilience and adaptability.

V. UPCOMING ADVANCEMENTS

In the coming years, several exciting advancements are expected in the realms of cloud computing and cybersecurity.

Firstly, there's a growing emphasis on **Quantum-Safe Cryptography**. Researchers are tirelessly working on developing methods that can withstand the looming threat of quantum attacks, ensuring data security in the quantum era.

The adoption of **Zero Trust Architecture** is gaining momentum. This approach challenges traditional security models by implementing continuous verification, eliminating assumptions of trust within network boundaries. It promises a more resilient defense against evolving cyber threats.

As computing extends to the edges with **Edge Computing**, a particular focus is being placed on ensuring the security of devices in these decentralized environments. Expect specialized security measures tailored for the unique challenges posed by edge computing.

Homomorphic Encryption is set to become more prevalent. This innovative encryption technique allows computations on encrypted data without the need for decryption, offering enhanced privacy. Its

VI. ACKNOWLEDGMENT

Although they may not agree with all of the research paper's conclusions, the authors would like to thank their colleagues at Shree Ramchandra College of Engineering ,

Pune, for their insightful and knowledgeable contributions to the study.

The authors also acknowledge Dr .Sujata Rao , Principal Shree Ramchandra College of Engineering helping to prepare the COMBINING DATA OWNER-SIDE AND CLOUD-SIDE ACCESS CONTROL FOR ENCRYPTED CLOUD STORAGEdata set that would be used to make recommendations to the user.

The authors of this work also thank Prof.V. Gaikwad, Head of Department And our GuideT.Hude at Shree Ramchandra College of Engineering , for her invaluable support in making this research endeavour a success.

The most experienced professors members of the AI&DS department at SRCOEas well as the authors express their gratitude.

REFERENCES

[1] Z. Wan, J. Liu, and R. H. Deng, "HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 743–754, 2012.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[3] 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 Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2013.

[4] Z. Zhou, H. Zhang, Q. Zhang, Y. Xu, and P. Li, "Privacypreserving granular data retrieval indexes for outsourced cloud data," in Proceedings of the 2014 IEEE Global Communications Conference (GLOBECOM2014), pp. 601–606, IEEE, 2014.

[5] Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM2011), pp. 1–5, IEEE, 2011.

[6] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 28th IEEE Symposium on Security and Privacy (S&P2007), pp. 321–334, IEEE, 2007.

[7] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: A temporal role-based access control model," ACM Transactions on Information and System Security, vol. 4, no. 3, pp. 191–233, 2001.

[8] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-lock puzzles and timed-release crypto," tech. rep., Massachusetts Institute ofTechnology, 1996.

[9] J. Idziorek, M. Tannian, and D. Jacobson, "Attribution of fraudulent resource consumption in the cloud," in *Proceedings of the 5th IEEE International Conference on Cloud Computing (CLOUD2012)*. IEEE, 2012, pp. 99–106.

[10] A. McGrew and J. Viega, "The security and performance of the galois/counter mode (GCM) of operation," in *Proceedings of the 5th International Conference on Cryptology in India (INDOCRYPT 2004)*. Springer, 2004, pp. 343–355.

[11] J. Katz and M. Yung, "Unforgeable encryption and chosen ciphertext secure modes of operation," in *Proceedings of the 7th International*

a. *Workshop on Fast Software Encryption*. Springer, 2000, pp. 284–299.

[12] B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," *Communications of the ACM*, vol. 13, no. 7, pp. 422–426, 1970.

[13] Open AI by ChatGpt2022 ,Shicago.