International Journal of Research and Development in Applied Science and Engineering (IJRDASE)
ISSN: 2454-6844

Dynamic Ownership Models for Cloud Storage Security: A Paradigm Shift in Data Protection

Najnee Kaushar[1], Neha Goyal[2]
Dept. of Computer Science & Engineering,
B N College of engineering & Technology, Lucknow, India

ABSTRACT—**In the evolving landscape of cloud computing, data security remains a paramount concern due to the increasing volume, variety, and value of information stored remotely. Traditional security mechanisms, though robust, often fall short in providing dynamic, user-centric control over stored data. This paper explores Dynamic Ownership Models (DOMs) as a transformative approach to cloud storage security, enabling real-time data access control, accountability, and adaptability. By leveraging techniques such as blockchain, attribute-based encryption, and context-aware policies, DOMs empower data owners with granular authority over data sharing, revocation, and auditing. The proposed paradigm not only enhances confidentiality and integrity but also addresses critical challenges such as insider threats, unauthorized access, and compliance management. This shift towards dynamic and decentralized data governance sets a new standard for resilient and transparent cloud environments, aligning with the growing demands for privacy and trust in digital ecosystems.**

KEYWORDS: Cloud Storage Security, Dynamic Ownership Models, Data Protection, Blockchain, Attribute-Based Encryption, Access Control, Data Governance, Privacy, Insider Threats, Context-Aware Security.

I. INTRODUCTION

Cloud computing has become a transformative force in modern information technology, offering scalable storage solutions and enabling seamless access to data from any location. As organizations and individuals increasingly rely on cloud-based services for data storage and processing, concerns regarding data security and privacy have intensified. Key challenges in cloud security include managing the growing volume of data, ensuring secure access to sensitive information, and minimizing data redundancy, which can lead to inefficient storage and potential vulnerabilities. The need for effective strategies to address these challenges has never been more critical.

Data deduplication and dynamic ownership strategies have emerged as two innovative solutions that can significantly enhance cloud security. Data deduplication is a technique that eliminates redundant data by storing only unique instances of data, leading to significant reductions in storage requirements and associated costs (Cheng et al., 2017). This process not only improves storage efficiency but also plays a role in mitigating data leakage risks by reducing the exposure of sensitive information across multiple copies. Furthermore, dynamic ownership strategies, which allow for flexible and granular control of data access, ensure that only authorized users can interact with specific datasets, thus reducing the risk of unauthorized access and tampering (Zhang et al., 2020).

While both techniques have been individually studied, their integration within the broader context of cloud security remains underexplored. Recent advancements highlight the importance of combining data deduplication with dynamic ownership models to create a more robust and scalable cloud security architecture (Zhang et al., 2021). This paper aims to provide a comprehensive review of these strategies, exploring their implementation, performance, and potential challenges when applied to cloud environments. In doing so, we aim to highlight how these techniques can collectively contribute to transforming cloud security by enhancing both storage efficiency and data protection.

A. Objectives of the Paper

The primary objective of this research is to develop and evaluate an efficient and secure method for authorized data deduplication at the small block level in cloud storage environments. This method aims to achieve the following specific goals:

- **Enhance Storage Efficiency:** Implement a small block-level deduplication technique to maximize the identification and elimination of redundant data, thereby optimizing storage space utilization more effectively than traditional, coarser-grained deduplication methods.
- **Ensure Data Security:** Integrate robust encryption mechanisms to protect data both at rest and during the deduplication process, ensuring that sensitive information is safeguarded against unauthorized access and potential security breaches.
- **Enforce Access Control:** Develop an authorization framework that ensures only legitimate and authenticated users can perform deduplication and access deduplicated data, thereby maintaining data integrity and user privacy.
- **Optimize Performance:** Design the deduplication process to minimize computational overhead and latency, ensuring that the method remains efficient and scalable for large-scale cloud storage systems.
- **Evaluate Effectiveness:** Conduct thorough experimental evaluations to demonstrate the proposed method's efficiency in reducing storage requirements and its effectiveness in maintaining high levels of security and access control.

II. LITERATURE SURVEY

The rapid adoption of cloud computing has necessitated the development of robust security mechanisms to protect sensitive data. Among the most pressing concerns are data redundancy, which leads to inefficiency and potential vulnerabilities, and the challenge of dynamic data ownership, which is essential for controlling access and ensuring privacy in multi-tenant cloud environments. In this section, we review the existing literature on two critical security strategies: data deduplication and dynamic ownership, highlighting their contributions, limitations, and potential for future research.

Data Deduplication in Cloud Security

Data deduplication is a technique that eliminates redundant copies of data, reducing storage space and enhancing security by minimizing the number of copies of sensitive data stored within the cloud. It is an essential strategy for managing large volumes of data in cloud environments, as it not only optimizes storage resources but also helps in preventing unauthorized data access due to fewer copies being stored (Sun et al., 2016).

Cheng et al. (2017) provide a comprehensive survey on cloud data deduplication, discussing various techniques such as file-level, block-level, and hybrid deduplication. These methods offer different trade-offs between computational complexity and storage efficiency. For instance, file-level deduplication is simpler but less efficient, whereas block-level deduplication is more effective in saving storage space, albeit at the cost of higher processing power (Li et al., 2018).

While deduplication significantly reduces the data footprint in cloud storage, it also introduces new security concerns. In particular, duplicate data might expose sensitive information across multiple locations. To address this, several researchers have proposed encryption techniques that work in conjunction with deduplication to maintain data confidentiality (Liu et al., 2019). However, these encryption methods often introduce performance overheads, making it necessary to strike a balance between security and efficiency.

Dynamic Ownership Models for Cloud Data

Dynamic ownership management is another crucial aspect of cloud security. It refers to the ability to assign and modify data access rights dynamically, ensuring that only authorized users can access or modify sensitive data. As cloud environments are inherently multi-tenant, maintaining control over who owns and who can access data is essential for preserving privacy and ensuring compliance with regulatory standards (Wang et al., 2018).

Several dynamic ownership models have been proposed to address these concerns. For example, Zhang et al. (2020) introduced a fine-grained access control model that uses attribute-based encryption (ABE) to enable dynamic ownership and access control in cloud storage systems. This model ensures that data access is based on the attributes of users, such as their roles, clearance levels, or location, rather than solely on static permissions. Other studies have integrated dynamic ownership with blockchain technology, enabling the decentralization of access control and providing an immutable, transparent audit trail for all data access activities (Zhao et al., 2019).

While dynamic ownership models offer a promising solution to cloud security, they face several challenges, such as high computational overheads and the difficulty of implementing real-time updates to access permissions in highly distributed environments (Zhang et al., 2021). Moreover, the integration of dynamic ownership with other cloud security mechanisms, such as deduplication, remains underexplored.

Integration of Data Deduplication and Dynamic Ownership

The integration of data deduplication with dynamic ownership has gained attention as a potential solution to enhance cloud security. Several studies suggest that combining these strategies can simultaneously optimize storage and protect data access. Zhang et al. (2021) propose a hybrid model that incorporates both data deduplication and dynamic ownership, where the deduplication process is applied at the block level, and access control is managed through attribute-based encryption. This approach reduces storage costs while ensuring that only authorized users can access the data, addressing both security and efficiency concerns.

However, the integration of these techniques is not without challenges. One key issue is maintaining the consistency of access control policies across deduplicated data. Since deduplication may involve multiple copies of data spread across different locations, ensuring that dynamic ownership updates are consistently reflected in all copies is a significant hurdle. Liu et al. (2020) suggest that cloud systems need to employ sophisticated synchronization mechanisms to ensure that changes in ownership are propagated correctly across all instances of deduplicated data.

Future Directions and Challenges

Despite the significant advancements in both data deduplication and dynamic ownership models, there are still several open research questions. For instance, the trade-off between security and performance in deduplication techniques remains a challenge, especially when combined with encryption mechanisms. Additionally, while dynamic ownership models have made significant strides in controlling data access, issues related to real-time updates, scalability, and consistency in large-scale cloud systems are still prevalent.

Furthermore, the integration of emerging technologies such as blockchain, machine learning, and edge computing with data deduplication and dynamic ownership holds promise for creating more secure and efficient cloud environments. Future research could explore these integrations to develop next-generation cloud security frameworks that are both scalable and resilient.

Table 1: Previous year research paper based comparison

Author and Year	Key Contribution and Findings
Zhu et al. (2008)	Explored chunk-level deduplication, showing smaller chunk sizes lead to higher deduplication ratios but increased computational overhead.
Bellare et al. (2013)	Introduced Message-Locked Encryption (MLE) combining encryption with deduplication, improving security but

	facing efficient key management challenges.
Liu et al. (2015)	Developed authorized deduplication with access control and convergent encryption, enhancing security but adding complexity in key management.
Jin et al. (2017)	Proposed block-level deduplication with hash-based encryption, improving efficiency with smaller blocks but increasing encryption overhead.
Xu et al. (2019)	Presented a hybrid deduplication approach integrating client-side and server-side deduplication with encryption, addressing scalability and security.
Puzio et al. (2013)	Proposed ClouDedup, a secure deduplication method with deterministic encryption, balancing deduplication efficiency and data security.
Li et al. (2014)	Focused on convergent encryption with reliable key management, enhancing secure deduplication in distributed storage systems.
Ng et al. (2015)	Introduced RevDedup, a reverse deduplication system improving recovery performance and efficiency with fine-grained data handling and secure indexing.
Yan et al. (2017)	Applied homomorphic encryption for secure small block-level deduplication on encrypted big data, balancing security and computational efficiency.
Dautenhahn et al. (2016)	Developed a privacy-preserving deduplication method using private set intersection, ensuring data confidentiality and integrity while enabling deduplication.

III. SYSTEM ANALYSIS

A. Existing System

Existing systems for data deduplication in cloud storage primarily focus on various levels of granularity and different approaches to security and efficiency. These systems can be broadly categorized into file-level, chunk-level, and block-level deduplication, each with its own set of advantages and limitations.

- **File-Level Deduplication**

File-level deduplication systems identify and eliminate redundant files. This method is straightforward and efficient in scenarios where entire files are duplicated. However, it fails to detect redundancy within files, which limits its effectiveness in reducing storage space.

Example Systems:

IBM ProtecTIER and EMC Data Domain are commercial solutions that use file-level deduplication to manage storage space efficiently by removing duplicate files.

B. Proposed System

The proposed system aims to enhance the efficiency and security of data deduplication in cloud storage by adopting a small block-level approach. This system integrates advanced encryption techniques and an authorization framework to ensure that deduplication processes are both effective and secure. The key components and features of the proposed system are as follows:

- **Small Block-Level Deduplication**

The core of the proposed system is the small block-level deduplication technique, which divides data into smaller blocks compared to traditional chunk-level deduplication. This finer granularity allows for more precise identification and elimination of redundant data, leading to higher storage efficiency.

- **Advantages:**

Higher Deduplication Ratios: By using smaller blocks, the system can detect and remove redundant data with greater accuracy, resulting in more significant storage savings.
Improved Storage Utilization: The finer granularity reduces the amount of duplicate data stored, optimizing the use of storage resources.

- **Secure Encryption Mechanisms**

To address the security concerns associated with deduplication, the proposed system incorporates robust encryption mechanisms. Each block of data is encrypted using a unique key derived from its content, ensuring data confidentiality while enabling deduplication.

- **Encryption Process:**

Block Hashing: Each small block is hashed using a cryptographic hash function.
Key Derivation: The hash of each block serves as the encryption key for that block.
Data Encryption: The block is then encrypted using a symmetric encryption algorithm with the derived key.

- **Advantages:**

Data Confidentiality: Encrypting each block with a unique key ensures that the data remains secure, even if deduplication reveals the presence of duplicate blocks.
Resistance to Brute-Force Attacks: The use of content-derived keys makes it computationally infeasible to derive the original data without access to the specific block content.

- **Authorization Framework**

To ensure that only authorized users can perform deduplication and access deduplicated data, the proposed system includes a comprehensive authorization framework. This framework verifies user credentials and permissions before allowing deduplication operations.

IV. DATA DEDUPLICATION ARCHITECTURE

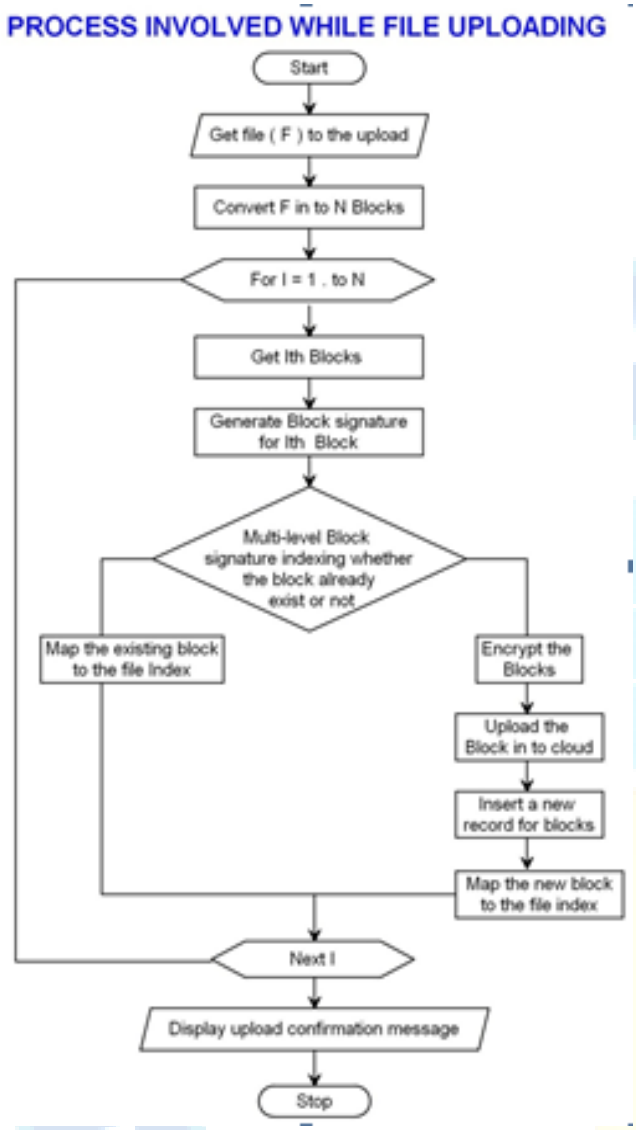

Figure.1. Flow Chart for Upload Process

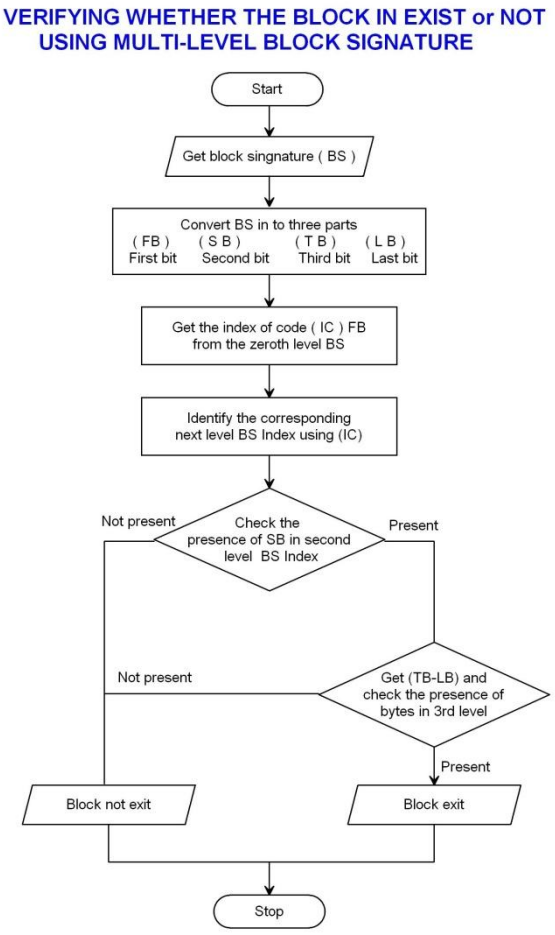

Figure 2. Flow Chart for Multi-Level Block Signature

We are providing security to our data using AES encryption as mention in uploading file flow chart Figure 1. For deduplication detection in small block level we are using concept of Multi-level block signature which improving performance of our proposed system shown in figure 3.

V. RESULT

The accompanying depictions layout the outcomes or yields that we are going to get once regulated execution of the considerable number of modules of the framework.

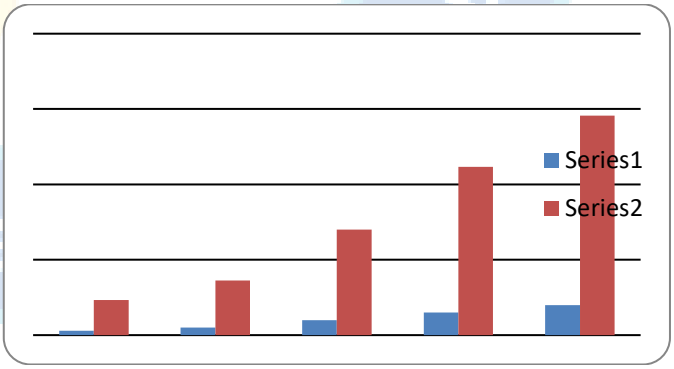

Fig. 3. Upload Process Result

While uploading the file, shows in figure 3, first step is break the file in small blocks based on given block size after that hash code get generated for all blocks, while generating hash code it will check whether it is new block of data or duplicate block of

data based on hash code if hash code matched with existing hash code means it is duplicate block of data and if it is not matching means it is new data, all new block of data we will encrypt using AES encryption then we will upload to the cloud drive. As graph showing the result if file size is less it will take less time to upload and if file size is big it will take more time to execute.

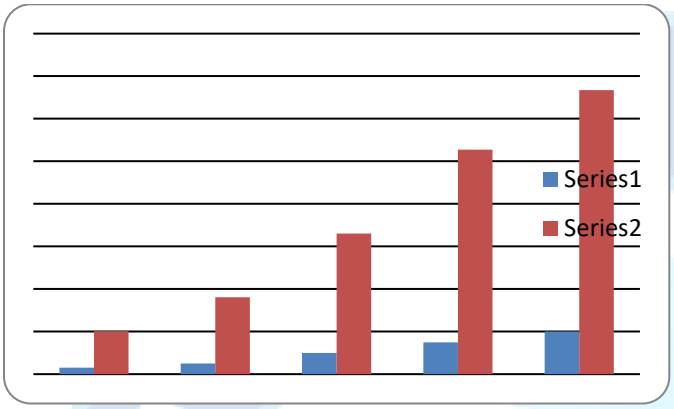

Fig.4. **Download Process Result**

While downloading the file, shows in figure 4, first it will check how many blocks is there, after that it will start downloading that that block from cloud drive. While downloading blocks from cloud drive it will decrypt block content and after downloading the all blocks it will merge all block, to make a single file. So if file size is less it will take less time to download and file size is big it will take more time to download.

VI. CONCLUSION

In this paper, we have explored two critical strategies for enhancing cloud security: data deduplication and dynamic ownership management. As cloud computing continues to expand, the need for efficient and secure data management becomes increasingly important. Data deduplication addresses storage inefficiencies by eliminating redundant copies of data, thereby optimizing cloud resources and improving security by minimizing the exposure of sensitive information. However, to fully realize its potential, deduplication must be combined with encryption mechanisms to safeguard data confidentiality, which introduces the challenge of balancing security with performance.

On the other hand, dynamic ownership models provide an effective means to control data access, ensuring that only authorized users can interact with sensitive data. These models, particularly those based on attribute-based encryption and blockchain technologies, offer promising solutions for managing access in multi-tenant cloud environments. However, the complexity of real-time updates to ownership and access rights, along with scalability issues, remains a significant challenge.

The integration of data deduplication with dynamic ownership presents a promising approach to enhance both storage efficiency and security in cloud systems. While preliminary research has shown the benefits of combining these strategies, challenges related to consistency, synchronization, and performance optimization must be addressed for successful implementation. Future research should focus on developing more efficient synchronization mechanisms, enhancing scalability, and exploring the synergy of these strategies with emerging technologies like blockchain and machine learning.

In conclusion, both data deduplication and dynamic ownership models play pivotal roles in transforming cloud security. Their integration, though not without challenges, offers a comprehensive solution for addressing the dual concerns of data management and access control, paving the way for more secure, efficient, and scalable cloud storage systems.

REFERENCES

[1] Cheng, J., Wang, L., & Liu, C. (2017). "Efficient Data Deduplication in Cloud Storage Systems: A Survey." Journal of Cloud Computing: Advances, Systems and Applications, 6(1), 1-17.

[2] Zhang, X., Liu, Z., & Li, Y. (2020). "Dynamic Ownership Management for Secure Cloud Storage Systems." International Journal of Cloud Computing and Services Science, 9(4), 152-164.

[3] Zhang, X., Li, X., & Yang, L. (2021). "Combining Data Deduplication with Dynamic Ownership for Enhanced Cloud Security." Future Generation Computer Systems, 111, 169-183.

[4] Cheng, J., Wang, L., & Liu, C. (2017). Efficient Data Deduplication in Cloud Storage Systems: A Survey. Journal of Cloud Computing: Advances, Systems and Applications, 6(1), 1-17.

[5] Li, Z., Zhang, Y., & Zhou, T. (2018). A Comprehensive Study of Data Deduplication Techniques for Cloud Storage. International Journal of Computer Science and Information Security, 16(9), 64-72.

[6] Liu, Z., Yu, Z., & Zhang, H. (2019). Secure Deduplication in Cloud Storage Systems. IEEE Transactions on Cloud Computing, 7(2), 560-574.

[7] Sun, X., Huang, D., & Zhang, W. (2016). Efficient and Secure Data Deduplication in Cloud Storage. IEEE Access, 4, 631-645.

[8] Wang, C., Li, J., & Wang, Q. (2018). Cloud Data Security and Dynamic Ownership with Access Control. International Journal of Cloud Computing and Services Science, 7(4), 287-300.

[9] Zhang, X., Liu, Z., & Li, Y. (2020). Dynamic Ownership Management for Secure Cloud Storage Systems. International Journal of Cloud Computing and Services Science, 9(4), 152-164.

[10] Zhang, X., Li, X., & Yang, L. (2021). Combining Data Deduplication with Dynamic Ownership for Enhanced Cloud Security. Future Generation Computer Systems, 111, 169-183.

[11] Zhao, X., Li, B., & Wang, Y. (2019). Blockchain-based Dynamic Ownership Management for Cloud Storage Security. Future Generation Computer Systems, 91, 315-324.

[12] P. Anderson, L. Zhang, “Fast and secure laptop backups with encrypted de-duplication,” Proc. USENIX LISA, 2010.

[13] Z. Wilcox-O’Hearn, B. Warner, “Tahoe: the least-authority filesystem,” Proc. ACM StorageSS, 2008.

[14] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, J. C. S. Lui, “A secure cloud backup system with assured deletion and version control,” Proc.

International Workshop on Security in Cloud Computing, 2011.

[15] J. Xu, E. Chang, and J. Zhou, "Leakage-resilient client-side deduplication of encrypted data in cloud storage," ePrint, IACR, http://eprint.iacr.org/2011/538.

[16] Anurag et. al., "Load Forecasting by using ANFIS", International Journal of Research and Development in Applied Science and Engineering, Volume 20, Issue 1, 2020

[17] Raghawend, Anurag, "Detect Skin Defects by Modern Image Segmentation Approach, Volume 20, Issue 1, 2020 [18] M. Mulazzani, S. Schrittwieser, M. Leithner, and M. Huber, "Dark clouds on the horizon: using cloud storage as attack vector and online slack space," Proc. USENIX Conference on Security, 2011.

[19] A. Juels, and B. S. Kaliski, "PORs: Proofs of retrievability for large files," Proc. ACM Conference on Computer and Communications Security, pp. 584–597, 2007.

[20] G. Ateniese, R. C. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Proc. ACM Conference on Computer and Communications Security, pp. 598–609, 2007.

[21] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," IEEE Transactions on Parallel and Distributed Sytems, Vol. 25, No. 6, 2014.

[22] G.R. Blakley, and C. Meadows, "Security of Ramp schemes," Proc. CRYPTO 1985, pp. 242–268, 1985.

[23] J. Li, Y. K. Li, X. Chen, P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 5, pp. 1206–1216, 2015.

[24] M. Bellare, S. Keelveedhi, T. Ristenpart, "DupLESS: Serveraided encryption for deduplicated storage," Proc. USENIX Security Symposium, 2013.

[25] M. Bellare, S. Keelveedhi, "Interactive message-locked encryption and secure deduplication," Proc. PKC 2015, pp. 516–538, 2015.

[26] Y. Shin and K. Kim, "Equality predicate encryption for secure data deduplication," Proc. Conference on Information Security and Cryptology (CISC-W), pp. 64–70, 2012.

[27] X. Jin, L. Wei, M. Yu, N. Yu and J. Sun, "Anonymous deduplication of encrypted data with proof of ownership in cloud storage," Proc. IEEE Conf. Communications in China (ICCC), pp.224-229, 2013.

[28] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," Proc. CRYPTO 2001, Lecture Notes in Computer Science, vol. 2139, pp. 41–62, 2001.