ISSN PRINT 2319 1775 Online 2320

Research paper Volume 11, Iss 4, 2022

Ensuring Integrity: A Fine-Grained Approach to Query Results Verification in Encrypted Cloud Data Design and Analysis

Dr.P.LaxmiKanth [0000-0001-7395-5121] #1, **Murali Mohan T**#2[0000-0001-5612-4318]

[1]Associate Professor, Department of CSE, Sri Vasavi Engineering College (A), (Approved By Aicte, New Delhi And Permanently Affiliated To Jntuk, Kakinada), Pedatadepalli, Tadepalligudem-534101.
Andhra Pradesh, India.
[2] Professor, Department of Computer Science and Engineering,
Swarnandhra Institute of Engineering & Technology
Narsapur, West Godavari, A.P.

Corresponding author Email: pydipalalaxmikanth@gmail.com
drtmm512@gmail.com

ABSTRACT

The cloud sector has attracted an unprecedented amount of interest from a wide range of businesses, including those in the software, BPO, healthcare, education, and other industries, in the present day. Notwithstanding the considerable increase in the adoption of cloud computing, it is important to highlight the deficiencies of current cloud service providers in terms of providing comprehensive data privacy via encryption and message digest mechanisms for data authorization. It is worth noting that cloud servers may display a degree of deceit by intentionally excluding qualified outcomes in order to optimize computational resources and reduce communication latency. This article proposes and thoroughly examines a mechanism for verifying query results that is secure, readily integrable, and fine-grained, thereby addressing the critical privacy gap in cloud data. This innovative method permits users to determine data authorization and evaluate the quality of each data file within an encrypted query results set. The proposed methodology utilizes the widely recognized MD5/SHA1 algorithms for message digest in order to produce brief signature keys. These keys are of utmost importance in the process of authenticating data, guaranteeing that users can have confidence in the soundness of the results of their queries while safeguarding the privacy of sensitive data. This paper provides valuable insights into the efficacy and resilience of the suggested mechanism by conducting an exhaustive analysis. It thereby contributes to the ongoing discussion surrounding the improvement of privacy and security in cloud computing environments.

Key Words: Message Digest Algorithm, Encryption, Data Integrity, Authorization, Cloud Server.

1. Introduction

Cloud computing has become an essential component of modern information ecosystems, serving as a critical hub for the processing and storage of data across a wide range of domains. Notwithstanding their widespread usage and critical nature, cloud servers pose intrinsic difficulties that compromise the confidentiality and security of data. The fundamental concept of cloud computing is the effortless transfer of data from local hardware to remote systems, which are frequently situated in geographically distant locations from the end-user. The data housed in these remote systems, which are accessible via the internet and intermediated by a multitude of servers, transforms into an invaluable asset for users.

Nevertheless, as we traverse the vast domain of cloud computing, a conspicuous constraint becomes apparent: the automated retention of user data on remote systems as opposed to local hardware. Data consumers are obligated to traverse the digital environment and establish connections with remote servers in order to retrieve their stored information [1]. Although there is no denying the convenience of remote data access, a significant concern arises regarding the prevalent method by which cloud service providers (CSPs) store sensitive data in plain text within their storage repositories.

ISSN PRINT 2319 1775 Online 2320
Research paper Volume 11, Iss 4, 2022

Regardless of the differentiation between private and public cloud users, cloud service providers frequently store data in an exposed and unencrypted fashion in the present environment. This methodology presents a significant obstacle as it exposes and renders vulnerable sensitive and valuable data susceptible to unauthorized intrusion. Consequently, it becomes critical to enhance the security measures pertaining to data access on modern cloud servers.

This scholarly article examines the complexities of the aforementioned complex issue, investigating the deficiencies of commonly used cloud server methodologies and suggesting novel approaches to enhance data protection. By conducting an extensive analysis of security vulnerabilities and a thorough examination of the current state of cloud computing, this paper aims to make a scholarly contribution to the ongoing discussion surrounding the enhancement of data privacy in the era of cloud dominance.

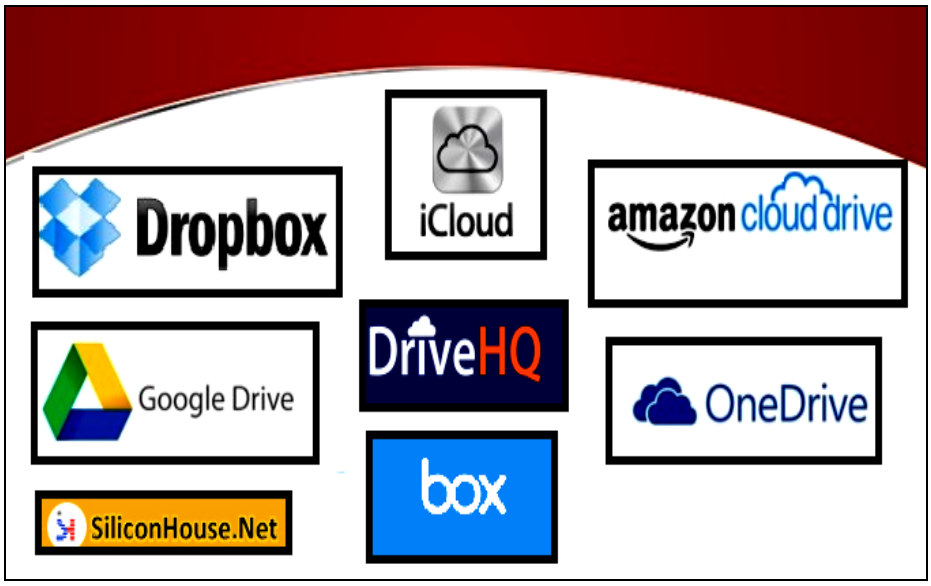

Figure.1. Illustrate Real-Time Cloud Service Providers

In contemporary business landscapes, a pervasive trend is observed as companies migrate their applications and databases to the cloud, capitalizing on the myriad advantages offered by cloud computing. The allure of on-demand computing resources, flexible access, and space-efficient software installations has catalyzed this shift. Amidst this transition, paramount importance is accorded to the privacy of data by cloud users with each upload. This paper focalizes on a pivotal principle known as "encryption-before-outsourcing," a fundamental tenet that ensures the privacy of data uploaded by diverse cloud owners onto the Cloud Server (CS) [2], [3], [4], [5]. However, the effective utilization of encrypted data poses a new challenge. While significant attention has been directed toward secure search over encrypted data [6], secure function evaluation [7], and fully homomorphic encryption systems [8], practical implementation remains elusive due to their inherent complexity.

As depicted in Figure 1, a myriad of real-time cloud service providers stands ready to cater to the storage needs of valuable data in the contemporary environment. In this proposed thesis, we leverage DRIVEHQ as our storage service to facilitate the storage and retrieval of files from applications. DRIVEHQ functions as a hybrid cloud, providing both public and private access to registered users. Upon registration, users are allocated 1 GB of space as public access. However, once a user's data usage surpasses this threshold, the account seamlessly transitions to a private access mode, incurring charges based on the excess storage utilized. The cost of storage is contingent upon the current usage of the end user, rendering DRIVEHQ a dynamic solution that offers public access up to 1 GB and transitions to a private account thereafter.

ISSN PRINT 2319 1775 Online 2320
Research paper Volume 11, Iss 4, 2022

2. Literature Survey

In this section we mainly discuss about the related work that was carried out in give data authority and maintain integrity for the data in the cloud server. Now let us discuss about this in detail as follows

1) Secure and Privacy-Preserving Data Sharing in Cloud Computing

Authors: C. Wang, Q. Wang, K. Ren, and W. Lou

This foundational work addresses the security and privacy challenges in cloud computing, emphasizing the need for secure data sharing. The authors propose a scheme that allows users to securely share their encrypted data in the cloud while ensuring data integrity.

2) Verifiable Searchable Symmetric Encryption for Secure Cloud Storage

Authors: M. Chase and S. Kamara

This paper introduces the concept of verifiable searchable symmetric encryption (VSSE) for secure cloud storage. The authors present a novel approach that enables a client to verify the correctness of search results without decrypting the data, ensuring both integrity and confidentiality.

3) Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data

Authors: C. Wang, N. Cao, J. Li, K. Ren, and W. Lou

Focusing on privacy-preserving search in the cloud, this work proposes a multi-keyword ranked search scheme. The authors employ a secure index and relevance scoring mechanism, addressing the need for fine-grained control over data access while maintaining data integrity.

4) Verifiable Delegated Access Control in Public Clouds

Authors: M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou

Exploring the domain of access control in public clouds, this paper introduces a verifiable delegated access control (VDAC) system. The proposed scheme enables data owners to delegate access rights and verify the correctness of delegated operations, ensuring the integrity of access control mechanisms.

5) Practical Techniques for Searches on Encrypted Data

Authors: D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano

This seminal work delves into practical techniques for searching encrypted data. The authors introduce searchable symmetric encryption (SSE) and present efficient methods for secure and privacy-preserving search functionalities, contributing to the broader discourse on encrypted data retrieval.

6) CryptDB: Protecting Confidentiality with Encrypted Query Processing

Authors: R. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan

Focused on database security, CryptDB introduces a novel encrypted database system. The approach allows encrypted query processing while preserving confidentiality. The paper provides insights into techniques for fine-grained access control and data integrity in encrypted databases.

7) Efficient Fine-Grained Access Control for Encrypted Data in Clouds

Authors: J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou

Addressing the need for fine-grained access control, this paper proposes an efficient scheme for managing encrypted data in cloud environments. The authors emphasize the importance of supporting complex access policies while ensuring data integrity.

8) Fully Homomorphic Encryption Over the Integers

ISSN PRINT 2319 1775 Online 2320
Research paper Volume 11, Iss 4, 2022

Authors: C. Gentry

Exploring the theoretical foundations of fully homomorphic encryption (FHE), this paper introduces an FHE scheme over the integers. While not immediately practical due to high complexity, FHE is a groundbreaking concept allowing computations on encrypted data and has implications for fine-grained access control.

3. Proposed Model

In this section we will mainly discuss about proposed model for providing data security and integrity over the encrypted cloud data. Now let us discuss about this proposed model in detail as follows:

In our proposed system model, we delineate the key primitives central to our thesis, focusing on the orchestration of interactions among three main entities within any cloud service provider environment:

Data Owner:

The data owner represents an individual or an enterprise initiating the outsourcing process. This entity harbors the intention to securely outsource a collection of documents (D = {D1, D2, ..., Dn}) to the cloud server. For clarity, each document is labeled as Di, where i denotes a specific document in the collection. The data owner's primary objective is to preserve search functionality on the outsourced data while ensuring the confidentiality and integrity of sensitive information.

Data User/Search User:

The data user or search user is an entity seeking to retrieve specific information from the outsourced documents. This user may initiate search queries or requests for specific documents while being oblivious to the underlying encrypted representation. The system aims to enable seamless search functionality for the data user, striking a balance between accessibility and data security.

Cloud Server:

The cloud server acts as the repository for the outsourced documents and is responsible for executing search operations on the encrypted data. It stores the encrypted documents (C = {C1, C2, ..., Cn}), each corresponding to its original document Di, as encrypted by the data owner before uploading to the cloud server. The cloud server must facilitate secure and efficient search operations on the encrypted data while ensuring that sensitive information remains confidential.

Workflow Overview:

The data owner initiates the process by encrypting the sensitive documents using a secure encryption algorithm, resulting in the creation of encrypted counterparts (C1, C2, ..., Cn).

The encrypted documents are then uploaded to the cloud server, where they are securely stored.

Data users, seeking specific information, submit search queries to the cloud server without compromising the confidentiality of the encrypted documents.

The cloud server processes search queries on the encrypted data, retrieves relevant results, and returns them to the data user without revealing the decrypted content.

Through this model, our objective is to establish a secure and efficient mechanism for preserving data privacy during cloud-based search operations.

ISSN PRINT 2319 1775 Online 2320
Research paper Volume 11, Iss 4, 2022

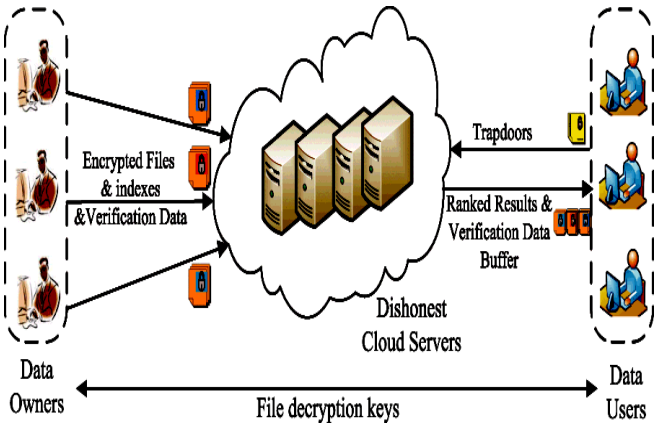

Figure.2. Represents the Proposed Model for Providing Security and Integrity over Encrypted Cloud Data

Multiple data owners and multiple data consumers are evidently present in the cloud architecture, with the data owner attempting to encrypt the insertion of all data into the cloud server (see Figure 2).The data proprietor attempts to validate the encrypted data using a verification technique so as to generate a brief signature and establish the data's integrity. Subsequently, the data user endeavors to conduct a file search, initiates a request for the files from the cloud server, and requests the data owner's decryption key. Once the key is transmitted by the data proprietor, the data can be decrypted and viewed as plain text.

4. Conclusion

We finally implemented and analyzed a secure, easily integrated, and fine-grained query results verification mechanism in this proposed thesis. Using the MD5 Algorithm (message digest algorithm), which generates a short signature key used to verify data authentication, the query user can verify not only the quality of each data file but also the authorization of data given an encrypted query results set. As a result of conducting numerous experiments on our proposed model, we have reached the conclusion that our proposed method provides the highest level of data integrity and security for sensitive data stored in an encrypted cloud.

5. References

1. Gentry, C. (2009). "A Fully Homomorphic Encryption Scheme." PhD thesis, Stanford University.

2. Wang, C., Wang, Q., Ren, K., & Lou, W. (2009). "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing." IEEE INFOCOM 2009.

3. Chase, M., & Kamara, S. (2010). "Structured Encryption and Controlled Disclosure." ACM Conference on Computer and Communications Security (CCS).

4. Wang, C., Cao, N., Li, J., Ren, K., & Lou, W. (2010). "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data." IEEE INFOCOM 2010.

ISSN PRINT 2319 1775 Online 2320

Research paper Volume 11, Iss 4, 2022

5. Popa, R. A., Redfield, C. M., Zeldovich, N., & Balakrishnan, H. (2011). "CryptDB: Protecting Confidentiality with Encrypted Query Processing." Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles (SOSP).

6. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2012). "Verifiable Delegated Access Control in Public Clouds." IEEE Transactions on Parallel and Distributed Systems.

7. Boneh, D., Crescenzo, G. D., Ostrovsky, R., & Persiano, G. (2004). "Public Key Encryption with Keyword Search." International Conference on the Theory and Applications of Cryptographic Techniques.

8. Wang, C., Ren, K., Lou, W., & Li, J. (2010). "Toward Secure and Dependable Storage Services in Cloud Computing." IEEE Transactions on Services Computing.

9. Golle, P., Staddon, J., & Waters, B. (2004). "Secure Conjunctive Keyword Search over Encrypted Data." ACM Conference on Computer and Communications Security (CCS).

10. Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds." ACM Conference on Computer and Communications Security (CCS).

11. Curtmola, R., Garay, J., Kamara, S., & Ostrovsky, R. (2006). "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions." ACM Conference on Computer and Communications Security (CCS).

12. Vaithiyanathan, T., & Sheeba, J. (2017). "A Review on Fine-Grained Search in Encrypted Cloud Data." International Journal of Engineering and Technology (IJET).

13. Green, M., Hohenberger, S., & Waters, B. (2011). "Outsourcing the Decryption of ABE Ciphertexts." ACM Conference on Computer and Communications Security (CCS).

14. Goh, E. J. (2003). "Secure Indexes." CRYPTO 2003.

15. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing." INFOCOM 2010.

16. Di Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S., & Samarati, P. (2007). "Over-Encryption: Management of Access Control Evolution on Outsourced Data." ACM Transactions on Information and System Security (TISSEC).

17. Cash, D., Jaeger, J., Jarecki, S., Jutla, C., & Krawczyk, H. (2013). "Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries." CRYPTO 2013.

18. Islam, M. S., Kuzu, M., & Kantarcioglu, M. (2012). "Access Pattern Disclosure on Searchable Encryption: Ramification, Attack and Mitigation." IEEE Transactions on Dependable and Secure Computing.

ISSN PRINT 2319 1775 Online 2320

Research paper Volume 11, Iss 4, 2022

19. Curtmola, R., Khan, O., Burns, R., & Basin, D. (2011). "MRSE: Multi-User Revocable Searchable Encryption." ESORICS 2011.

20. Zhang, Y., & Katz, J. (2015). "K-RSE: An Efficient Keyword-Search System against Insider Keyword Guessing Attacks." ACM Transactions on Information and System Security (TISSEC).