Journal of Science and Technology
ISSN: 2456-5660 Volume 8, Issue 07 (July -2023)
www.jst.org.in *DOI:https://doi.org/10.46243/jst.2023.v8.i07.pp140- 145*

Secure Mobile Cloud Storage

Bodasu Manisha[1] | Dr.V.Bapuji[2]

[1]Departmen of MCA, Vaageswari College of Engineering,
[2]Professor & HoD,Department of MCA, Vaageswari College of Engineering,

To Cite this Article

. **Bodasu Manisha | Dr.V.Bapuji , "Secure Mobile Cloud Storage "** *Journal of Science and Technology, Vol. 08, Issue 07,- July 2023, pp140-145*

Article Info

Received: 04-06-2023 Revised: 08-07-2023 Accepted: 18-07-2023 Published: 27-07-2023

ABSTRACT

Data may be stored on a cloud and accessible from anywhere using mobile devices thanks to mobile cloud storage (MCS). MCS services are provided for commercial use by sizable firms like Apple I Cloud, Dropbox, Microsoft One Drive, and Google Drive. Since customers may not fully trust clouds, data security may be achieved using encryption techniques. However, sensitive data, including location data, is frequently included in location-based apps. This exposed data can be used to deduce the client's behavior and encrypted data. For instance, 80% of search queries may be recognized by a searchable encryption system using a generic inference attack with access pattern leaking and little prior knowledge. The activity of the client can also be inferred via oblivious technologies, such as oblivious transfer and oblivious storage.This study presents a mobile cloud storage system that simultaneously safeguards data confidentiality and privacy while being effective, secure, and privacy-preserving. An oblivious selection and update (OSU) protocol built on onion additive homo morphic encryption with constant encryption layers serves as the underlying primitive. This dramatically lowers computation and transmission costs by enabling clients to covertly retrieve encrypted data items from the cloud and update them with new information. The suggested approach is more appropriate for MCS situations because it has beneficial characteristics such a fine-grained data structure, minimal client-side processing, and constant communication overhead. The "verification chunks" technique also confirms that the strategy is resistant to malicious cloud assaults. According to the comparison and assessment, the suggested plan is more effective than currently available oblivious storage options in terms of client .A valuable tool for distant storage, akin to cloud storage, is remote data integrity checking.

KEYWORDS: *Cloud computing, third-party verify, data, remote storage, cloud storage, CSP schema.*

INTRODUCTION

Cloud computing is gaining popularity in the business community due to its scalable,pay-on-demand,location-independent storage services. However, it also presents new security challenges, such as Data Loss & Leakage. To ensure data integrity, protocols must be developed that allow data owners to verify their data storage in the cloud. Cloud service providers (CSP) have become increasingly popular due to their ability to share data and process it efficiently at a low cost. However, the integrity of outsourced data is difficult to guarantee due to lack of transparency and the reputation of CSP. To design a secure and efficient audit mechanism for dynamic shared data in cloud storage, several challenges must be efficiently addressed. The traditional method of data integrity verification is to download all data from the data owner directly from the CSP and check the integrity of the data locally. However, this method wastes network transmission resources and local storage resources, weakening the advantages of cloud service.

The proposed scheme meets provable data possession, avoids certificate management problems, and achieves data privacy preservation without leaks of the data owner's identity information. As information

abundance increases, users increasingly store their data in the cloud to reduce storage pressure. However, cloud service providers may delete infrequently used data to reduce server overhead, leading to data loss. Researchers have proposed several cloud auditing schemes, allowing the TPA to check shared data on behalf of users, reducing the burden on users. which has problems such as certificate management and UNTRUSTWORTHY of the private key generator.

I. EXSITING SYSTEM

Oblivious schemes consider introducing data locality to improve efficiency, as it reveals the client's tendency to access data over a short time. Spatial and temporal locality are two types of reference locality of data access. The advantages of cloud computing are obvious, but it also poses new security risks[1]. Users attempt to share their data in cloud storage and process it effectively at a reasonable cost when cloud service usage grows. Users attempt to share their data in cloud storage and process it effectively at a reasonable cost when

cloud service usage grows[2]. Taking into account the spatial situation in the event of temporary overload, unconscious communication patterns,
muted communication overhead while accessing a series of items is lower than accessing one item independently. Consequently, how to lessen the workload and compute demands placed on cloud services providers is now a pressing issue that has to be resolved[6]. Integrating data from diverse sources is necessary to improve decision support for farmers[4]. Taking advantage of temporal locality can also significantly improve efficiency of oblivious schemes, as it requires lightweight.

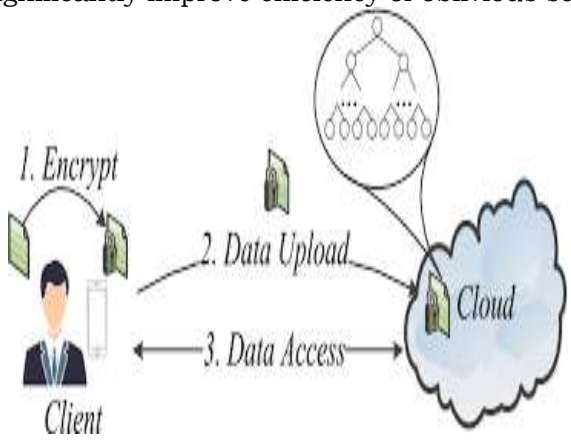

Fig.1: System Model

Researchers proposed many cloud auditing systems to verify the accuracy of cloud data[7]. However, there is no related work that has considered temporal locality. The user of the data should thus be given an assurance that their data will be stored on the cloud server exactly as they were initially[5]. Mobile devices are connected to the Internet via wireless networks, which means they have limited communication bandwidth for downloading and uploading data.

Numerous computer resources may be made available via the cloud architecture[9]. Some schemes suffer from the communication bandwidth overhead lower bound result O (log N) and cannot be employed in Mobile Computing System (MCS) due to heavy communication overhead.

Modern mobile devices have improved computing capabilities but cannot compete with powerful devices, and complicated computation reduces battery life. Some schemes based on fully homo morphemic encryption (FHE) or multi layer onion

additive homo morphemic encryption are not suitable for MCS due to complex client-side encryption and decryption computation, despite circumventing the communication lower bound and achieving constant communication bandwidth overhead.

DISADVANTAGES OF EXISTING SYSTEM

1. It does not safeguard the user's privacy and confidentiality.
2. Less security is used in the system's implementation

II. PROPOSED SYSTEM

This article proposes an efficient, secure, and privacy-preserving mobile cloud storage system (MCS) that can protect privacy and access patterns at the same time. The proposed scheme is provably secure against two types of adversaries and efficient in unrestricted use, distribution, and reproduction.

The proposed scheme has smaller element sizes, less client-side computing power, and constant communication overhead compared to existing schemes. Temporal locality is also taken into account to improve performance.

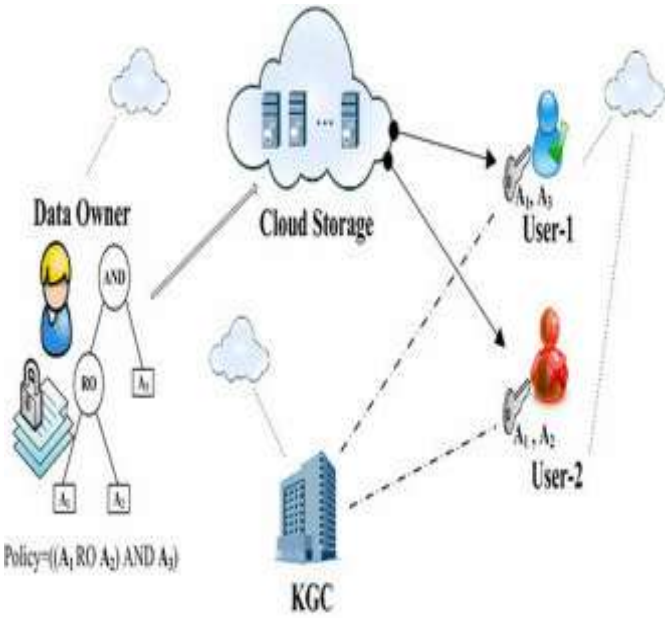

FIG : 2 Scientific diagram.

The proposed scheme can be tested for resistance to malicious clouds by combining additional

methods An unknowing pick-and-update protocol was introduced as a building block of the proposed MCS, allowing customers to unknowingly pick and update cloud-offloaded encrypted data items using a small vendor.

Due to the small number of calculations and client communications, this protocol can be of independent importance for other secure multi-party application scenarios. The document defines a two-way protocol, the Unconscious Select and Update (OSU) protocol, that allows clients to unknowingly download encrypted data from the cloud and update it with a new value. OSU requires less client communication and computation than other methods and has O(1) communication complexity for given data sizes.

Based on the proposed OSU protocol, this article introduces an efficient, secure, and privacy-preserving mobile cloud storage scheme that can protect the data content while keeping the access scheme private.

The scheme features a small element size, low client-side computations, and constant communication overhead. The "verification snippets" method is combined in a way that is verifiable and resistant to bad clouds. The article evaluates the construction and other related works and shows that the proposed system is more efficient.

ADVANTAGES OF PROPOSED SYSTEM

1. Our method reduces communication costs, reduces client-side processing, and reduces component size.

2. Applications benefit from increased computing and data storage capability.

3. A company that uses cloud computing is more agile and able to react quickly than one that uses in-house or external resources.

4. MCS Cloud offers a guarantee of data residency and jurisdictional laws, ensuring that your data is always safe and within the law.

III. RESULTS AND ANALYSIS

Proposed mobile cloud storage scheme analyzed for security and parametarization. This study

proposed a mobile cloud storage solution that is safe, protects user privacy, and is suitable for lightweight applications.

The employed initialization, access, and data structure notations are all described.

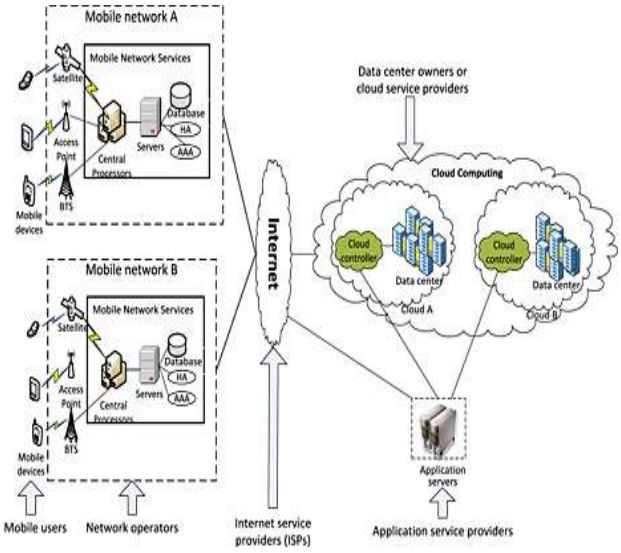

Fig. 3: The performance results

IV. CONCLUSION

This paper discusses remote data integrity checking protocol privacy issues and suggests an enhanced version for zero-knowledge privacy. With less computational overhead and suitability for cloud storage with regular outsourced data transfer, it enables a safe and effective audit method for shared dynamic data. A block chain based effective data integrity verification method utilizing music and Petersen commitment technology is also presented in the study. Data, Data Extraction, Retrieval, and Integration Service make up the four layers that make up the architecture for integrating and analyzing data utilizing cloud computing. Compared to previous similar methods, the public auditing scheme for cloud-assisted body area networks and the privacy-preserving cloud auditing strategy for multiple users provide improved security and efficiency aspects.

V.REFERENCES

[1]. Yu, Y., Au, M.H., Mu, Y. et al. Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage. Int. J. Inf. Secur. 14,
307–318(2015). https://doi.org/10.1007/s10207-014-0263-8

[2]. Ohmin Kwon, Dong young Koo, Yongjoo Shin, Hyunsoo Yoon, "A Secure and Efficient Audit Mechanism for Dynamic Shared Data in Cloud Storage", The Scientific World Journal, vol. 2014, Article ID 820391, 10 pages, 2014. https://doi.org/10.1155/2014/820391

[3]. Y. Zhang, H. Geng, L. Su and L. Lu, "A BLOCK CHAIN-BASED Efficient Data Integrity Verification Scheme in Multi-Cloud Storage," in IEEE Access, vol. 10, pp. 105920-105929, 2022, doi: 10.1109/ACCESS.2022.3211391.

[4]. A. Goldstein, L. Fink and G. Ravid, "A Cloud-Based Framework for Agricultural Data Integration: A Top-Down-Bottom-Up Approach," in IEEE Access, vol. 10, pp. 88527-88537, 2022, doi: 10.1109/ACCESS.2022.3198099.

[5]. Xiuguang Li, Ruifeng Li, Xu An Wang, Ke Niu, Hui Li, Xiaoyuan Yang, "Improved Efficient Privacy-Preserving Certificateless Provable Data Possession Scheme for Cloud Storage", Security and Communication Networks, vol. 2022, Article ID 7302767, 9 pages,2022.https://doi.org/10.1155/2022/7302767

[6]. G. Bian, Y. Fu, B. Shao and F. Zhang, "Data Integrity Audit Based on Data Blinding for Cloud and Fog Environment," in IEEE Access, vol. 10, pp. 39743-39751, 2022, doi: 10.1109/ACCESS.2022.3166536.

[7]. X. Yang, M. Wang, T. Li, R. Liu and C. Wang, "Privacy-Preserving Cloud Auditing for Multiple Users Scheme With Authorization and Traceability," in IEEE Access, vol. 8, pp. 130866-130877,2020,doi:10.1109/ACCESS.2020.3009539.

[8]. Tengfei Tu, Lu Rao, Hua Zhang, Qiaoyan Wen, Jia Xiao, "Privacy-Preserving Outsourced Auditing Scheme for Dynamic Data Storage in Cloud", Security and Communication Networks, vol. 2017, Article ID 4603237, 17 pages, 2017. https://doi.org/10.1155/2017/4603237

[9]. K. Zhao, D. Sun, G. Ren and Y. Zhang, "Public Auditing Scheme With Identity Privacy Preserving Based on CERTIFICATE LESS Ring Signature for Wireless Body Area Networks," in IEEE Access, vol. 8, pp. 41975-41984, 2020,doi:10.1109/ACCESS.2020.2977048.

[10]. E. Stefanov and E. Shi, "Obliviate: High Performance Oblivious Cloud Storage," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 2013, pp. 253-267, doi: 10.1109/SP.2013.25.