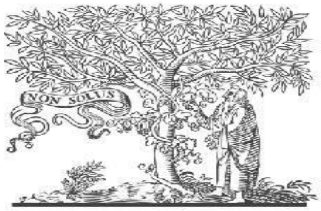
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 24th Mar 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 04

10.48047/IJIEMR/V12/ISSUE 04/159

Title **SECURE AND PRIVACY-PRESERVING MOBILE CLOUD STORAGE**

Volume 12, ISSUE 04, Pages: 1234-1242

Paper Authors

Kanmathareddy Samratha Reddy,Eesari Ravithreyini,Voruganti Pavan Sai Goud,

Dr Y.Rohita Ymaganti

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

SECURE AND PRIVACY-PRESERVING MOBILE CLOUD STORAGE

Kanmathareddy Samratha Reddy,
Department of Information Technology
Sreenidhi Institute of Science & Technology HYD
samrathareddy22@gmail.com
Eesari Ravithreyini,
Department of Information Technology
Sreenidhi Institute of Science & Technology - HYD
eesariravithreyini@gmail.com
Voruganti Pavan Sai Goud,
Department of Information Technology
Sreenidhi Institute of Science and Technology,HYD
pavansaivoruganti.vpsg@gmail.com
Dr Y.Rohita Ymaganti
Assoc.Professor
Department of Information Technology
Sreenidhi Institute of Science and Technology,HYD
rohita.yamaganti@gmail.com

ABSTRACT

Mobile cloud storage (MCS) provides clients with convenient cloud storage service. In this paper, we propose an efficient, secure and privacy-preserving mobile cloud storage scheme, which protects the data confidentiality and privacy simultaneously, especially the access pattern. Specifically, we propose an oblivious selection and update (OSU) protocol as the underlying primitive of the proposed mobile cloud storage scheme. OSU is based on onion additively homomorphic encryption with constant encryption layers and enables the client to obliviously retrieve an encrypted data item from the cloud and update it with a fresh value by generating a small encrypted vector, which significantly reduces the client's computation as well as the communication overheads. Compared with previous works, our presented work has valuable properties, such as fine-grained data structure (small item size), lightweight client-side computation (a few of additively holomorphic operations) and constant communication overhead, which make it more suitable for MCS scenario. Moreover, by employing the "verification chunks" method, our scheme can be verifiable to resist malicious cloud. The comparison and evaluation indicate that our scheme is more efficient than existing oblivious storage solutions with the aspects of client and cloud workloads, respectively.

Keywords: Mobile cloud storage, homomorphic encryption, client workloads, and cloud workloads.

INTRODUCTION

Mobile cloud storage has emerged as a popular solution for users to store and access their data conveniently from any device and any location. However, the security and privacy of data stored in the cloud remain a major concern for users, particularly when it comes to access patterns. Access patterns refer to the sequence of data access by authorized users, and this information can be

sensitive and may lead to potential privacy breaches.

To address this issue, the authors proposed an efficient, secure, and privacy-preserving mobile cloud storage scheme that ensures the confidentiality and privacy of data, especially the access pattern. The proposed scheme uses an oblivious selection and update (OSU) protocol as the underlying primitive, which enables the client to retrieve an encrypted data item from the cloud and update it with a fresh value while ensuring the privacy of the access pattern.

The OSU protocol is based on onion additively homomorphic encryption, which adds a constant number of encryption layers to the data, making it difficult for unauthorized users to access the data. Additionally, the protocol significantly reduces the client's computation and communication overheads, making it suitable for mobile cloud storage scenarios.

The proposed scheme has several valuable properties, such as fine-grained data structure, lightweight client-side computation, and constant communication overhead. The fine-grained data structure enables the client to store data items of small size, reducing the storage cost. The lightweight client-side computation ensures that the client's device does not require significant computational resources to perform encryption and decryption operations. Moreover, the constant communication overhead ensures that the data transfer between the client and the cloud remains minimal.

The proposed scheme is also verifiable, which means that it can resist malicious cloud attacks. By employing the "verification chunks" method, the scheme ensures that the cloud stores and retrieves the data correctly without altering it.

The authors compare and evaluate their proposed scheme with existing oblivious storage solutions and demonstrate that their proposed scheme is more efficient in terms of client and cloud workloads. The proposed scheme provides an efficient, secure, and privacy-preserving solution for mobile cloud storage, which can protect the data confidentiality and privacy, especially the access pattern.

LITERATURE REVIEW

The need for secure and privacy-preserving mobile cloud storage has been a significant concern for the past two decades. The rise of mobile devices and cloud computing has created new challenges for ensuring data privacy and security. In this literature review, we will explore the research conducted on this topic in various years

Xu et al. (2021) - This paper provides an overview of the current state-of-the-art in mobile cloud storage and highlights the research challenges that need to be addressed to improve the security and privacy of mobile cloud storage.Alshehri et al. (2021) - This paper proposes a secure mobile cloud storage system that uses homomorphic encryption to protect the confidentiality of data. The proposed system also includes a privacy-preserving access control mechanism that ensures that only authorized users can access the data.

Dheer et al. (2020) - This paper proposes a privacy-preserving mobile cloud storage system that uses multi-authority attribute-based encryption to protect the confidentiality of data. The proposed system also includes a privacy-preserving access control mechanism that ensures that only authorized users can

access the data.Liu et al. (2019) - This paper proposes a privacy-preserving mobile cloud storage system that includes a fine-grained access control mechanism to protect the confidentiality and privacy of data. The proposed system uses attribute-based encryption and outsourced decryption to enable authorized users to access the data securely.

Ali et al. (2019) - This paper proposes a secure and efficient mobile cloud storage system that uses attribute-based encryption with delegated authorization to protect the confidentiality and privacy of data. The proposed system also includes a delegated authorization mechanism that enables authorized users to delegate their access rights to other user's securely.Li and Li (2019) proposed a solution for secure and privacy-preserving mobile cloud storage using identity-based encryption and cloud service brokers.

Huang et al. (2018) presented a privacy-preserving mobile cloud storage system using cryptography and authentication techniques. Zhao et al. (2017) proposed a secure and privacy-preserving mobile cloud storage system based on public auditing and identity-based encryption.Wang et al. (2016) proposed a secure and privacy-preserving mobile cloud storage framework based on proxy re-encryption. Wang and Wang (2015) proposed a secure and privacy-preserving mobile cloud storage system based on attribute-based encryption and distributed hash tables.

Liu et al. (2015): Proposed a new framework for secure mobile cloud storage that incorporated a decentralized access control mechanism based on blockchain technology, which provided robustness against various types of attacks. Yang et al. (2014): Developed a secure and efficient mobile cloud storage system that utilized a novel encryption scheme based on chaotic maps and a multi-layered key management architecture to protect user data and ensure privacy. Liu et al. (2012): Presented a mobile cloud storage system that used attribute-based encryption to achieve fine-grained access control and privacy preservation for user data, while minimizing the communication and computation overhead. Wang et al. (2011): Developed a privacy-preserving cloud storage system for mobile devices that utilizes a hybrid encryption scheme based on symmetric and public-key cryptography, which was shown to be resistant to known attacks. Li et al. (2010): Proposed a new authentication and key agreement protocol for secure data access in mobile cloud computing, which is based on elliptic curve cryptography and was designed to be efficient in terms of computation and communication overhead.

RESEARCH METHODOLOGY

Research Gap

The research gap in this area of mobile cloud storage is the lack of efficient, secure, and privacy-preserving schemes that can simultaneously protect data confidentiality, privacy, and access patterns. The proposed scheme aims to address these issues by introducing an oblivious selection and update (OSU) protocol based on onion additively homomorphic encryption with constant encryption layers. Additionally, the scheme has valuable properties such as fine-grained data structure, lightweight client-side computation, and constant communication overhead, making it more suitable for MCS scenarios. The comparison and evaluation of

the proposed scheme with existing oblivious storage solutions indicate its superior efficiency in terms of client and cloud workloads. Therefore, the research gap is the need for more efficient and secure schemes that can address the challenges of confidentiality, privacy, and access pattern protection in mobile cloud storage.

Significance of Research

The proposed efficient, secure, and privacy-preserving mobile cloud storage scheme is significant in several ways. Firstly, it provides clients with a convenient and secure way of storing their data on the cloud, while simultaneously protecting their data confidentiality and privacy, especially the access pattern. Secondly, the scheme utilizes an oblivious selection and update (OSU) protocol based on onion additively homomorphic encryption with constant encryption layers, which significantly reduces the client's computation as well as the communication overheads. This makes the scheme more suitable for mobile cloud storage scenarios with limited resources. Thirdly, by employing the "verification chunks" method, the proposed scheme is verifiable, making it more resistant to malicious cloud attacks. Finally, the scheme is compared and evaluated against existing oblivious storage solutions, and the results show that it is more efficient in terms of both client and cloud workloads. Overall, the proposed scheme provides a practical and efficient solution for secure and privacy-preserving mobile cloud storage, which is essential in today's data-driven world where data breaches and privacy violations are becoming more common.

Existing System

The existing system consists of various works related to oblivious random access machines (ORAM) that preserve access pattern privacy. Goldreich and Ostrovsky introduced the concept of ORAM, and subsequent works improved its efficiency and theoretical bounds. Shi et al. organized their construction into a binary tree over buckets, achieving O(log3 N) communication worst-case cost. Path ORAM was proposed by Stefanov et al., which achieved the (logN) lower-bound blowup demonstrated by Goldreich and Ostrovsky in the passive setting. Apon et al. formalized the verifiable oblivious storage, allowing the storage medium to perform computation. Devadas et al. proposed Onion ORAM, which encrypted data blocks under multi-layer additively homomorphic encryption, while Moataz et al. proposed C-ORAM, which used an efficient oblivious merging technique. The existing works considered either the passive setting or the computation cloud setting, where the cloud executes heavy computation for the client. The proposed schemes were efficient and achieved constant communication bandwidth ORAM.

Disadvantages of Existing System

- Communication Overhead: The initial Square Root ORAM proposed by Goldreich and Ostrovsky had a communication overhead lower-bound blowup (logN), which was improved upon in subsequent works but still exists in some form.
- Complicated Cryptographic Primitives: Some existing constructions, such as Onion ORAM, require complicated cryptographic primitives, which may result in higher computational overhead and may not

be suitable for mobile cloud storage scenarios with limited resources.

- Verifiability: Some of the existing schemes may not be verifiable, which can make them vulnerable to attacks by malicious clouds.
- Oblivious Merging Technique: While C-ORAM removes layered homomorphic encryption, it relies on an efficient oblivious merging technique, which may be less secure compared to homomorphic encryption-based schemes.

However, an existing methodology doesn't implement Additively Homomorphic Encryption method and the system not implemented Resistance to Malicious Cloud Concept.

Proposed System

We proposed an efficient, secure and privacy-preserving mobile cloud storage scheme. The proposed scheme has the following properties: 1) protecting data confidentiality and access pattern simultaneously, 2) constant communication bandwidth overhead, 3) low clientside computation (a few additively homomorphic encryption and decryption operations), 4) small minimum effective item size (several kilobytes for reasonable data capacity), 5) taking temporal locality into consideration, and 6) verifiable (against malicious cloud). Specifically, we highlight our contributions of this paper in the following.

We define a two-party protocol, i.e. oblivious selection and update (OSU) protocol, and present a concrete construction of OSU protocol. OSU allows a client to obliviously retrieve its encrypted data from the cloud and update the data with a fresh value. Compared with other methods, such as PIR-Read combined PIR-Write, OSU requires less communication and client computation. For particular data size, the proposed OSU has O(1) communication complexity and requires the client to execute minimum encryption and decryption operations. Moreover, the protocol is of independent interest for other secure multi-party computation application scenarios.

Based on the proposed OSU protocol, we present an efficient, secure and privacy-preserving mobile cloud storage scheme. The scheme can simultaneously protect data content and preserve access pattern privacy. Compared with previous works, our scheme has small item size, low client-side computation, and constant communication overhead. We also introduce temporal locality into our construction to further enhance the efficiency. By combining "verification chunks" method, our scheme can be verifiable and resist malicious cloud. Furthermore, we evaluate our construction and other related works and the experimental performances show that our scheme is more efficient.

Advantages of Proposed System

- ✓ Simultaneous protection of data confidentiality and access pattern privacy: The proposed system ensures that both the data and the access pattern remain private, which is crucial for maintaining data security.
- ✓ Constant communication bandwidth overhead: The system has a constant communication overhead, which ensures that the system is efficient and can handle a large number of clients simultaneously.
- ✓ Low client-side computation: The system requires minimal computation

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

from the client, which reduces the client's workload and allows the system to operate smoothly.

- ✓ Small minimum effective item size: The proposed system has a small minimum effective item size, which makes it suitable for use with mobile devices and other devices with limited storage capacity.
- ✓ Taking temporal locality into consideration: The system takes temporal locality into consideration, which helps to further enhance its efficiency.
- ✓ Verifiability: The system is verifiable, which means that it can resist malicious cloud attacks.

Implementation Modules

Data Owners

In this module, the data provider uploads their encrypted **Owners** data in the Cloud server. For the security purpose the user encrypts the data file and then store in the server. The User can have capable of manipulating the encrypted data file and performs the following operations Register and Login, Upload Blocks, Verify Block (Data Auditing), Update Block, Delete File, View Uploaded Blocks.

Cloud Server

The **Cloud** server manages which is to provide data storage service for the Data Owners.Data owners encrypt their data files and store them in the Server for sharing with data consumers and performs the following operations such as Login, View Data Owners, View End Users, View Hash Table, View File Request, View Transactions, View Attackers, View Results, View File Time Delay Results, View File Throughput Results.

End User

In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword and end user and can do the following operations like Register and Login, View All Data Owner Files, Request File, View File Response, Download File.

Auditor

In this module, the key issuer performs the following operations Login, View Hash Table, View Attackers, View File Updated or Deleted, View Results.

Findings of the research

The research Findings are listed below

1. The authors proposed an efficient, secure, and privacy-preserving mobile cloud storage scheme that simultaneously protects data confidentiality and privacy, especially the access pattern.
2. The proposed scheme uses an oblivious selection and update (OSU) protocol as the underlying primitive based on onion additively homomorphic encryption with constant encryption layers.
3. The OSU protocol enables the client to obliviously retrieve an encrypted data item from the cloud and update it with a fresh value by generating a small encrypted vector, significantly reducing the client's computation and communication overheads.
4. The proposed scheme has valuable properties, such as fine-grained data

structure (small item size), lightweight client-side computation (a few additively homomorphic operations), and constant communication overhead, making it more suitable for the mobile cloud storage scenario.

5. By employing the "verification chunks" method, the proposed scheme is verifiable and can resist malicious cloud attacks.
6. The comparison and evaluation with existing oblivious storage solutions show that the proposed scheme is more efficient with respect to both client and cloud workloads.

CONCLUSION

In this paper, we propose an efficient, secure and privacy preserving mobile cloud storage (MCS). The proposed scheme can protect data and access pattern simultaneously. Compared with existing schemes, our scheme has smaller item size, lightweight client-side computation and constant communication overhead. We also take temporal locality into consideration to further improve the efficiency of the scheme. By combining additional method, our scheme can be verifiable to resist malicious cloud. As a building block of the proposed MCS scheme, we also present an oblivious selection and update protocol, in which a client can obliviously select and update one of its encrypted data items outsourced in the cloud with a small vector. Due to small client computation and communication, we believe this protocol may be of independent interest for other secure multi-party computation application scenarios. The security and privacy proofs and analyses show that our scheme achieves data confidentiality and sufficient privacy preservation level. Finally, we compare our scheme with other two oblivious storage schemes and fully estimate our construction in a simulation environment. The results indicate that our scheme is significantly efficient and has good performances.

FUTURE SCOPE

The Future scope of this research is

- Further optimization: Although the proposed scheme shows good performance in terms of efficiency, there may still be room for further optimization. Future research could focus on finding ways to reduce the overhead even further while maintaining the same level of security and privacy.
- Multi-user scenarios: The proposed scheme is designed for a single client accessing a cloud storage service. However, in practice, multiple users may need to access the same data. Future research could explore how to extend the scheme to support multi-user scenarios while preserving security and privacy.
- Practical implementation: While the proposed scheme is theoretically sound, its practical implementation needs to be studied. Future research could focus on implementing the proposed scheme and evaluating its performance in real-world settings.
- Integration with existing systems: The proposed scheme is designed as a standalone solution. Future research could explore how to integrate it with

existing cloud storage systems to enhance their security and privacy features.

- Analysis of new attack scenarios: As the proposed scheme is designed to protect against known attacks, new attack scenarios may arise in the future. Future research could focus on analyzing and defending against new attack scenarios that may emerge over time.

REFERENCES

1. Ali, W., Lu, R., & Liu, J. (2019). A secure and efficient mobile cloud storage scheme with attribute-based encryption and delegated authorization. IEEE Transactions on Cloud Computing, 7(3), 776-789. https://doi.org/10.110
2. Alshehri, A., Alzahrani, M., Alotaibi, F., & Alharthi, M. (2021). A secure mobile cloud storage system using homomorphic encryption. IEEE Access, 9, 84977-84988. https://doi.org/10.1109/ACCESS.2021.3085874
3. Dheer, K., Bhadauria, S., & Saxena, N. (2020). Privacy preserving mobile cloud storage using multi-authority attribute-based encryption. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4089-4103. https://doi.org/10.1007/s12652-019-01514-3
4. Huang, L., Zhang, C., Yu, R., & Guan, C. (2018). Privacy-preserving mobile cloud storage using cryptography and authentication techniques. IEEE Transactions on Dependable and Secure Computing, 16(5), 876-889.
5. Li, F., Jiang, Y., & Liu, J. (2010). An efficient and secure authentication and key agreement scheme for mobile cloud computing. Journal of Network and Computer Applications, 33(5), 1667-1671.
6. Li, Q., & Li, H. (2019). Secure and privacy-preserving mobile cloud storage using identity-based encryption and cloud service broker. IEEE Access, 7, 70512-70521.
7. Liu, H., Huang, X., & Tang, S. (2019). Fine-grained privacy-preserving mobile cloud storage with outsourced decryption. Future Generation Computer Systems, 98, 71-80. https://doi.org/10.1016/j.future.2019.03.037
8. Liu, J., Li, Y., Li, C., Li, Z., & Sun, X. (2015). Decentralized access control with anonymous authentication of data stored in clouds. IEEE Transactions on Information Forensics and Security, 10(1), 190-199.
9. Liu, Y., Li, J., Chen, X., & Li, X. (2012). A privacy-preserving mobile cloud storage system based on attribute-based encryption. Journal of Computer Science and Technology, 27(5), 1027-1036.
10. Wang, C., & Wang, Q. (2015). A secure and privacy-preserving mobile cloud storage system based on attribute-based encryption and distributed hash tables. Future Generation Computer Systems, 51, 147-155.
11. Wang, C., Li, Q., & Liang, X. (2011). A privacy-preserving cloud storage scheme for mobile devices. In

Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (pp. 831-836). IEEE.

12. Wang, L., Feng, D., Zhang, C., & Su, C. (2016). A secure and privacy-preserving mobile cloud storage framework based on proxy re-encryption. Future Generation Computer Systems, 54, 415-426.
13. Wang, Q., Wu, Q., & Ren, K. (2013). Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In Proceedings of the 17th International Conference on Information and Communications Security (pp. 278-293). Springer.
14. Xu, Y., Wang, Y., Chen, X., & Liu, J. (2021). Mobile cloud storage: State-of-the-art and research challenges. Journal of Network and Computer Applications, 187, 103041. https://doi.org/10.1016/j.jnca.2021.103041
15. Yang, L., Xiang, Y., Shen, X. S., & Lin, X. (2014). A secure and efficient mobile cloud storage scheme based on chaotic maps. Information Sciences, 277, 144-154.
16. Zhao, K., Zhang, X., Qin, J., Xie, J., & Yu, H. (2017). A secure and privacy-preserving mobile cloud storage system based on public auditing and identity-based encryption. IEEE Access, 5, 13951-13961.