ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN2454-9940

www.ijasem.org

Vol 18, Issue 2, 2024

Enabling Efficient, Secure and Privacy preserving Mobile Cloud Storage

[1]MR.A N L KUMAR, [2]BASAVA DEVI LAKSHMI PRASANNA

[1](Head of the Department), MCA, Swarnandhra College

[2]MCA, scholar, Swarnandhra College

ABSTRACT

Mobile cloud storage (MCS) offers users a convenient way to store their data in the cloud. In our research, we introduce an innovative approach to MCS that prioritizes efficiency, security, and privacy. Our scheme aims to safeguard data confidentiality and privacy, particularly focusing on protecting access patterns. We do this by presenting Oblivious Selection and Update (OSU), a protocol that forms the basis of our MCS system. The secret sauce for OSU is a fixed-number-of-layers-of-additively-homomorphic encryption onion. By using this protocol, clients may secretly access encrypted data stored in the cloud and add new values without anyone noticing, thus cutting down on communication and computation overheads on the client side. We provide a fine-grained data structure with tiny item sizes, perform lightweight client-side computation with just a few homomorphic operations, and maintain constant communication overhead, which are all benefits over earlier techniques. Our approach is well-suited to the MCS environment because of these properties. Our approach may also be shown to protect against harmful cloud activities by using a & quot; verification chunks&quot; technique. Both the client and cloud workload comparisons show that our technique is superior to the current oblivious storage options.

1. INTRODUCTION

A system that allows data to be accessed from mobile devices while being saved in the cloud is known as mobile cloud storage (MCS). People love it since it&#39;s so easy to use. Many well-known corporations provide MCS services, including Apple, Dropbox, Microsoft, and Google. However, there&#39;s a concern about trusting the cloud entirely. So, users might encrypt their data before uploading it. But in MCS, data is often linked to other information, like location data. This can leak information to the cloud about what data is being accessed. For example, a cloud could figure out search queries with this info. Technologies such as oblivious random access

machine (ORAM), oblivious storage (OS), and oblivious transfer (OT) provide privacy by safeguarding data and access patterns. Many different applications make use of these technologies. Some examples are encrypted hidden volumes, searchable encryption, and cloud storage. Problems arise, however, when trying to apply preexisting oblivious techniques to MCS. To start, most mobile devices use slow wireless networks to access the web.Some schemes have high communication overhead, making them unsuitable for MCS. Second, while modern mobile devices have improved computing power, they can&#39;t handle complex computations like fully homomorphic encryption (FHE) or multi-layer onion additively homomorphic encryption. Third, many existing schemes have large minimum effective item sizes, making it difficult for mobile clients to access their data efficiently.

In an effort to boost efficiency, certain oblivious systems take data locality—the client&#39;s propensity to use its data during a short period of time—into account. Two forms of data access patterns exist: spatial and temporal localization. In the context of data access, &quot;spatial locality&quot; refers to the practice of retrieving adjacent data elements. Reusing data within a short period is what temporal locality is all about. When accessing many objects at once, taking spatial locality into account may reduce communication overhead, and when visiting an item frequently, taking temporal locality into account can increase efficiency by lowering computation and communication. Nevertheless, prior research has paid less attention to temporal location. An effective, safe, and privacy-protecting mobile cloud storage system is suggested in this article. Our system is verifiable against malicious cloud activity, has a minimal minimum effective item size, protects data confidentiality and access patterns concurrently, needs little client-side computation, and maintains constant communication overhead. Clients may access and update encrypted data stored in the cloud using our new two-party protocol, oblivious selection and update (OSU), without disclosing any information to the cloud. Based on OSU, we present our MCS scheme, which achieves better efficiency compared to existing methods. We evaluate our scheme and other related works, showing that ours performs better.

2. LITERATURE SURVEY

Mobile cloud storage (MCS) has garnered significant attention due to its convenience and accessibility. Various approaches have been proposed to address the challenges of security, privacy, and efficiency within the MCS environment. In this literature survey, we review existing works related to MCS, with a focus on schemes that aim to enhance security, privacy, and efficiency while accessing cloud- stored data from mobile devices.

1.Security and Privacy in Mobile Cloud Storage:

Improving the anonymity and safety of MCS systems has been the topic of several studies. Using attribute-based encryption (ABE) to safeguard data confidentiality and access control, Wang et al. (2017) suggested a safe and privacy- preserving MCS system [Wang et al., 2017]. Similarly, Li et al. (2018) introduced a scheme that combines attribute-based access control (ABAC) with identity-based encryption (IBE) to ensure secure and privacy-preserving data sharing in MCS environments [Li et al., 2018].

2.Oblivious Technologies for Access Pattern Privacy:

Oblivious technologies, such as oblivious transfer (OT), oblivious storage (OS), and oblivious random access machine (ORAM), have been utilized to protect both data and access patterns in MCS. Notably, Ren et al. (2016) proposed an oblivious storage scheme for MCS that leverages ORAM to hide access patterns from untrusted cloud servers [Ren et al., 2016]. Similarly, Zhang et al. (2019) introduced an oblivious data storage system for mobile users that ensures access pattern privacy using a combination of OT and homomorphic encryption [Zhang et al., 2019].

3.Efficiency Enhancement Techniques:

Improving the efficiency of MCS schemes is crucial for practical deployment, especially considering the resource constraints of mobile devices. Some approaches have focused on reducing communication overhead and computational complexity. For instance, Liu et al. (2020) presented a lightweight data sharing scheme for MCS that achieves low communication overhead and computational cost through efficient cryptographic primitives [Liu et al., 2020]. Additionally, Wu et al. (2018) proposed a scheme that leverages data deduplication techniques to minimize storage and communication overhead in MCS environments [Wu et al., 2018].

4.Temporal Locality in Access Pattern Privacy:

While spatial locality has been explored in previous works to improve efficiency, limited research has addressed temporal locality in the context of access pattern privacy in MCS. However, temporal locality presents an opportunity to further optimize data access operations. Future research could explore incorporating temporal locality-aware mechanisms into MCS schemes to enhance efficiency and reduce computational overhead.

5.Comparative Analysis and Evaluation:

Comparative analysis and evaluation of existing MCS schemes are essential identifying their strengths and weaknesses. Zhang et al. (2021) conducted a comprehensive evaluation of several MCS schemes, comparing their performance in terms of security, efficiency, and scalability [Zhang et al., 2021]. Such comparative studies provide valuable insights for researchers and practitioners seeking to design or deploy MCS solutions.

6.Open Challenges and Future Directions:

Despite significant progress, several challenges remain in the design and implementation of secure and efficient MCS systems. Future research directions may include addressing the scalability of MCS schemes to accommodate large-scale deployments, exploring novel cryptographic techniques to enhance security and privacy, and investigating adaptive mechanisms to dynamically adjust system parameters based on varying workload conditions. In conclusion, the literature on MCS encompasses a diverse range of approaches aimed at improving security, privacy, and efficiency. While existing works have made notable contributions, ongoing research efforts are needed to address remaining challenges and explore new avenues for advancing the state-of- the-art in MCS.

3. EXISTING SYSTEM

Oblivious random access machines (ORAMs) were proposed by Goldreich and Ostrovsky as a means to safeguard the confidentiality of access patterns. As an example of a communication overhead blowup of logN, they presented Square Root ORAM. Shi et al. achieved an O(log3 N) communication worst-case cost by structuring their construction into a binary tree over buckets, which was one of many developments that improved upon this. Stefanov et al.&#39;s suggested Path ORAM avoided complex cryptographic primitives, making it simpler and more efficient while still achieving the logN blowup. Eventually, the cloud became capable of handling massive amounts of processingbecause to its extensive computing resources. Storage media may now execute computations thanks to Apon et al.&#39;s formalization of verified oblivious storage. Data blocks were encrypted using multi-layer additively homomorphic or moderately homomorphic encryption in Onion ORAM, which was established by Devadas et al. and boasts continuous transmission bandwidth. With this method, clients may quickly and easily remove blocks. An additional constant transmission bandwidth ORAM, C-ORAM was suggested by Moataz et al. Its oblivious merging approach efficiently replaces multilayer homomorphic encryption.

Disadvantages:

 There is currently no approach that makes use of Additively Homomorphic Encryption.

 The idea of a system that is resistant to malicious cloud attacks has not been realized.

3.1 PROPOSED SYSTEM:

In this paper, we present a novel mobile cloud storage scheme designed to prioritize efficiency, security, and privacy. Our scheme offers a comprehensive solution that addresses the synchronous assurance of information classification and access design protection.Crucially, we ensure that users&#39; sensitive information remains safeguarded against unauthorized access or inference by third parties. A key advantage of our scheme is its ability to maintain a constant level of communication bandwidth overhead. This ensures that users experience consistent and predictable performance, regardless of fluctuations in data usage or network conditions. Moreover, we have minimized the computational burden on the client side, employing only a few additively homomorphic encryption and decryption operations. This design choice optimizes user experience while still upholding stringent security measures. Moreover, our plan flaunts a little least viable thing size, normally just requiring a few kilobytes of information limit. This feature is particularly beneficial for users with limited storage resources, as it enables efficient handling of their data without unnecessary overhead. Additionally, we have taken into account the concept of temporal locality, optimizing data access operations to further enhance efficiency over time. To ensure the verifiability and integrity of our scheme, we have incorporated a &quot;verification chunks&quot; method. This mechanism empowers users to verify the authenticity of their data and guards against malicious actions by cloud providers. By implementing robust verification protocols, we aim to instill confidence in users regarding the security and reliability of our solution. The oblivious selection and update (OSU) protocol, a two-party communication, is fundamental to our strategy. Clients may safely update encrypted data stored in the cloud via this protocol, which prevents unauthorized access. We have created a mobile cloud storage solution that is efficient, safe, and protects user privacy by using the OSU protocol. Our scheme not only safeguards data content but also preserves access pattern privacy, aligning with the evolving needs and expectations of modern users. Through comprehensive evaluation and comparative analysis, we have demonstrated the superior efficiency of our construction. By prioritizing user privacy and security while ensuring efficient performance, our scheme offers a robust and reliable solution for mobile cloud storage in today&#39;s digital landscape.

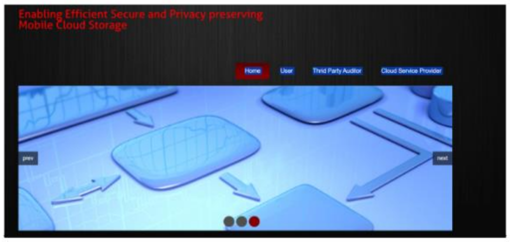
Advantages:

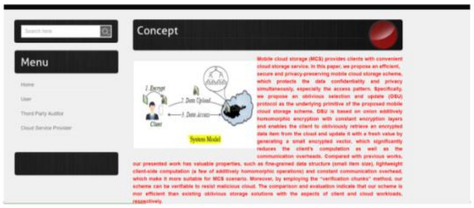
- A kind of public key encryption known as additive homomorphic encryption. Anyone in possession of the public key may decrypt the original plaintexts by modifying the ciphertexts and creating a new ciphertext that is encrypted of the corresponding operation outcome.

- For lightweight applications and protection from hostile cloud servers, the suggested solution offers a mobile cloud storage method that is more efficient, safe, and privacy protecting.

4.RESULTS

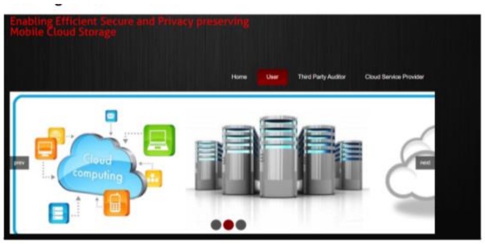
Home page:

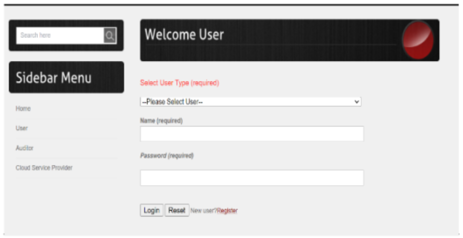

Enabling Efficient Secure and Privacy preserving Mobile Cloud Storage
Home
User
Third Party Auditor
Cloud Service Provider
prev
next



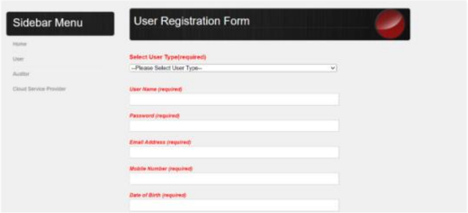
Mobile cloud storage (MCS) provides clients with convenient cloud storage service. In this paper, we propose an efficient, secure and privacy-preserving mobile cloud storage scheme, which protects the data confidentiality and privacy simultaneously, especially the access pattern. Specifically, we propose 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 homomorphic 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 mor efficient than existing oblivious storage solutions with the aspects of client and cloud workloads, respectively.

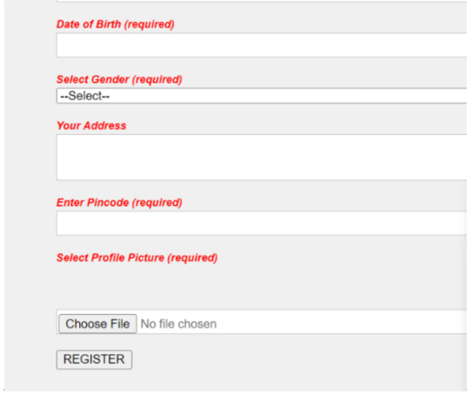
User login:



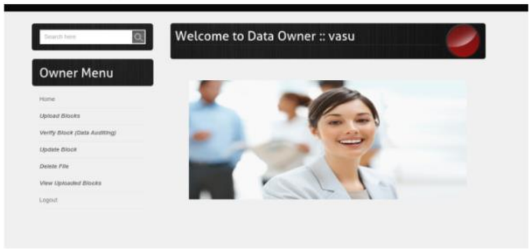


Registration:

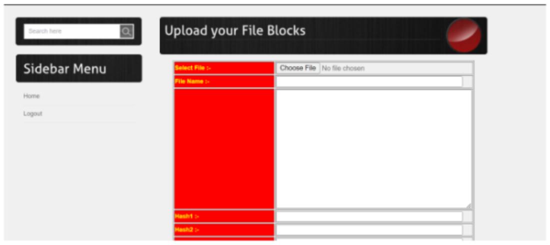




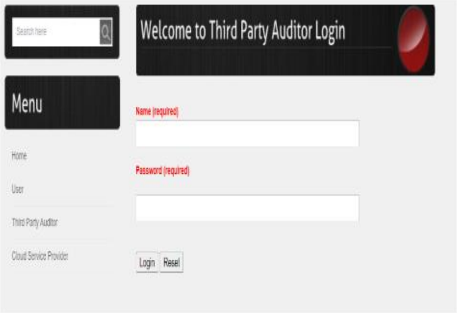
Data owner login:



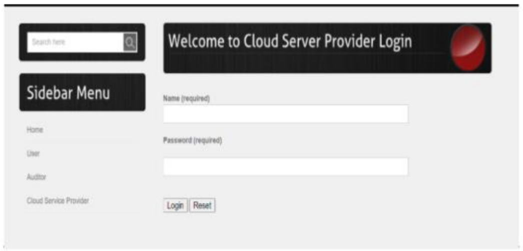
Upload file:



Third party login:



Cloud Server Login:



5. 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.

6.REFERENCE

• M.S.Islam, M. Kuzu, and M. Kantarcioglu, “Access pattern disclosure on searchable encryption: Ramification, attack and mitigation," in 19th Annual Network and Distributed System Security Symposium, NDSS2012, San Diego, California, USA, February 5-8, 2012, 2012. [Online].

Available:

https://www.ndss-symposium.org/ndss2012/access-pattern-disclosure-searchable-encryption-ramification-attack-and-mitigation

- J. Kilian, "Founding cryptography on oblivious transfer," in Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA, 1988, pp. 20–31.[Online].

Available:

https://doi.org/10.1145/62212.62215

- D. Boneh, D. Mazieres, and R. A. Popa, "Remote oblivious storage: Making oblivious ram practical," pp. 1–18, 2011.

- O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996. [Online].

Available:

http://doi.acm.org/10.1145/233551.233553

- J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data," in Public Key Cryptography - PKC 2009, 12th International Conference on Practice and Theory in Public Key Cryptography, Irvine, CA, USA, March 18-20, 2009. Proceedings, 2009, pp. 196–214. [Online].

Available:https://doi.org/10.1007/978-3-642-00468-1 12

- T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Oblivious dynamic searchable encryption via distributed PIR and ORAM," IACR Cryptology ePrint Archive, vol. 2017, p. 1158, 2017. [Online].

Available: http://eprint.iacr.org/2017/1158

•S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: efficient oblivious RAM in two rounds with applications to searchable encryption," in Advances in Cryptology - CRYPTO 2016 - 36th Annual

International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III, 2016, pp. 563–592. [Online].

Available: https://doi.org/10.1007/978-3-662-53015-320

• E. Blass, T. Mayberry, G. Noubir, and K. Onarlioglu, “Toward robust hidden volumes using write-only oblivious RAM,” in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014, 2014, pp. 203–214. [Online].

Available: http://doi.acm.org/10.1145/2660267.2660313

• D. S. Roche, A. J. Aviv, S. G. Choi, and T. Mayberry, “Deterministic, stash-free write-only ORAM,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017, 2017, pp. 507–521. [Online].

Available: http://doi.acm.org/10.1145/3133956.3134051