International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

ENABLING EFFICIENT, SECURE AND PRIVACY-PRESERVING MOBILE CLOUD STORAGE

B. Prathyusha1, G. Sai Priya2, M. Jyothika3, M. Preethi4
1Assistant Professor Department of Information Technology Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.
2,3,4 UG students Department of Information Technology Malla Reddy Engineering College for Women (UGC-Autonomous) Maisammaguda,Hyderabad, TS, India.

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 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 more efficient than existing oblivious storage solutions with the aspects of client and cloud workloads, respectively.

INTRODUCTION

In mobile cloud storage (MCS), data is stored on a cloud and can be accessed from anywhere with mobile devices. Due to the attractive properties, MCS is becoming more and more popular. Some large companies provide MCS services for business purposes, i.e. Apple I Cloud, Drop box, Microsoft One Drive and Google Drive.

In many situations, the cloud is not considered fully trusted. Thus, the client may employ encryption schemes to keep data confidential before uploading it to the cloud. However, in MSC-based applications, data always be related to certain information, such as location information in location based services. In this situation, which item of data is being accessed leaks addition information to the cloud server. By utilizing this leaked information of access pattern, the cloud may infer the operation of the client and even the content of the encrypted data. For example, in a searchable encryption system, a cloud can identify approximately 80% of the search queries by applying a general inference attack with access pattern leakage and minimal background knowledge [1]. Oblivious technology, such as oblivious transfer (OT) [2], oblivious storage (OS) [3] and oblivious random access machine (ORAM) [4], is a kind of technology that can protect both data and access pattern. Generally speaking, these technologies allow a client to access its outsourced data stored in an un trusted cloud without revealing which items have been visited or even what kinds of operations are requested. Due to the high level privacy preservation, these technologies have been widely applied in various application scenarios such as searchable encryption, encrypted hidden volumes, cloud storage, multi-party computation, etc. However, there are some challenges to employ existing oblivious schemes into MCS scenario due to several reasons. Firstly, mobile devices are generally connected to the Internet via wireless networks, such as ad-hoc, LTE, and Wi-Fi. That means the mobile devices have limited communication bandwidth to download and upload data. Thus, some schemes suffered by the well-known communication bandwidth overhead lower bound result O(log N) [4] can not be employed into MCS due to the heavy communication overhead. 1 Secondly, although modern mobile devices, such as mobile phones and tablets, have significantly improvement in terms of computing capability, they still cannot compete with personal computers or other powerful devices. Complicated computation also reduces the battery life of mobile devices. Therefore, some schemes based on fully homomorphic encryption (FHE) [19] or multi-layer onion additively homomorphic encryption [20] are also not suitable for MCS due to complex client-side encryption and decryption computation, although they circumvent the communication lower bound and achieve constant communication bandwidth overhead. Thirdly, many existing oblivious schemesare also suffered by the lager minimum effective item size. Minimum effective item size refers to the minimal number of bits in an effective item of an oblivious scheme required to meet the predefined communication complexity (constant or logarithmic). Lager item size prevents the mobile client from fine-grained accessing its own data. Moreover, it also further increases the communication or computation overhead of existing oblivious schemes.

Some oblivious schemes consider to introduce data locality to improve efficiency. Data locality reveals the tendency of a client to access its data over a short time. Spatial locality and temporal locality are two typical types of reference locality of data access. Spatial locality refers that the client may access the nearby data items if a particular item is accessed. Temporal locality refers that the client will reuse data repeatedly within a short time. By taking spatial locality into consideration in non-constant communication overhead oblivious schemes, the amortized communication overhead whiling accessing a series of items is lower than that whiling accessing one item independently [21]. Taking advantage of temporal locality can also significantly improve efficiency of particular oblivious schemes since if an item is visited, it only requires lightweight computation and communication to access the item again in a short time. However, as far as we know, there is no related work that has considered temporal locality.

Existing system

Goldreich and Ostrovsky introduced the first concept, oblivious random access machine (ORAM), to preserve access pattern privacy. They proposed a concrete solution, Square Root ORAM, and demonstrated a communication overhead lower-bound blowup (logN). In their setting (passive setting), the memory, or cloud in cloud computing application, acted as a passive storage entity and does not execute any computation on data. Under this setting, a series of works had been improved in terms of theory and efficiency. Shi et al. first organized their construction into a binary tree over buckets. By operating blocks along tree paths, the proposed construction achieved O(log3 N) communication worst-case cost. Path ORAM was proposed by Stefanov et al. based upon the binary tree ORAM framework. It achieved the (logN) lower-bound blowup demonstrated by Goldreich and Ostrovsky in passive setting. It was also extremely simpler than other constructions by avoiding using complicated cryptographic primitives and efficient with small end-to-end delay for reasonable parameters.

PROPOSED SYSTEM

In this paper, we propose 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.

Methodology

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.

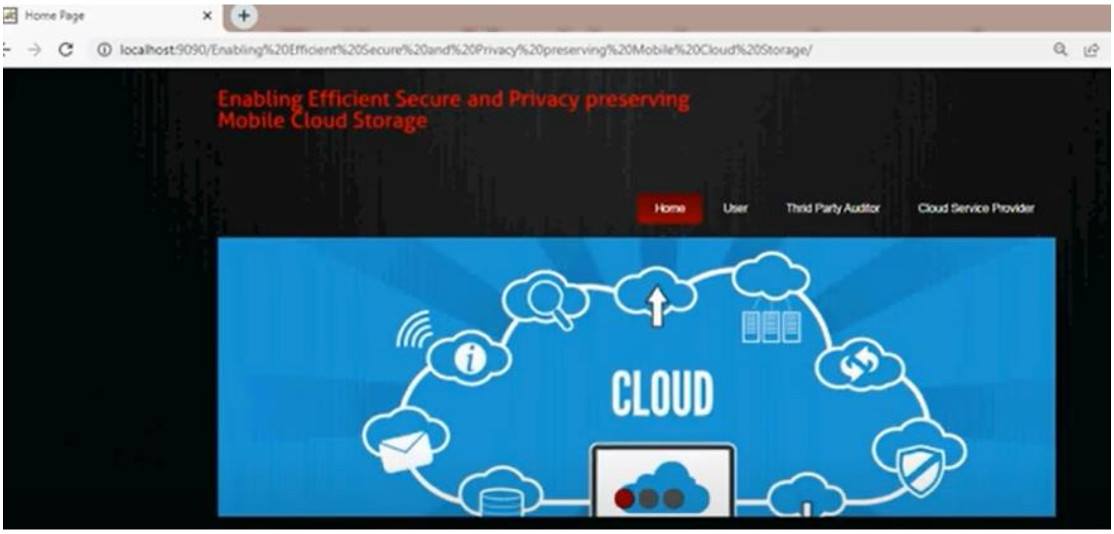

Home Page
localhost:9090/Enabling%20Efficient%20Secure%20and%20Privacy%20preserving%20Mobile%20Cloud%20Storage/
Enabling Efficient Secure and Privacy preserving Mobile Cloud Storage
Home
User
Third Party Auditor
Cloud Service Provider
CLOUD

Fig.1. Home page.

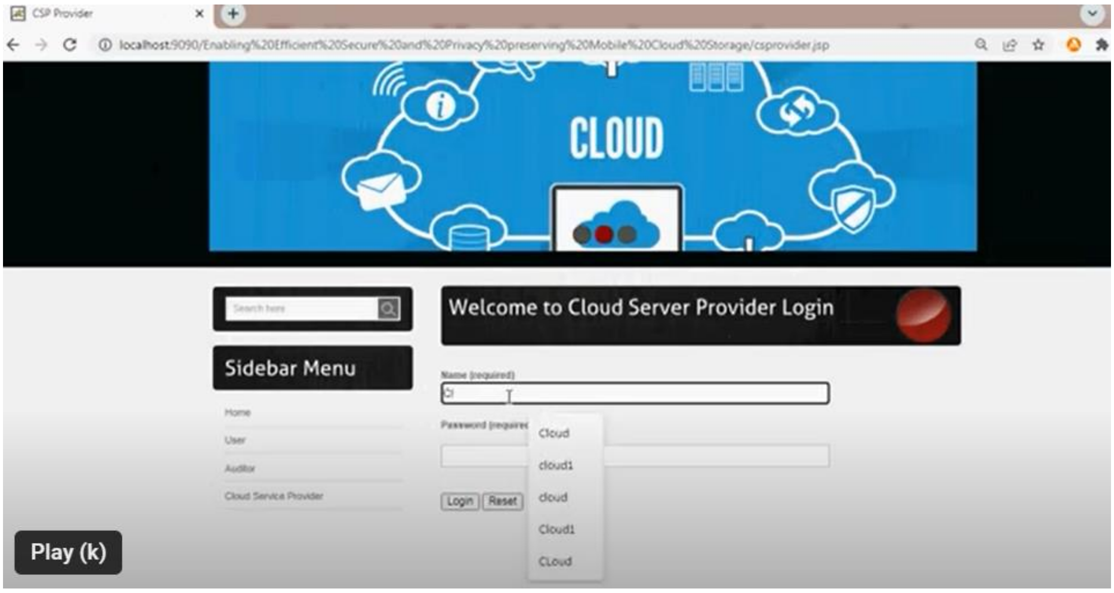


Fig.2. user details

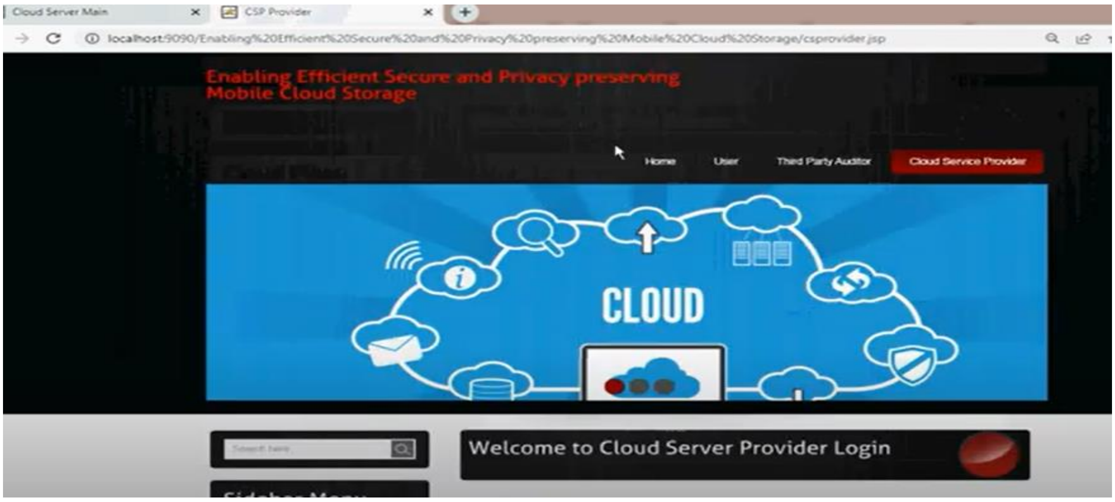
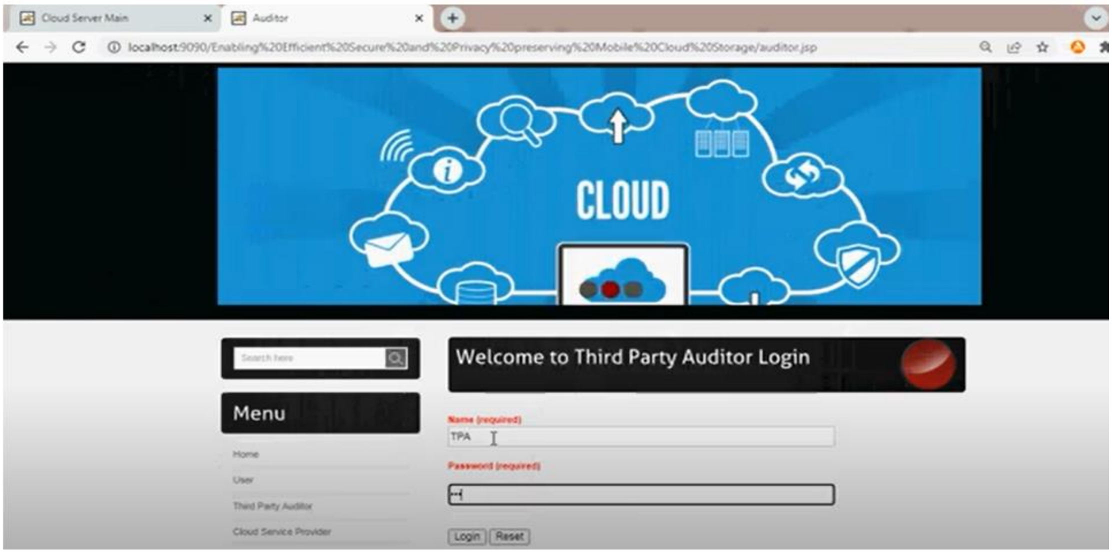

Cloud Server Main
CSP Provider
localhost:9090/Enabling%20Efficient%20Secure%20and%20Privacy%20preserving%20Mobile%20Cloud%20Storage/csprovider.jsp
Enabling Efficient Secure and Privacy preserving Mobile Cloud Storage
Home
User
Third Party Auditor
Cloud Service Provider
CLOUD
Search here
Welcome to Cloud Server Provider Login

Fig.3. server login.



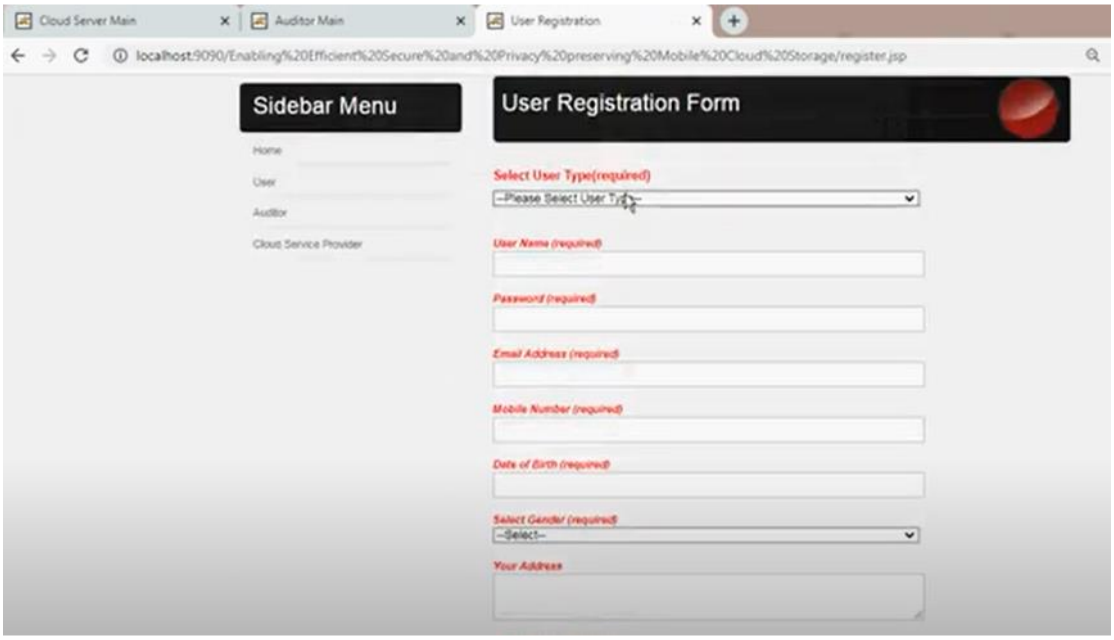
localhost:9090/Enabling%20Efficient%20Secure%20and%20Privacy%20preserving%20Mobile%20Cloud%20Storage/auditor.jsp

Welcome to Third Party Auditor Login

Name (required)
TPA

Password (required)

Fig.4. Third party login.



localhost:9090/Enabling%20Efficient%20Secure%20and%20Privacy%20preserving%20Mobile%20Cloud%20Storage/register.jsp

User Registration Form

Select User Type(required)
--Please Select User Type--

User Name (required)

Password (required)

Email Address (required)

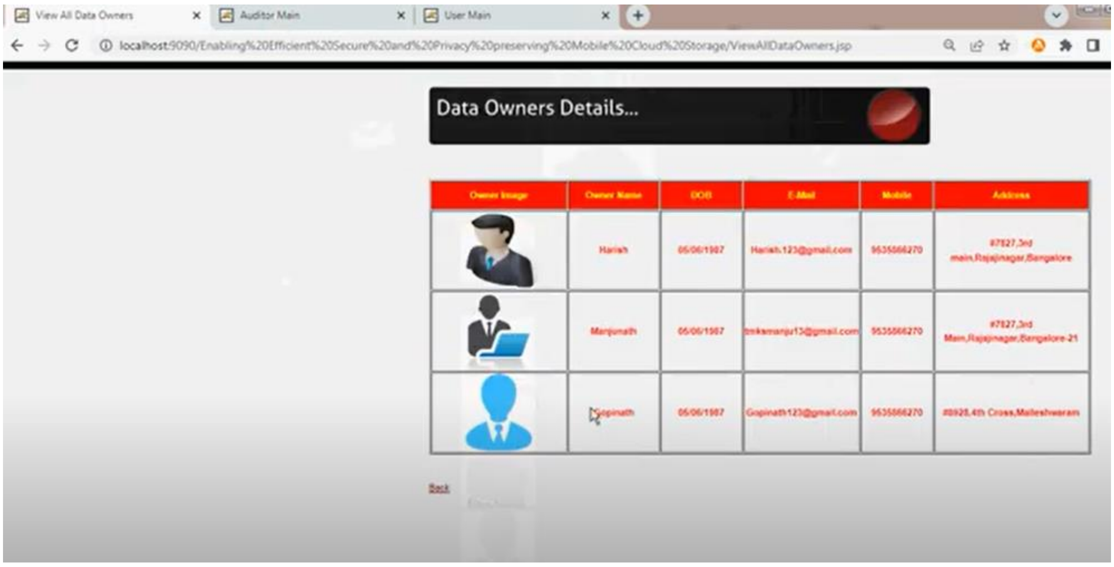
Mobile Number (required)

Date of Birth (required)

Select Gender (required)
--Select--

Your Address

Fig.5. user registration page.



localhost:9090/Enabling%20Efficient%20Secure%20and%20Privacy%20preserving%20Mobile%20Cloud%20Storage/ViewAllDataOwners.jsp

Data Owners Details...

Owner Image	Owner Name	DOB	E-Mail	Mobile	Address
	Harish	05/06/1987	Harish.123@gmail.com	9535866270	#7827,3rd main,Rajajinagar,Bangalore
	Manjunath	05/06/1987	tmksmanju13@gmail.com	9535866270	#7827,3rd Main,Rajajinagar,Bangalore-21
	Gopinath	05/06/1987	Gopinath123@gmail.com	9535866270	#8928,4th Cross,Malleshwaram

Back

Fig.6. Data owners details

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.

REFERANCES

[1] 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, NDSS 2012, 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

[2] 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

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

[4] O. Goldreich and R. Ostrovsky, "Software protection andsimulation on oblivious rams," J. ACM, vol. 43, no. 3, pp.431–473, 1996. [Online]. Available: http://doi.acm.org/10.1145/233551.233553

[5] J. Camenisch, M. Kohlweiss, A. Rial, and C. Sheedy, "Blindand anonymous identity-based encryption and authorisedprivate searches on public key encrypted data," in Public KeyCryptography - PKC 2009, 12th International Conference on Practiceand Theory in Public Key Cryptography, Irvine, CA, USA, March18-20, 2009. Proceedings, 2009, pp. 196–214. [Online]. Available:https://doi.org/10.1007/978-3-642-00468-1 12

[6] T. Hoang, A. A. Yavuz, F. B. Durak, and J. Guajardo, "Obliviousdynamic searchable encryption via distributed PIR and ORAM,"IACR Cryptology ePrint Archive, vol. 2017, p. 1158, 2017. [Online].Available: http://eprint.iacr.org/2017/1158

[7] S. Garg, P. Mohassel, and C. Papamanthou, "TWORAM: efficientoblivious RAM in two rounds with applications to searchableencryption," 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

[8] E. Blass, T. Mayberry, G. Noubir, and K. Onarlioglu, "Towardrobust hidden volumes using write-only oblivious RAM,"in Proceedings of the 2014 ACM SIGSAC Conference onComputer and Communications Security, Scottsdale, AZ, USA,November 3-7, 2014, 2014, pp. 203–214. [Online]. Available:http://doi.acm.org/10.1145/2660267.2660313

[9] D. S. Roche, A. J. Aviv, S. G. Choi, and T. Mayberry,"Deterministic, stash-free write-only ORAM," in Proceedings of the2017 ACM SIGSAC Conference on Computer and CommunicationsSecurity, CCS 2017, Dallas, TX, USA, October 30 - November 03,2017, 2017, pp. 507–521. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134051

[10] E. Stefanov and E. Shi, "Oblivistore: High performance obliviouscloud storage," in 2013 IEEE Symposium on Security and

Privacy,SP 2013, Berkeley, CA, USA, May 19-22, 2013, 2013, pp. 253–267. [Online]. Available: https://doi.org/10.1109/SP.2013.25.