# ABSTRACT

Data storage in remote servers has become popular in recent years with an increasing number of enterprises using services such as Amazon EC2 and github for storing valuable (and potentially private) data. Privacy of this data is essential. One such tool for ensuring complete privacy of server-hosted data is by deploying an Oblivious RAM (ORAM) [] for accessing data. An ORAM effectively "hides" the data access patterns of a user by making all access patterns computationally indistinguishable.

ORAM technology has advanced rapidly in recent years [2–5] with PathORAM [4] achieving the near-optimal bandwidth lower bound established in [1]. Inspite of these promising developments, ORAMs are yet to become feasible for deployment on commercial clouds.

In this paper, we attempt to make PathORAM [4] more practical by reducing the average latency of concurrent client queries. This is achieved by using multiple parallel threads for fetching and eviction of data. We show an improvement in query response time proportional to the number of threads used.


# 1. REFERENCES


[1] Goldreich, O., and Ostrovsky, R. Software protection and simulation on oblivious rams. *Journal of the ACM 43* (1996), 431–473.

[2] Ren, L., Fletcher, C., Kwon, A., Stefanov, E., Shi, E., van Dijk, M., and Devadas, S. Constants count: Practical improvements to oblivious ram. In *24th USENIX Security Symposium (USENIX Security 15)* (Washington, D.C., Aug. 2015), USENIX Association, pp. 415–430.

[3] Shi, E., Chan, T.-H. H., Stefanov, E., and Li, M. Oblivious ram with o((logn)3) worst-case cost. In *ASIACRYPT* (2011).

[4] Stefanov, E., van Dijk, M., Shi, E., Fletcher, C., Ren, L., Yu, X., and Devadas, S. Path oram: An extremely simple oblivious ram protocol. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security* (New York, NY, USA, 2013), CCS '13, ACM, pp. 299–310.

[5] Williams, P., Sion, R., and Tomescu, A. Privatefs: A parallel oblivious file system. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security* (New York, NY, USA, 2012), CCS '12, ACM, pp. 977–988.