Dynamic Searchable Symmetric Encryption

Arpan Kapoor
arpan_b120555cs@nitc.ac.in

September 20, 2015

Domain: Computer Security

Abstract

Searchable symmetric encryption (SSE) allows a client to encrypt its data in such a way that this data can still be searched. The most immediate application of SSE is to cloud storage, where it enables a client to securely outsource its data to an untrusted cloud provider without sacrificing the ability to search over it.

A practical SSE scheme should (at a minimum) satisfy the following properties: sublinear search time, security against adaptive chosen-keyword attacks, compact indexes and the ability to add and delete files efficiently. A SSE scheme to satisfy all the properties outlined above is discussed.

References

[1] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. “Dynamic Searchable Symmetric Encryption”. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS ’12. Raleigh, North Carolina, USA: ACM, 2012, pp. 965–976. ISBN: 978-1-4503-1651-4. DOI: 10.1145/2382196.2382298. URL: http://doi.acm.org/10.1145/2382196.2382298.