SEARCH ON ENCRYPTED DATA

Brisilda Munguli[1], Ana Ktona[2]

[1]Faculty of Natural Science, Albania, Email: brisilda.munguli@fshn.edu.al
[2] Faculty of Natural Science, Albania, Email: ana.ktona@fshn.edu.al

Abstract

A large amount of sensitive and private information is being collected and stored in corporate and government systems throughout the world. With the rise of cloud computing and storage in the last decade, many people have raised concerns about the security issues of outsourced data. The importance and utility of this data, however, prevents it from being encrypted since we would lose the ability to search over it. And to match this, cryptographers have come up with many proposals aiming to solve all of these problems. The area of encrypted search, which is concerned with the design and analysis of cryptographic techniques for searching on encrypted data, could solve this dilemma and fundamentally transform the way we store and process information. The aim of this article is to introduce recent advances in cryptography that address the conflict between two important trends that occur when data gets bigger: on one hand our increased reliance on search and on the other our growing inability to properly secure data. The most well-known of these methods are: property-preserving encryption, functional encryption, fully-homomorphic encryption, searchable symmetric encryption, oblivious RAMs and secure two-party computation. We will look on this technique in details and see the various tradeoffs they provide between efficiency, security and functionality. Property preserving encryption supports fast search on encrypted data but, unfortunately, leaks quite a bit of information to the server. Functional encryption provides slower search but guarantees better security. Fully Homomorphic Encryption, can in theory offer a perfect solution to this, but is extremely inefficient and not currently practical for most real-world situations. Other solutions include Oblivious RAM and special forms of identity-based encryption, but these are both still pretty expensive.

Keywords: *Encrypted data, Big data, Cloud computing, Security*