Preserving Data/Query Privacy Using Searchable Symmetric Encryption

Kevin Curran

Ulster University, School of Computing, Engineering and Intelligent Systems
Londonderry, Northern Ireland

Abstract

The benefits of Cloud computing include reduced costs, high reliability, as well as the immediate availability of additional computing resources as needed. Despite such advantages, Cloud Service Provider (CSP) consumers need to be aware that the Cloud poses its own set of unique risks that are not typically associated with storing and processing one's own data internally using privately owned infrastructure. Recent years have seen several such incidents occur, whereby customer data hosted on the Cloud has been leaked. The true level of anxiety people feel when it comes to being compromised through a cloud service is a difficult measure to ascertain. There has been a change in some enterprises perceptions to the cloud since the Snowden leaks. Once it was leaked that the NSA has indeed been tapping into the links of servers belonging to the likes of Google, Yahoo and Microsoft to capture information from the fiber optic cables - the game changed forever. These companies had seemed to be taken proper precautions as they provided customer traffic encryption in the form of SSL/TLS to users who access some of their main services thus seeming to protect the traffic. They had not it seems counted on the NSA tapping the Google backend 'private' cloud which does not encrypt the traffic. This therefore will be one of the biggest moves in cloud service provision in the days ahead - to provide encryption everywhere possible.

The benefits of the cloud however should win over the concerns. There are some unique security concerns to the cloud such as protecting Virtual Machines, containers, disk images on shared hosts but updates have been rolled out for many of these exploits. The ideal solution to achieving an optimal balance of data security and functionality within the Cloud involves the CSP having the ability to search and operate on data while it is in encrypted form.

New techniques such as Fully Homomorphic Encryption and Searchable Encryption have arisen to make this a reality. Fully-Homomorphic Encryption supports computations over data in encrypted form but an efficient Fully-Homomorphic Encryption remains someway off. Searchable Encryption however, despite being a relatively obscure form of Cryptography is now at the point that it can be deployed and used within the Cloud. Searchable Encryption can allow CSP customers to store their data in encrypted form, while retaining the ability to search that data without disclosing the associated decryption keys to CSPs.

Symmetric Search Encryption (SSE) represents one of the few forms of Searchable Encryption that is achievable using established standardised encryption algorithms. This talk will discuss a Searchable Symmetric Encryption scheme which is efficient enough to be deployed in a Cloud environment to achieve industry acceptable search speeds whilst maintaining Data Privacy.

Keywords: *Homomorphic Encryption, Searchable Symmetric Encryption, Cloud, Privacy*