

Muchos como nosotros, atropellados por la realidad tecnológica, ya tenemos muchos datos en la llamada nube. Tenemos una fe ciega en sea quien sea el respectivo proveedor o administrador nuestros datos están seguros. No se perderán ni alterarán de ninguna forma. Sin embargo, la gran mayoría usamos herramientas gratuitas, sin habernos leído las reglas contractuales aplicables, en las que generalmente se indica que el proveedor puede cerrar el servicio cuando quiera y no se compromete a indemnizar daños que imprevistos causen a los datos.

Mientras tanto los entendidos, así como celebran el desarrollo de esta nueva tecnología también están desarrollando controles y formas de auditoría para proteger los datos más allá de las responsabilidades del proveedor.

Recientemente leímos en una investigación titulada [An efficient data integrity auditing protocol for cloud computing](#), escrita por Neenu Garg, Seema Bawa y Neeraj Kumar, publicada por *Future Generation Computer Systems*, publicada por Elsevier en agosto de 2020, el siguiente resumen: “*Cloud data storage has brought a revolution in Information Technology (IT) sector with its inherent benefits like ease of use, cost efficiency, location independence etc. By outsourcing data on cloud servers, users can reduce the hardware expenditures and can simplify the data management process. A Cloud Service Provider (CSP) is responsible for offering secure data storage services. However, using these services in a secured*

manner and ensuring data integrity in these remote cloud servers remains to be an issue for the clients. In this paper, we propose an efficient approach for data integrity auditing in cloud computing. The objective of proposed protocol is to minimize the computational complexity of client during system setup phase of the auditing protocol. Based on the properties of bilinear pairings, the proposed protocol is publicly verifiable and supports dynamic operations on data. The security of proposed protocol relies on the stability of Computational Diffie Hellman Problem (CDHP) in a Random Oracle Model (ROM). Finally, the performance of proposed protocol has been evaluated by implementing a prototype of the protocol and conducting experiments. The results obtained have been compared with state-of-the-art protocols and demonstrates the high efficiency and adaptability of proposed protocol by clients with limited resources.”

Cada vez son más las áreas en las que se hace necesaria una auditoría para aumentar la seguridad que hemos depositado en unas afirmaciones que hace un tercero. Las hay de informaciones y las hay de procesos como en el caso que hemos planteado.

La cuestión es que el dominio de los sistemas de información, que no se queda en su diseño o uso, pues comprende su control y aseguramiento, es cada vez más importante y necesario para los contadores, inevitablemente comprometidos a trabajar en el medio empresarial que invierte sistemáticamente en estas herramientas.

Hernando Bermúdez Gómez