

Homomorphic encryption for cloud users

January 17 2020, by David Bradley



Credit: CC0 Public Domain

A new approach to encryption could improve user perception of cloud computing services where the users are concerned about private or personal data being exposed to third parties. Writing in the *International Journal of Cloud Computing*, the team outlines a proposed homomorphic encryption system.

Homomorphic [encryption](#) was developed more than a decade ago and represented something of a significant breakthrough in security. By definition, it allows computations to be carried out on a ciphertext (the user's data in the cloud [service](#), for instance), generating an result that is still encrypted but when decrypted by the user matches exactly the result that would be obtained if the same computational operations had been carried out on the user's plain-text as opposed to the uploaded ciphertext. It is thus very useful for ensuring the privacy of data uploaded to cloud and other outsourced computer services.

Despite all the benefits of cloud computing, the very nature of the services wherein a user by necessity must share data with a third party, the cloud service provider, means that there are endless issues of trust. Indeed, many users have not adopted [cloud services](#) because they recognize that those services being in a different domain to their own personal or private system offers malicious third parties an opportunity to access their data in a way that would not be possible if that data were held only on the user's domain. The use of sophisticated tools such as [homomorphic encryption](#) adds a layer or reassurance that should open up cloud services to all but the most neurotic of user at least within limits.

More information: Secure cloud computing using homomorphic construction. arxiv.org/ftp/arxiv/papers/1409/1409.0829.pdf

Swathi, V. and Vani, M.P. (2019) 'Secure cloud computing using homomorphic construction', Int. J. Cloud Computing, Vol. 8, No. 4, pp.354-370. www.inderscience.com/jhome.php?jcode=ijcc

Provided by Inderscience

Citation: Homomorphic encryption for cloud users (2020, January 17) retrieved 23 April 2024

from <https://techxplore.com/news/2020-01-homomorphic-encryption-cloud-users.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.