Locking down the cloud

November 8 2013

A software re-encryption system could allow users to pay for and run applications "in the cloud" without revealing their identity to the cloud host. The same approach would also allow the software providers to lock out malicious users.

Writing in the International Journal of Grid and Utility Computing, Ronald Petrlic, Stephan Sekula and Christoph Sorge of the University of Paderborn, Germany, explain how the emergence of cloud computing has allowed end users access to powerful computer resources hosted at remote locations via the internet. Such services include simple applications such as web-based email and file storage as well as more sophisticated social networking and multimedia communication tools, website hosting systems, file editing and manipulation and many other applications.

However, with ease of access, comes the issue of privacy. To utilize proprietary cloud services users must provide personal details or otherwise tie their identity to the digital rights management (DRM) system or the license built into the software. Inherent in this approach to access is the problem that the cloud provider may not be the licensing body for the software itself and so a third party will often require access to the user's credentials too, which gives rise to privacy issues. Moreover, there is no reason why a legitimate user of the software need give their identity to the software provider either, as long as they have fulfilled their commitments - financial or otherwise - to obtaining a license to use the software.

Petrlic and colleagues have developed what they call "a privacy-friendly architecture" for future cloud computing systems where software licensing and software payment is required. The utility of their approach will be immediately apparent once cloud software providers abandon so-called freemium and advertising-driven business models and simply start charging users to use the applications they develop. In this system, users authorise a service provider - the cloud host - to buy a certain piece of software from a software provider. However, the service provider does not learn what software is bought, as the software provider sends an encrypted version of the application together with the corresponding licence to the cloud host. Each time the user wants to use the software on their cloud host, the program execution is initialized at a computing centre of their choosing anonymously.

By implementing such a system, the cloud host is remunerated for the hosting services and the encryption facilities, they provide, the software company gets its license fee, and the user gets to use the software they paid for "in the cloud" without the cloud host being able to identify them or even knowing what software is being used.

"Privacy protection will become more important in the cloud computing scenarios of the future," the team says, equally, "Proper payment concepts are crucial for software providers to take part in future cloud computing."

More information: "A privacy-friendly architecture for future cloud computing" in *Int. J. Grid and Utility Computing*, 2013, 4, 265-277

Provided by Inderscience Publishers

Citation: Locking down the cloud (2013, November 8) retrieved 27 April 2024 from

https://phys.org/news/2013-11-cloud.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.