

# Anti-hacker team develops data sharing scheme for cloud storage

December 21 2018

---



SUSU students. Credit: SUSU

In cloud computing, there is still a pressing issue of data security. Scientists from the Laboratory of Problem-Oriented Cloud Computing at [South Ural State University](https://www.susu.ru/) have developed an algorithm of improving

information security, which allows to avoid providers' conspiracy.

For several years, the relevant methods of ensuring [information](#) security in [cloud systems](#) have been studied by the SUSU scientists, members of the international team supervised by Andrei Tchernykh, Head of the Laboratory of Problem-Oriented Cloud Computing Environments at the University and Director of the Laboratory at the Centre for Scientific Research and Higher Education at Ensenada, Mexico.

"There exist different methods of ensuring [information security](#), like cryptography. With the appearance of cloud computing, distributed [clouds](#), and information saving in cloud computing, we also get a problem of how to save information stored in a cloud," explains Andrei Tchernykh.

One of the main problems is putting trust in a [service provider](#), along with guaranteeing confidentiality, integrity, authenticity and fail-safety of information at all stages of its existence, as well as with smoothness of operation, protection against unauthorised access, and saving of users' personal data transferred and processed via a cloud. Moreover, [cloud computing](#) experts claim that there exists a risk of a cloud providers' collusion.



Prof. Andrei Tchernykh. Credit: SUSU

The international team of researchers has managed to close access to information in case of such a "collusion." The article, published in the International Journal of Approximate Reasoning (listed in Q1 of Scopus scientometrical database), suggested a mechanism of double coding of information.

"We have proved that the developed algorithm complies with the formal definition of computing security. If the conspirators do not know the secret key, the chance of getting to the secret is minimal. This solution is reliable when it comes to protection against insiders; even if you have access to some part on the inside, you won't be able to obtain the

complete information," states Andrei Tchernykh.

The existing reliable systems that are next-to-impossible to be hacked are overly redundant, as when standard coding methods are used, the volume of information has to be increased so that it could not be restored from separate chunks. This requires additional financial expenses. The algorithm suggested by the SUSU scientists and their partners is less redundant but still solves the security problem.

To test the feasibility of the suggested approach, an experiment is being designed, which will allow for simultaneous use of up to 10 cloud resources to store data. To read the data, the system will retrieve them upon a user's click. Such an approach will ensure automatic distribution of the user's data among a number of cloud services while improving the [security](#) and reliability of cloud storage.

**More information:** Andrei Tchernykh et al. AC-RRNS: Anti-collusion secured data sharing scheme for cloud storage, *International Journal of Approximate Reasoning* (2018). [DOI: 10.1016/j.ijar.2018.07.010](#)

Provided by South Ural State University

Citation: Anti-hacker team develops data sharing scheme for cloud storage (2018, December 21) retrieved 25 April 2024 from <https://phys.org/news/2018-12-anti-hacker-team-scheme-cloud-storage.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.