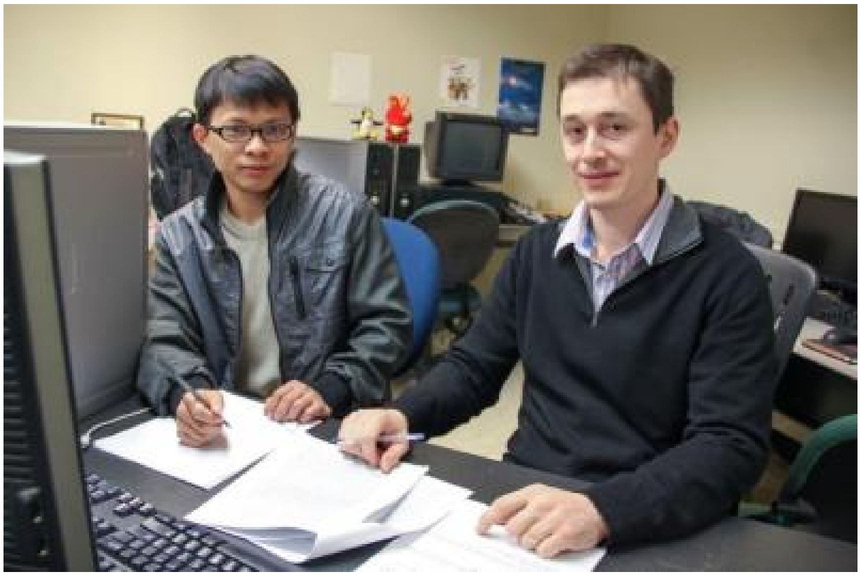
Computer scientists feted for ways to store data with untrusted cloud providers

March 4 2013



NJIT researchers received a top honor for their ideas on better ways to ensure the integrity and long-term reliability of data stored at potentially untrusted cloud storage providers. "Towards Self-Repairing Replication-Based Storage Systems Using Untrusted Clouds," was written by Bo Chen, a doctoral candidate, and his advisor, Assistant Professor Reza Curtmola, New Jersey Institute of Technology. Credit: NJIT

NJIT researchers received a top honor for their ideas on better ways to ensure the integrity and long-term reliability of data stored at potentially untrusted cloud storage providers. "Towards Self-Repairing Replication-Based Storage Systems Using Untrusted Clouds," was written by Bo

Chen, a doctoral candidate, and his advisor, NJIT Assistant Professor Reza Curtmola, both in NJIT's College of Computing Sciences (CCS).

The work recently received the "Outstanding Paper Award" from the prestigious 3rd ACM Conference on Data and Application Security and Privacy (CODASPY 2013) and was published in February of 2013 in the *Proceedings of the Third ACM Conference on Data and Application Security and Privacy.*

"We are very happy to see that this important work has received such a high level of peer recognition," said CCS Interim Dean James Geller and chair of the department of computer science. "Computer security today is on everyone's mind and we take our mission seriously at NJIT to get the word out so that computing can be safer and easier for everyone—whether people are trying to protect banking accounts or military secrets. This is an enormous growth area in research and education."

"We wanted to take an in depth look at cloud storage security," said Curtmola. "This is an especially important issue for anyone dealing with large amounts of data that are supposed to be stored for a long period, such as archival and backup data. Using our techniques data owners can audit the service provided by the cloud and assess the risk of outsourcing their data to the cloud. We think the information will be of great help to anyone dealing with data storage."

Unlike previous work in this area, the NJIT paper proposed a new paradigm, in which the data owner is able to outsource not only the storage but also the management of her data. Whenever data corruption is detected, the storage servers collaborate among themselves to repair the corruption, and the data owner acts only as a coordinator. This minimizes the load on the data owner during repair and represents a departure from previous work, which imposes a heavy burden on the data owner during data repair.

The proposed paradigm has the advantage of minimizing the workload for data owners, but it also introduces a new type of attack: A set of malicious storage servers could collude to generate on the fly data that should be stored at all times. Thus, the main technical challenge in the paper was how to enforce that the untrusted servers manage the data properly over time. The main insights behind the solution were: (a) replicas of the data are differentiated based on a controllable amount of masking, which offers flexibility in handling different adversarial strengths, and (b) replica generation is time consuming. The NJIT researchers validated the practicality of their solution through a software prototype built on Amazon's cloud platform.

This work is part of a series of articles supported by a National Science Foundation CAREER grant awarded to Curtmola in 2011.

Curtmola is an expert in information security and applied cryptography. His research interests include security of cloud services, security of wireless networks and security of mobile computing.

Provided by New Jersey Institute of Technology

Citation: Computer scientists feted for ways to store data with untrusted cloud providers (2013, March 4) retrieved 23 June 2024 from https://phys.org/news/2013-03-scientists-feted-ways-untrusted-cloud.html