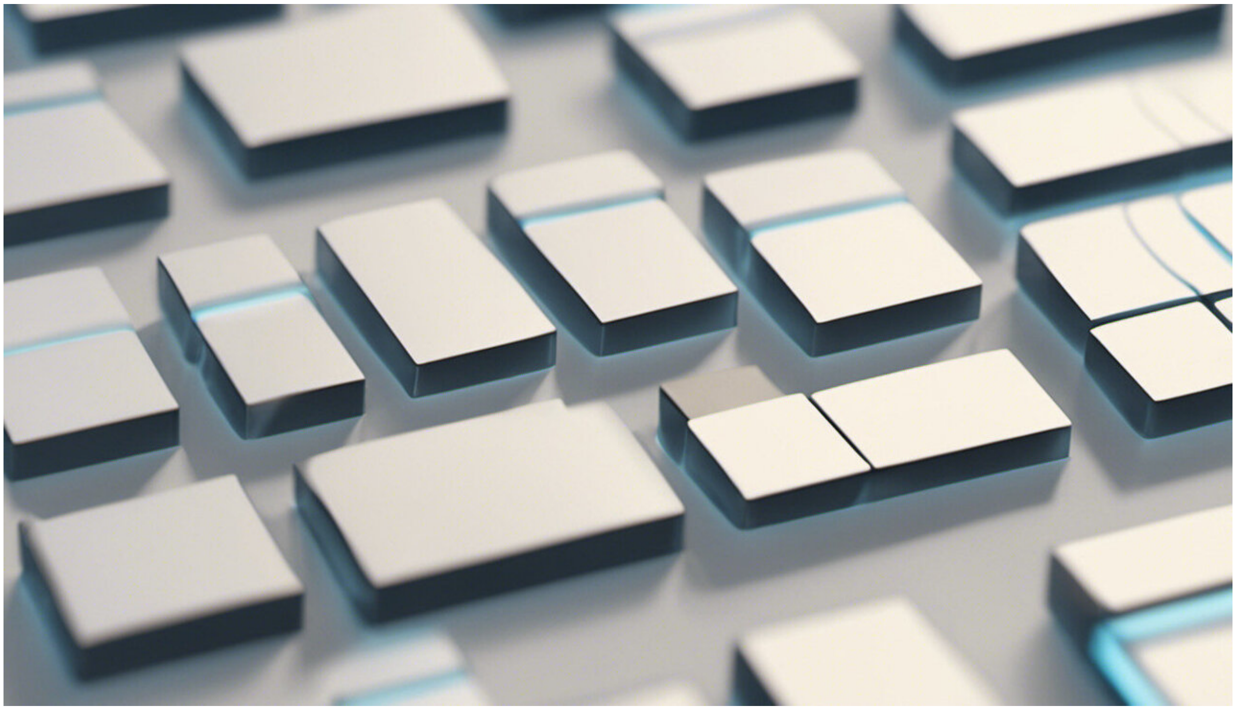
Data-sharing scheme shows the way towards low-cost, flexible and secure cloud storage

August 14 2013



Credit: AI-generated image (disclaimer)

Wider adoption of cloud storage services by organizations has been hindered by security and privacy issues. A consequence of storing data on the cloud is that, by its very nature, the storage infrastructure is not owned by the same organization that owns the data. In addition, the data of one user is stored along with that of many others. Traditional schemes for ensuring security can only protect data privacy by sacrificing convenient operations such as searching and sharing.

Now, Shu Qin Ren and his colleague Khin Mi Mi Aung at the A*STAR Data Storage Institute in Singapore have devised a scheme that would not only allow organizations to store data on the cloud without loss of privacy but also permit searching and sharing of the data. The system is able to preserve the benefit of the cloud's specialized low-cost storage infrastructure while overcoming its current privacy and flexibility limitations. "The scheme may potentially push forward the wider adoption of cloud storage usage for organizations," says Ren.

The solution proposed by the researchers involves a central 'key manager', who specifically manages data authentication and access authorization. In their scheme, data stored on the cloud is encrypted by its owner and hence is indecipherable to anyone else—including the cloud storage provider. A secret key required to unlock the encryption is generated and kept by the owner, who also determines an access policy for other users. This policy is implemented by the key manager, who generates a second access key, which is then passed back to the owner. Next, the owner wraps the original encryption key in this second layer of protection. The key manager is then able to pass on the second 'public' key to authorized third parties to allow them to access the data.

Under traditional privacy schemes, the owner manages both the encryption of and access to their data. Sharing with a third party typically involves retrieval and decryption of the data by the owner and therefore some loss of privacy. Under Ren and Aung's scheme—entitled 'Privacy Preserved Data Sharing'—the third party only deals with the key manager and, after authorization, receives the public key without interacting with the data's owner, thus allowing privacy to be maintained.

"The research team is now building a secure data searching and sharing prototype to test on structured data such as in databases," says Ren. "The next step is to support unstructured data."

More information: Ren, S. Q. & Aung, K. M. M. PPDS: Privacy Preserved Data Sharing scheme for cloud storage, *International Journal of Advancements in Computing Technology* 4, 493–499 (2012). www.aicit.org/ijact/global/pap … l?jname=IJACT&q=1294

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: Data-sharing scheme shows the way towards low-cost, flexible and secure cloud storage (2013, August 14) retrieved 2 May 2024 from https://phys.org/news/2013-08-data-sharing-scheme-low-cost-flexible-cloud.html