Cloud data storage security approach taps quantum physics

November 14 2023

Secure cloud data storage method uses quantum random numbers as encryption keys and disperses them via Shamir's secret sharing algorithm. Credit: American Institute of Physics

Distributed cloud storage is a hot topic for security researchers around the globe pursuing secure data storage, and a team in China is now merging quantum physics with mature cryptography and storage techniques to achieve a cost-effective cloud storage solution.

Shamir's secret sharing, a known method, is a key distribution algorithm. It involves distributing private information to a group so that "the secret" can be revealed only when a majority pools their knowledge. It's common to combine quantum key distribution (QKD) and Shamir's secret sharing algorithm for secure storage—at an utmost security level. But utmost security solutions tend to bring substantial cost baggage, including significant cloud storage space requirements.

In *AIP Advances*, the team presents its method that uses quantum random numbers as encryption keys, disperses the keys via Sharmir's secret sharing algorithm, applies erasure coding within ciphertext, and securely transmits the data through QKD-protected networks to distributed clouds. The article it titled "Quantum-secure fault-tolerant distributed cloud storage system."

Their method not only provides quantum security to the entire system but also offers fault tolerance and efficient storage—and this may help speed the adoption of quantum technologies.

"In essence, our solution is quantum-secure and serves as a practical application of the fusion between quantum and cryptography technologies," said corresponding author Yong Zhao, vice president of QuantumCTek Co. Ltd., a quantum information technology company. "QKD-generated keys secure both user data uploads to servers and data transmissions to dispersed cloud storage nodes."

The team explored whether quantum security services could expand beyond secure data transmission to offer a richer spectrum of quantum security applications such as data storage and processing.

They came up with a more secure and cost-effective fault-tolerant cloud storage solution. "It not only achieves quantum security but also saves storage space when compared to traditional mirroring methods or ones

based on Shamir's secret sharing, which is commonly used for distributed management of sensitive data," said Zhao.

When the team ran the solution through experimental tests ranging from encryption/decryption, key preservation, and data storage, it proved to be effective.

The solution is currently feasible from both technological and engineering perspectives: It meets the requirement for relevant quantum and cryptographic standards to ensure a secure storage solution capable of withstanding the challenges posed by quantum computing.

"In the future, we plan to drive the commercial implementation of this technology to offer practical services," said Zhao. "We'll explore various usage models in multiuser scenarios, and we're also considering integrating more quantum technologies, such as quantum secret sharing, into cloud storage."

More information: Quantum-secure fault-tolerant distributed cloud storage system, *AIP Advances* (2023). DOI: 10.1063/5.0172384

Provided by American Institute of Physics