Size-Efficient Encryption Scheme that Secures Clouds and Blockchains

(2018-004)

Encryption method that allows for data stored in the cloud to remain encrypted and secure during seaches.

Market Overview

This encryption method provides the ability for users of cloud storage platforms to retrieve or query encrypted information or data without having to first decrypt the data, reducing the risk of exposing sensitive data. Hackers have broken into preexisting encrypted clouds, accessing the personal data of millions of people worldwide. In 2017, data breaches jumped to 29 percent in the United States alone; hitting a record high. With preexisting encryption technologies, data cannot be searched without decrypting it first, which puts it at a higher risk of being accessed to malicious parties. A Clemson University researcher has developed a fully homomorphic encryption (FHE) method that allows data to be searched while still remaining encrypted, reducing the risk of access for unauthorized parties.

Technical Summary

As distributed computing becomes more and more popular, there is an urgent need to protect privacy of massive sensitive data stored in clouds and blockchains. The traditional encryption schemes can not allow searching on encrypted data without decryption first. The proposed fully homomorphic encryption method is a practical encryption scheme that protects the privacy of massive amounts of sensitive data stored in clouds, blockchains, and company databases. In addition to this, the FHE scheme allows for all possible searches to be performed in encrypted form, and decrypted by the data owner.

Application

Encryption, Data Security

Development Stage

Prototype

Advantages

- Data is encrypted with a private key, decrypting only for the user with the private key
- Data encryption has a much smaller ciphertext expansion, reducing the total file size
- All search functions can be performed with this method, allowing information to be found in encrypted form

App Type	Country	Serial No.	Patent No.	CURF Ref. No.	Inventors
Provisional	United States	62/687,681	N/A	2018-004	Dr. Shuhong Gao

About the Inventors

Dr. Shuhong Gao

Professor of Mathematics at Clemson University

Dr. Shuhong Gao earned his Ph.D. in Combinatorics and Optimization from the University of Waterloo in Ontario, Canada. From 1993-1995, Dr. Gao was a postdoctoral fellow of computer science at the University of Toronto. Dr. Gao currently serves on the Editorial Board of the international Journal Finite Fields and Their Applications. He has authored and coauthored over 50 scholarly articles, and coauthored two books on cryptology. Dr. Gao's research focuses on cryptography, finite fields, symbolic computationl, and quantum computation.

For more information on this technology contact:

curf@clemson.edu
Please put technology ID in subject line of email.