Using blockchain for efficient management of data access (2019-026)

Blockchain protocol for access security

Market Overview

The number of data breaches is steadily growing and is prompting the need for new approaches to encrypting data access. Current methods for encrypting data are rapidly reaching the end of their lifespan due to the capabilities and effectiveness of quantum computing. However, the demand for blockchain security is currently growing. Several companies are in dire need of encryption technologies that effectively address the new generation of cyber security threats. Clemson researchers have created a new method managing data encryption that uses blockchain to enable streamlined data and access storage. This invention allows audit and compliance staff to identify the individuals who had access to which versions of specific data in a privacy preserving manner.

Technical Summary

This technology enables the management of data access by leveraging blockchain. The method utilizes key encryption keys (KEK) to efficiently add and remove access to data. The system is self-documenting, which allows data forensics personnel to determine who had access to which version of the data. Using the blockchain to update data access permissions allows this to be done in an anonymous way. It is also resilient to denial of service attacks, since the distributed ledger is more resistant to those attacks.

Application

Cyberinfrastructure; cyber encryption

Development Stage

Preliminary Prototype

Advantages

- Efficient management of data access permissions
- Acces right indelibly documented
- Distibution of rights can be anonymous and is resilient to denial of service attacks

App Type	Country	Serial No.	Patent No.	CURF Ref. No.	Inventors
Provisional	United States	NA	NA	2019-026	Dr. Richard Brooks, Tony Skjellum, Lu Yu

About the Inventors

Dr. Richard Brooks

Professor of Electrical and Computer Engineering at Clemson University

Dr. Richard Brooks is a professor of electrical and computer engineering at Clemson University. He received his Ph.D. in Computer Science from Louisiana State University. Brooks has been a Principal Investigator on several research projects funded by the National Science Foundation, Department of Energy, National Institute of Standards, Army Research Office, Office of Naval Research, and the BMW Corporation. These projects included research on coordination of combat missions among autonomous combat vehicles (ARO), situation and threat assessment for combat command and control (ONR), detection of protocol tunneling through encrypted channels (AFOSR), security of intelligent building technologies (NIST), experimental analysis of Denial of Service vulnerabilities (NSF), mobile code security (ONR), and security analysis of cellular networks used for vehicle remote diagnostics (BMW). His current research efforts focus on authentication and authorization of exa-scale computing systems and establishing Internet freedom in West Africa.

For more information on this technology contact:

A. Chris Gesswein
Director of Licensing for Technology Transfer
E: agesswe@clemson.edu
P: (864) 656-0797