Block Verifiable Dynamic Searchable Encryption Using Redactable Blockchain

Authors: Ruizhong Du, Na Liu, Mingyue Li, Junfeng Tian

Abstract: To solve the problems of low efficiency, inflexible updates, and the high storage cost of existing result-verifiable searchable encryption schemes, we propose a dynamic, searchable encryption scheme with block verification using a redactable blockchain. First, the inverted index is divided into blocks, the verification tag corresponding to the block index is uploaded to the redactable blockchain, and smart contracts are used to perform block verification of the query results to improve the query and verification performance. Furthermore, we use blockchain rewriting technology to update the tags in the result checklist, improving the data update performance and scalability of the blockchain and ensuring the constant storage overhead of the blockchain. Security analysis confirms that our proposals guarantee the correctness and completeness of the query results. Experimental results show that our proposed approach can improve query efficiency and result in verification efficiency under the premise of the low-speed growth of the blockchain data scale. In particular, the advantages become more significant as the data collection scale grows.

Keywords: searchable encryption, redactable blockchain, block index, result verification, smart contract

Conference Title: ICICS 2023: International Conference on Information and Computer Security
Conference Location: Amsterdam, Netherlands
Conference Dates: January 23-24, 2023