sensors

MDPI

Article

Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage

Hassan Mansur Hussien [1,*], Sharifah Md Yasin [1,2,*], Nur Izura Udzir [1] and Mohd Izuan Hafez Ninggal [1]

[1] Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang 43400, Malaysia; izura@upm.edu.my (N.I.U.); mohdizuan@upm.edu.my (M.I.H.N.)
[2] Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, Serdang 43400, Malaysia
* Correspondence: hassanalobady@gmail.com (H.M.H.); ifah@upm.edu.my (S.M.Y.); Tel.: +60-182015604 (H.M.H.)

Abstract: Blockchain technology provides a tremendous opportunity to transform current personal health record (PHR) systems into a decentralised network infrastructure. However, such technology possesses some drawbacks, such as issues in privacy and storage capacity. Given its transparency and decentralised features, medical data are visible to everyone on the network and are inappropriate for certain medical applications. By contrast, storing vast medical data, such as patient medical history, laboratory tests, X-rays, and MRIs, significantly affect the repository storage of blockchain. This study bridges the gap between PHRs and blockchain technology by offloading the vast medical data into the InterPlanetary File System (IPFS) storage and establishing an enforced cryptographic authorisation and access control scheme for outsourced encrypted medical data. The access control scheme is constructed on the basis of the new lightweight cryptographic concept named smart contract-based attribute-based searchable encryption (SC-ABSE). This newly cryptographic primitive is developed by extending ciphertext-policy attribute-based encryption (CP-ABE) and searchable symmetric encryption (SSE) and by leveraging the technology of smart contracts to achieve the following: (1) efficient and secure fine-grained access control of outsourced encrypted data, (2) confidentiality of data by eliminating trusted private key generators, and (3) multikeyword searchable mechanism. Based on decisional bilinear Diffie–Hellman hardness assumptions (DBDH) and discrete logarithm (DL) problems, the rigorous security indistinguishability analysis indicates that SC-ABSE is secure against the chosen-keyword attack (CKA) and keyword secrecy (KS) in the standard model. In addition, user collusion attacks are prevented, and the tamper-proof resistance of data is ensured. Furthermore, security validation is verified by simulating a formal verification scenario using Automated Validation of Internet Security Protocols and Applications (AVISPA), thereby unveiling that SC-ABSE is resistant to man-in-the-middle (MIM) and replay attacks. The experimental analysis utilised real-world datasets to demonstrate the efficiency and utility of SC-ABSE in terms of computation overhead, storage cost and communication overhead. The proposed scheme is also designed and developed to evaluate throughput and latency transactions using a standard benchmark tool known as Caliper. Lastly, simulation results show that SC-ABSE has high throughput and low latency, with an ultimate increase in network life compared with traditional healthcare systems.

Keywords: blockchain; decentralised storage; data privacy; attribute-based encryption; searchable encryption; access control; chosen-keyword attack; standard adversary model

Citation: Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Ninggal, M.I.H. Blockchain-Based Access Control Scheme for Secure Shared Personal Health Records over Decentralised Storage. *Sensors* **2021**, *21*, 2462. https://doi.org/10.3390/s21072462

Academic Editor: Valderi R. Q. Leithardt

Received: 2 January 2021
Accepted: 15 February 2021
Published: 2 April 2021

1. Introduction

Blockchain technology has gained considerable attention in many industrial and academic aspects. In particular, the merging of blockchain technology and smart contracts has enabled a ubiquitous decentralised interaction of nodes, thereby yielding an applaudable opportunity for certain applications in private and public domains, such as healthcare systems [1], biomedical sciences [2], and smart cities [3]. In healthcare systems, blockchain