Decentralized Framework for Medical Images Based on Blockchain and Inter Planetary File System

Mohamed Yaseen Jabarulla, Giljun Jung, and Heung-No Lee*, *Senior Member, IEEE*

***Abstract*—Current practices regarding electronic sharing of medical image data cause privacy concerns because they rely on third-party services. In this work, we implement a secure sharing of medical image data using blockchain and a distributed file system known as Inter Planetary File System (IPFS). The image content is hashed and protected by an open asymmetric encryption technique. In addition, we use the steganography technique to encode the patient's description on medical images to protect the originality of the image. The proposed framework eliminates third-party intermediaries for image sharing and stores secure images on the network.**

I. Introduction

Medical health record sharing over high speed network is a common practice for expediting diagnosis and allowing immediate treatment. However, current technologies for transferring medical images are inadequate owing to maintenance cost, privacy, storage, and security concerns. It is important for a storage solution to be secure while allowing un-delayed accessibility for radiologists and patients without the risk of privacy and the cost of medical image acquisition by eliminating centralized parties [1].

In this abstract, we aim to propose a new decentralized system in which the two technologies IPFS [2] and blockchain [3] are effectively combined, enabling the provision of secure sharing of medical images over a cross domain network.

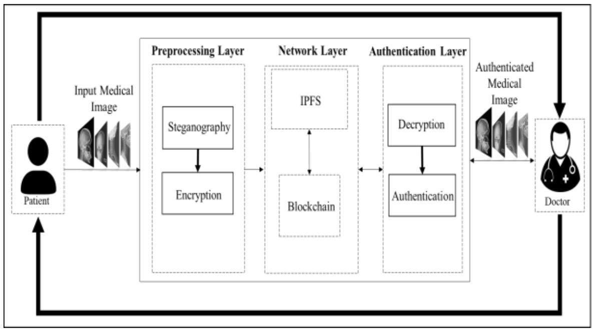

Figure.1: Overview of Proposed System.

II. System Description and Prototype Testing

The proposed scheme is shown in Fig. 1. It consists of the preprocessing layer, network layer, and authentication layer. The image pre-processing layer includes the steganography and encryption techniques [4]. The network layer is used to upload encrypted image in IPFS and store user information on the blockchain ledger. Finally, the authentication layer performs decryption and verifies the authenticity of the image.

The image preprocessing layer is used to hide patient information on the image. This procedure accomplished by calling the Stegencoder function in Matlab. Further, asymmetric encryption is performed using the openPGP (Pretty Good Privacy) protocol.

We initialized our own IPFS in a Windows 10 operating system and uploaded the encrypted file to the IPFS network. At this point, we are updating our transactions on the blockchain server using a Postman API software. Once the block is approved, content such as IPFS hash, image description, timestamp, sender and receiver address will be stored on the blockchain. Now, a legitimate user can retrieve the image from the IPFS node using a IPFS hash value.

For the sake of brevity, we highlight, the authenticity of the image is verified by two cases: 1) Image is verified with its checksum, so if the hash is changed, then IPFS knows the image has been tampered. 2) If the information in the blockchain ledger does not match with the extracted hidden information, then any further processing of the transaction is not allowed.

III. Conclusion

We presented a decentralized application based on blockchain and IPFS for storing and sharing medical images. The image files are secured before uploaded to IPFS using a steganography and asymmetric encryption technique. Decentralized storage and sharing of medical images are protected with multilevel security measures, and the need for third party intermediaries and administrative structures can be eliminated.

References

[1] S. G. Shini, T. Thomas, and K. Chithraranjan, "Cloud based medical image exchange-security challenges," Procedia Eng., vol. 38, 2012, pp. 3454–3461.

[2] J. Benet, "IPFS - content addressed, versioned, P2P file system," 2014.

[3] T. T. Kuo, H.E. Kim and L. O. Machado, "Blockchain distributed ledger technologies for biomedical and health care applications". J. Am. Med. Inform. Assoc., Vol. 24, no. 6, 2017, pp.1211-1220.

[4] S. Gupta, A. Goyal, B. Bhushan, "Information hiding using least significant bit steganography and cryptography". Int. J. Educ. Comput. Sci. Vol. 6, 2012, pp. 27–34.

This work was supported by a National Research Foundation of Korea (NRF) grant provided by the Korean government (MSIP) [NRF-2018R1A2A1A19018665].

M. Y. Jabarulla, G. Jung, H. N. Lee* are with Gwangju Institute of Science and Technology, Gwangju, 61005, South Korea.
E-mail:Yaseen@gist.ac.kr, jinpeg112@gist.ac.kr, heungno@gist.ac.kr.