International Journal of E-Health and Medical Communications
Volume 11 • Issue 1 • January-March 2020

SeFra:
A Secure Framework to Manage eHealth Records Using Blockchain Technology

Charanya R., Vellore Institute of Technology, Vellore, India
Saravanaguru R.A.K., Vellore Institute of Technology, Vellore, India
Aramudhan M., PKIET, Karaikal, India

ABSTRACT

Electronic health information is an efficient technique for providing health care services to society. Patient health information is stored in the cloud, to allow access of eHealth information from anywhere, and at any time, but the technical problems are security, privacy, etc. Sharing the medical data in a trustless environment is overcome by the proposed framework SeFra. The proposed work provides a secure framework to manage the eHealth record by using blockchain (SeFra). For authentication purposes, a temporal shadow is used and the integrity of health records is ensured by blockchain technology.

KEYWORDS

Ehealth, EHR, Merkle Tree, Sefra, Temporal Shadow

INTRODUCTION

Nowadays, most of the industries are moving through a digital transformation journey and technologies like IoT, cloud, and mobility. Digital transformation is applicable for Healthcare system too, but the only problem is trust and security. Sharing the healthcare data in cross-institute is one of the biggest challenging tasks (Cheong, Shin, & Joeng, 2009). Even healthcare data are shared securely, integrity problem is still unchecked, this is will be overcome by the proposed framework. The patient details are very sensitive information, so it's our responsibility to protect from an unauthorized user. The existing eHealth system facing a lot of privacy and security issues. In the proposed system the sensitive encrypted health is protected over the cloud. In this paper, the authors focus on privacy, integrity, and anonymity. The data privacy means only authorized user can access the healthcare data (Kolodner, Cohn, & Friedman, 2008). The institutional health data is highly confidential and it is an asset to the institution. The anonymity is another way to secure the health record, remove the identical information and share only partial data (Charanya, Aramudhan, Mohan, & Nithya, 2013). Adding privacy in the healthcare system is more important for patient and service provider (Charanya & Aramudhan, 2016). This is achieved by using Blockchain.

DOI: 10.4018/IJEHMC.2020010101

Blockchain technology was first introduced by Satoshi Nakamoto in 2008. It's a new technology used in online cryptocurrency like bitcoin. Blockchain enables trust and transparency due to the peer-to-peer distributed ledger. The Blockchain is a distributed ledger, an endless list of records called blocks. The Cryptography techniques are used to secure the records. By using the hash pointer, each block is linked with the previous block. The two types of blockchain configuration are public and private. Public means its permissionless, anyone can participle in the network, whereas private means its permission, it's available to the known person. For example, an organization performs 15 transactions per second, each transaction receives its own signature, the digital signature is combined by using a tree structure and form single fingerprint. The fingerprint is sent to the next layer such as a service provider. Once validated its stored in the blockchain, then all users can see, then the copy is sent to the organization to store locally. The main disadvantage of the traditional blockchain, speed, scalability, and storage capacity.

The Blockchain is a distributed public ledger, with a set of rules the transactions get appended, achieved by distributed consensus of participants in the system. Participants can keep track of the transaction in a distributed way, where each participant have the copy of transactions (ledger). The Integrity of data is validated by using Blockchain.

Blockchain technology is used in healthcare to solve healthcare security problems. The encrypted health information is hashed and hashed value is stored in a distributed way, shared by multiple parties that secure all the records. The information is stored in the blockchain. Here each record is added to the previous record, never removed. Each record has own timestamp. All the transactions are encrypted and verified by the network. Keyless Signature Infrastructure blockchain deployed by Estonia government, data scales to 10^{12} items of data every second.

The existing work drawback is overcome by our proposed system. According to Provchain, the user has to pay fees to get provenance service and also pay for blockchain network also it's not supporting federated cloud. The BSPP protocol secures the eHealth system also it allows the authorized doctor to access the patient health record and it's not supporting the conjunctive keyword search, also planning to propose specific miner and verification election algorithm. The entire drawback is overcome by the proposed SeFra framework.

The objective of the proposed work is to give rights to the authenticated user to access the health record, also it maintains the integrity of the health record by using blockchain. The mostly researcher are the miners and the rewards are to get the anonymized record, also this framework is work with both blockchain, and cloud service provider is used. It supports the services like a doctor can access the health record and also the doctor can view the patient history details. The time taken to store the encrypted health record and retrieve the record is only a few seconds. The access privilege service is provided by means of a smart contract. The patient billing details are automatically sent to the insurance company. The researchers get the anonymized details as miner reward.

ROAD MAP

This paper is organized as follows: Section I Is Introduction. Section II discussed existing techniques and its drawbacks. Section III discussed Overview of the framework and its functionalities. Section IV Implementation, and result and conclude in Section V.

RELATED WORK

In attribute-based encryption, private key issued by the trusted authority and verified the attributes issued for each user. The user shares data according to a policy written over attributes and issued across different user domains. Limitation in this approach is the trusted authority has to perform a dual role like verify attributes across the different organization and issue private keys to every user. This is overcome by using blockchain. In blockchain, permissions are given based on the ownership