Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of
Informatics and Radioelectronics

UDC 621.396

GAO
Yalu

MEDICAL DOCUMENT MANAGEMENT SYSTEM BASED ON BLONCHAIN TECHNOLOGY

Abstract
for a Master's Degree
in the Specialty 1-45 80 01 Infocommunication Systems and Networks

_____

Supervisor
PhD,
Astrovskiy I.I

_____

Minsk 2024

INTRODUCTION

With the advent of technology, electronic technology has gradually permeated every aspect of human life. The traditional healthcare system has failed to keep pace with the rapid development of modern life, and the emergence of electronic health records (EHR) has effectively addressed the issues of storing, querying, sharing, and preventing medical errors related to patient diagnosis information. EHRs enable patients to have a more comprehensive diagnosis information, allowing doctors to quickly and accurately understand their medical history during consultations and provide new diagnosis results.

However, the current EHR system faces two major challenges: centralized storage and difficulty in sharing medical information. The centralized storage of medical records in hospitals raises the risk of data tampering, and the lack of interoperability between different hospital systems makes it difficult for patients to share their medical records when seeking treatment at other hospitals. If medical records are lost or misplaced, doctors can only rely on patient communication to understand their medical history, which may lead to biases and affect medical judgment or result in repeated tests, thereby wasting medical resources. Furthermore, doctors' treatment plans are also crucial information that can provide new insights for other doctors, but currently, there is no mechanism for sharing treatment plans.

Blockchain technology has three main features immutability, decentralization and transparency. It can solve the problem of medical information silos. And the data storage of blockchain is completely open, each node in the blockchain can store transaction information, and can selectively store all or part of it according to the situation. If someone wants to alter the data stored in the blockchain, they need to alter more than half of the nodes, which is theoretically impossible. This feature enables the implementation of immutable blockchain, ensuring data security. Moreover, through the design of blockchain codes, treatment plans can be shared.

This study introduces a novel blockchain-based electronic health record (EHR) system that utilizes the inherent advantages of blockchain technology to improve the security and accessibility of medical records. By doing so, it addresses the critical issue of centralized storage and the challenges associated with sharing medical information across different healthcare systems. In addition, the study provides an in-depth comparative analysis of two advanced encryption techniques: proxy-heavy encryption algorithms and searchable encryption algorithms. This in-depth analysis aims to identify the most effective methods to ensure secure storage and fast retrieval of medical data in cloud environments.

The findings and methodology of this research are directly aligned with the stated aim and task of the research, as detailed in the general description.

GENERAL DESCRIPTION OF WORK

Relevance of the subject

The work corresponds to paragraph 1 «*Digital information and communication and interdisciplinary technologies, production based on them*» of the State Program of innovative development of the Republic of Belarus for 2021–2025.

The work was carried out in the educational institution Belarusian State University of Informatics and Radioelectronics within the framework of research work 21-2033 "Processing, coding and transmission of information in network-centric systems".

The aim and tasks of the work

The aim of the work is looking for solving centralized storage and difficulty sharing problems in medical information recording.

To achieve this aim, the following tasks were solved in the dissertation:

1 Analyse the features of blockchain and apply them to build a blockchain-based medical system. The blockchain medical system primarily consists of five layers, and we mainly focus on the data layer, which explores how to add patient information to the blockchain to achieve decentralization and tamper-proof features. Blockchain is a decentralized distributed ledger technology that achieves immutability, transparency, and decentralization through a series of structural features. The proposed solution utilizes private chains and consortium chains, where each hospital has its private chain and server, and multiple private chains are combined to build a consortium chain

2 Implement secure access to patient data for third-party data users using proxy re-encryption technology. With the patient's authorization, nodes on the consortium chain search for the original ciphertext of the patient's medical records, perform proxy re-encryption on the original ciphertext, and send the transformed ciphertext to the third-party data user. The data user then decrypts the ciphertext using their private key.

3 Implement secure search using searchable encryption techniques. The consortium chain stores a secure index constructed by keyword indexing. When a patient or data user needs to use electronic medical records, the patient generates a search trapdoor using their private key and sends it to the consortium chain. The nodes on the consortium chain then perform the search.

Personal contribution of the author

The content of the paper reflects the individual contributions of the authors. It includes algorithm improvement, conducting experiments, comparing with existing algorithms, processing and analysing results, and formulating conclusions.

Testing and implementation of results

The main provisions and results of the dissertation work were reported and discussed at: International scientific and technical seminar ″Technologies of information transmission and processing″ (Minsk, April, 2024) and 60th scientific conference of graduate students, undergraduates and students(Minsk, March, 2024)

Author's publications

According to the results of the research presented in the dissertation, 2 author's works was published, including: 1 articles and 1 abstracts in conference proceedings.

Structure and size of the work

The dissertation work includes an introduction, an overview of related work, proposed algorithms, experimental results, conclusion, and bibliography.

The total volume of the thesis work is 68 pages, including 58 pages of text, 26 figures, 4 tables, a list of bibliographic sources used, and a list of author's publications on the topic of the thesis.

Plagiarism

An examination of the dissertation «*MEDICAL DOCUMENT MANAGEMENT SYSTEM BASED ON BLONCHAIN TECHNOLOGY*» by Author's Full Name was carried out for the correctness of the use of borrowed materials using the network resource «Turnitin» (access address: www.turnitin.com/login_page.asp) in the online mode 29.05.2024. As a result of the verification, the correctness of the use of borrowed materials was established (the originality of the thesis is 81 %)

SUMMARY OF WORK

Introduction

The widespread adoption of electronic health record (EHR) systems has significantly enhanced the efficiency of storing and sharing medical information. Despite these advancements, current EHR systems still encounter several critical challenges. Firstly, the centralized storage of medical records is vulnerable to data leakage and tampering, compromising patient privacy and data integrity. Secondly, the lack of effective interconnectivity between EHR systems of different medical institutions impedes information sharing, negatively impacting the diagnostic and treatment efficiency for patients seeking care across institutions.

Blockchain technology, with its distributed ledger, encrypted security, and tamper-proof features, offers a promising solution to these challenges. Its decentralized architecture can replace traditional centralized storage, ensuring the

security and integrity of medical data. Moreover, the open and sharable nature of blockchain can break down medical information silos, facilitating efficient interconnection of medical data across organizations and regions.

Comparative Analysis

This study conducts a comparative analysis of the proxy re-encryption algorithm and the searchable encryption algorithm, aiming to optimize secure storage and rapid retrieval of medical data in cloud environments.

Blockchain Architecture

In the first chapter, the main architecture of blockchain applications is analyzed, focusing on six layers: Data, Network, Consensus, Incentive, Contract, and Application. This study primarily examines the Data layer and the integration of patient data into the blockchain.

When a new transaction occurs (e.g., patient information), it is broadcast to the entire blockchain network. Each node in the network verifies the transaction's legitimacy via algorithms like Proof of Work or Proof of Stake. This consensus mechanism ensures that the blockchain remains secure and reliable.

Implementation

In the second chapter, the study explores blockchain technology's application in the healthcare system using the Ganache and MetaMask platforms. MetaMask allows secure user authentication and transaction signing with private keys, while Ganache provides a local blockchain network for developing and testing EHR systems. Figures 1 and 2 illustrate these processes.

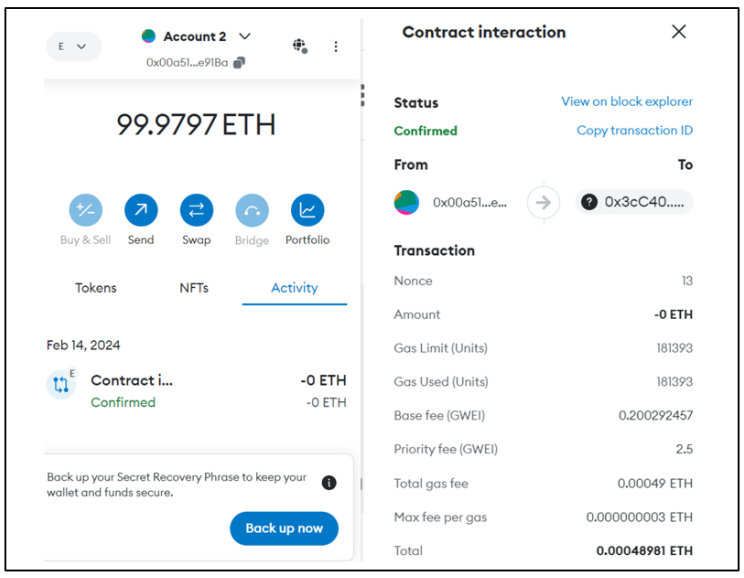

Figure 1 –User authentication and transactions

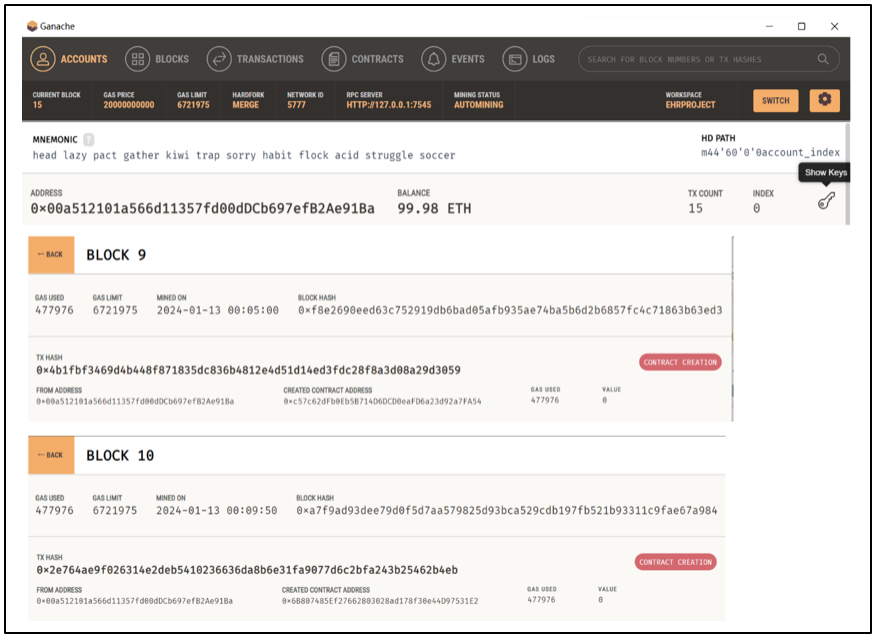

Figure 2 – Virtual local blockchain environment

Proxy Re-Encryption

Chapter two demonstrates that blockchain technology can effectively address data security and information sharing issues in current EHR systems. However, data access and sharing by third parties still pose privacy risks. Proxy re-encryption (PRE) allows for secure data sharing without exposing the data owner's decryption key.

Searchable Encryption

In the third chapter, to facilitate rapid searches for patient information in extensive medical data, a searchable encryption scheme is proposed. This scheme enables searching encrypted data without revealing the plaintext. There are two types: Symmetric Searchable Encryption (SSE) and Asymmetric Searchable Encryption (ASE). The study primarily focuses on SSE and its various algorithms for different scenarios.

Experimental Results

The study tested the running times of several SSE algorithms on a database of 600 documents, as depicted in Figure 9. Results indicate that while some algorithms (e.g., PI or Construction 5.1) offer faster search speeds, others (e.g., SSE-1 or SSE-2) require less storage space. For large datasets and complex queries, PIBAS or PI2LEV may be preferable, whereas DP17 is ideal for frequently updated datasets. Table 1 provides a comprehensive comparison of different searchable algorithms, considering factors such as search speed, algorithm complexity, and storage space requirements.

Table 1 – Comparison of different searchable algorithms

	Time Complexity	Space Complexity	Database size
SSE-1	O(n)	O(n)	n
SSE-2	O(n)	O(n)	n
PIBAS	O(log n)	O(n)	n
PIPTR	O(log n)	O(n)	n
PI2LEV	O(log n)	O(n)	n
PI	O(log^2 n)	O(n)	n
Section 5	O(log n)	O(n)	n
DP17	O(log n)	O(n)	n

This study demonstrates that blockchain technology, combined with advanced cryptographic techniques like proxy re-encryption and searchable encryption, can significantly improve data security and sharing efficiency in EHR systems. The findings suggest practical implementations for enhancing patient data security and accessibility across healthcare institutions.

CONCLUSION

Contributions and innovations of this thesis

This research explores the use of blockchain technology in healthcare systems, specifically addressing the decentralized and tamper-proof characteristics that can still lead to unauthorized access to patient data and difficulties in securely granting third-party users access to patient data. To address these issues, the study proposes the use of a proxy re-encryption algorithm in the blockchain-based healthcare system to enable secure access to patient data for third-party users. The algorithm transforms ciphertext among the delegator, proxy, and delegate, allowing the proxy to convert the ciphertext generated by the delegate into the ciphertext of the same message generated by the delegator.

The study also proposes the use of searchable encryption technology to enable secure searching and protect data privacy. The consortium blockchain stores a secure index composed of keyword indices, and when a patient or data user needs to access EHR data, the patient uses their private key to generate a search trapdoor and sends it to the consortium blockchain, where the nodes perform the search.

Chapter 2 and Chapter 3 explore the feasibility of proxy re-encryption and searchable encryption, respectively, in blockchain-based healthcare systems. The research applies the proxy re-encryption algorithm to the data retrieval stage of the blockchain-based EHR solution, ensuring secure access to patient data by third-party data users.

The study also examines the current state of research on searchable encryption technology, introducing the research mechanisms and analyzing symmetric and asymmetric searchable encryption. The research compares and contrasts different searchable encryption algorithms, each with its advantages and disadvantages, and considers the specific medical scenario, encryption and decryption efficiency, search performance, and the balance between security, efficiency, and functional requirements. The main contributions and innovations of the whole paper can be summarized as follows:

1 Proposed the use of a proxy re-encryption algorithm to enable secure access to patient data for third-party users in a blockchain-based healthcare system, addressing the issues of unauthorized access and secure data sharing.

2 Introduced the application of searchable encryption technology in blockchain-based healthcare systems, allowing for secure searching and retrieval of encrypted patient data while protecting privacy.

3 Conducted a thorough analysis and comparison of different searchable encryption algorithms, providing insights into the trade-offs between security, efficiency, and functional requirements for specific medical scenarios.

Further research work

While we have individually investigated the applicability of proxy re-encryption and searchable encryption in blockchain-based healthcare systems, how to integrate these two techniques to achieve greater synergistic effects is a direction for our future research as follows:

1 Investigate the scalability and performance optimization of the proposed proxy re-encryption and searchable encryption solutions in large-scale blockchain-based healthcare systems. Given the continuous growth of electronic health record (EHR) data volumes, research is needed to optimize the system to support fast and secure data access and searching.

2 Study the deep integration of the proxy re-encryption and searchable encryption techniques with emerging blockchain platforms and healthcare data standards, ensuring the seamless integration of the proposed solution with existing systems and improving the convenience of deployment and application

3 Conduct comprehensive security and privacy assessments of the proposed EHR data sharing solution based on proxy re-encryption and searchable encryption. Provide formal proofs to demonstrate the security of keyword privacy and message privacy, and verify the security of the solution through real-world testing.

4 Further expand the research scope to consider more complex use cases and requirements in the medical domain, such as supporting complex queries based on symptoms, diagnoses, and other criteria, implementing finer-grained access control

policies, and integrating data analytics capabilities into the system to support medical decision-making.

LIST OF AUTHOR'S PUBLICATIONS

A-1 Yalu Gao Design of speech recognition system based on attention mechanism / Yalu Gao // Технологии передачи и обработки информации : материалы Международного научно-технического семинара, Минск, март-апрель 2023 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол.: В. Ю. Цветков [и др.]. – Минск, 2023. – С. 132–134.

A-2 Yalu Gao Application of blockchian in electronic healthare record / Yalu Gao // 60-я научная конференция аспирантов, магистрантов и студентов, Минск, 11-15 марта 2024 года / Белорусский государственный университет информатики и радиоэлектроники; – Минск, 2024 (in publish).