Enhanced Decentralized Cyber security for Medical Data Sharing Using Digital Signature

Mrs.G.Pavithra[1], Mrs.Shankari[2], Dr.N.Purushothaman[3]

[1] Master of Engineering, Department of Computer Science and Engineering, SKP Engineering College, Tiruvannamalai.

[2] Assistant Professor, Department of Computer Science and Engineering, SKP Engineering College, Tiruvannamalai.

[3] Professor and Head of the Department, Department of Computer Science and Engineering, SKP Engineering College, Tiruvannamalai.

Abstract- *An infrastructure build in the edge computing platform which is reliable to challenge the commercial and non-commercial IT development communities of data streams in high dimensional data cluster modeling. This project research is mainly focuses the effective medical disease prediction and data sharing scheme in the cloud storage is presented. In our security system, we remove the attribute matching function, where attributes will be hidden into the anonymous access structure. In the AKE(Authentication Key Exchange) Algorithm, the collected information for encrypted and then stored on a cloud server such that only authorized users, such as the data owner and the doctors, can access. However, smart terminals are usually limited in computing power and users' privacy issues remain.*

Keywords: AKE, Cloud computing, Medical disease prediction, Secure data sharing, Access control

I. INTRODUCTION

The rapid growth of digital healthcare systems has made electronic medical records (EMRs) an essential part of modern healthcare. Medical data is frequently shared among hospitals, laboratories, insurance companies, and healthcare professionals. However, centralized storage systems are vulnerable to cyberattacks, unauthorized access, data breaches, and single points of failure.

A decentralized cybersecurity framework combined with digital signature technology provides a secure solution for medical data sharing. Decentralization distributes medical records across multiple nodes, reducing the risk of data loss and improving system availability. Digital signatures ensure authentication, integrity, and non-repudiation, allowing only authorized users to access or modify medical records. The proposed system enhances patient privacy while maintaining secure and efficient healthcare communication.

II. RELATED WORK

Several researchers have proposed secure healthcare data-sharing mechanisms using blockchain, encryption, and digital signatures.

Blockchain-based healthcare systems provide decentralized storage but often suffer from scalability and storage limitations.

Cloud-based medical record systems offer easy accessibility but remain vulnerable to centralized cyberattacks.

Attribute-Based Encryption (ABE) enables fine-grained access control but increases computational overhead.

RSA and ECC-based digital signatures provide authentication and integrity for sensitive medical data.

Hybrid security frameworks combine blockchain, encryption, and digital signatures to improve privacy and security.

Despite these advancements, many existing systems face challenges in scalability, latency, and efficient key management. The proposed system addresses these limitations through an enhanced decentralized architecture with optimized digital signature verification.

III. METHODOLOGY

The proposed methodology consists of the following phases:

Step 1: User Registration

Patients, doctors, hospitals, and administrators register with the system.

Step 2: Key Generation

Public and private keys are generated using Elliptic Curve Cryptography (ECC).

Step 3: Medical Data Upload

Patient records are encrypted before storage in decentralized nodes.

Step 4: Digital Signature Creation

The healthcare provider digitally signs the encrypted medical record using their private key.

Step 5: Secure Data Sharing

Authorized users request access to patient records.

Step 6: Signature Verification

The receiver verifies the digital signature using the sender's public key.

Step 7: Data Access

After successful verification, the encrypted data is decrypted and displayed.

IV. EXPERIMENTAL RESULTS

Software Requirements

Operating System: Windows 10/11 or Linux

Programming Language: Python or Java

Database: MongoDB/MySQL

Framework: Flask/Django/Spring Boot

Blockchain Platform: Hyperledger Fabric or Ethereum

IDE: Visual Studio Code / Eclipse

Hardware Requirements

Processor: Intel Core i5 or above

RAM: 8 GB

Storage: 256 GB SSD

Internet Connection

V. SYSTEM IMPLEMENTATION

Software Requirements

Operating System: Windows 10/11 or Linux

Programming Language: Python or Java

Database: MongoDB/MySQL

Framework: Flask/Django/Spring Boot

Blockchain Platform: Hyperledger Fabric or Ethereum

IDE: Visual Studio Code / Eclipse

Hardware Requirements

Processor: Intel Core i5 or above

RAM: 8 GB

Storage: 256 GB SSD

Internet Connection

VI. SYSTEM MODULES

Module 1: User Registration

Registers patients, doctors, hospitals, and administrators.

Module 2: Authentication Module

Verifies user identity using secure login credentials.

Module 3: Medical Record Management

Uploads, stores, and updates encrypted medical records.

Module 4: Digital Signature Module

Generates and verifies digital signatures for medical documents.

Module 5: Decentralized Storage Module

Stores encrypted medical data across decentralized nodes.

Module 6: Access Control Module

Allows only authorized users to access patient records.

Module 7: Audit and Monitoring Module

Maintains logs of all data access and sharing activities

VII. ADVANTAGES

- Enhanced cybersecurity through decentralization.
- Strong authentication using digital signatures.
- Ensures data integrity and confidentiality.
- Prevents unauthorized modifications.
- Eliminates a single point of failure.
- Supports secure medical data sharing.
- Improves patient privacy.
- Fast signature verification.
- High availability and scalability.
- Suitable for modern smart healthcare systems.

REFERENCES

[1]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
[2]. W. Stallings, Cryptography and Network Security, 8th Edition, Pearson.
[3]. D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography, 2020.
[4]. M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
[5]. A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Healthcare: Challenges and Opportunities," IEEE Access.
[6]. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics," Future Generation Computer Systems, 2018.
[7]. NIST, Digital Signature Standard (DSS), FIPS PUB 186-5, 2023.