COMP3018 Computing Project 2024/2025

Contents

Project Title

CloudChain: Exploring Consensus Algorithms for Scalable and highly available Blockchain Data Inventory Systems

Links

Github Link: https://github.com/DCYXboi/MAL3018-Computing-Project

Problems of blockchain technology in healthcare sector

The healthcare industry has seen a surge in digital transformation, with cloud computing and blockchain technologies playing increasingly prominent roles. Blockchain technology offers several potential benefits, including improved data integrity, security, and transparency. However, its application in cloud security within the healthcare sector presents distinct challenges. These issues stem from the nature of blockchain itself, as well as the complexities of healthcare data management. This essay explores the key problems associated with implementing blockchain technology in cloud security for healthcare and solutions provided to further improve the technology.

Existing Applications in healthcare sector using blockchain technology

Blockchain Type

- **Permissioned blockchains** (like Hyperledger Fabric, Guardtime's KSI, and Chronicled) ensure more control over who can participate in the network, providing enhanced security in healthcare settings where strict access control is necessary.
- **Public or hybrid blockchains** (like Ethereum used by MedRec, Solve.Care) rely on smart contracts for transparency and patient control but may require more robust measures to ensure privacy and scalability

All applications listed below is permissioned based blockchain application which I will be explain in detailed below.

App/platform	Primary purposes	Blockchain type	Data Management	Security Features	Key Benefits	Best For
Guardtime	Securing national-level health data	KSI blockchain	Immutable logs, no key management	Real-time auditing, data integrity verification	National-scale security for healthcare data	National healthcare systems (e.g., Estonia)
MedicalChain	Secure sharing and management of electronic health records	Hyperledger Fabric	Decentralized health record sharing via smart contracts	Role-based access, permissioned blockchain	Telemedicine support, secure sharing of records	EHR integration with patient-centric control

Patientory	HIPAA-compliant patient data management	Ethereum-based (Permissioned)	Decentralized storage of health data	HIPAA compliance, encryption, patient-centric control	Secure decentralized medical data management	Healthcare data management with compliance
Chronicled	Pharmaceutical supply chain verification	Ethereum (Permissioned)	Tracking drug authenticity and chain of custody	Tamper-proof tracking, real-time monitoring	Reduces counterfeit drugs, ensures supply chain security	Pharma companies tracking drug authenticity
Nebula Genomics	Genomic data storage and management	Permissioned blockchain	Patient-controlled genomic data storage	Privacy-focused, patient data monetization	Secure genomic data sharing and patient monetization	Researchers and patients sharing sensitive genomic data

Data Management

- **Guardtime** employs its KSI (Keyless Signature Infrastructure) blockchain technology primarily to secure health data at a national scale. It focuses on ensuring the integrity of data rather than storing the data itself on the blockchain. Guardtime provides a way to timestamp and verify the authenticity of health records, enabling organizations to maintain an immutable audit trail of all data interactions. This approach facilitates data integrity without the need to share sensitive patient information directly on the blockchain, enhancing privacy and security
- **MedicalChain** provide decentralized access to health records, ensuring data is stored and shared across multiple providers with patient control.
- **Chronicled** focus on the pharmaceutical industry, ensuring the integrity and traceability of drugs and supply chain data.
- **Nebula Genomics** emphasizes patient control over highly sensitive genomic data, enabling patients to decide who can access their data.
- **Factom** integrates with existing health systems to provide immutable, timestamped logs of interactions with medical records, ensuring transparency and integrity.
- **Patientory** focuses on managing Electronic Health Records (EHR) securely and efficiently using a permissioned blockchain infrastructure. It allows healthcare providers to store and access patient data while giving patients control over their health records. Patientory's platform uses decentralized storage for health data, ensuring that patient information is only accessible by authorized individuals. This model not only enhances security but also allows for interoperability among different healthcare providers.

As mentioned above, all existing healthcare systems using blockchain technology focuses on authenticity, integrity, traceability and decentralizing the whole systems, improving in data security. CloudChain is a system that will be focused more on the scalability and availability aspects while also maintaining the data integrity and security that is available in all other applications. This application will be similar to Nebula Genomics, which primary focus is genomic data storage and management, while CloudChain will be focusing on storing patient's sensitive data in the cloud server and isolated physical server as backup.

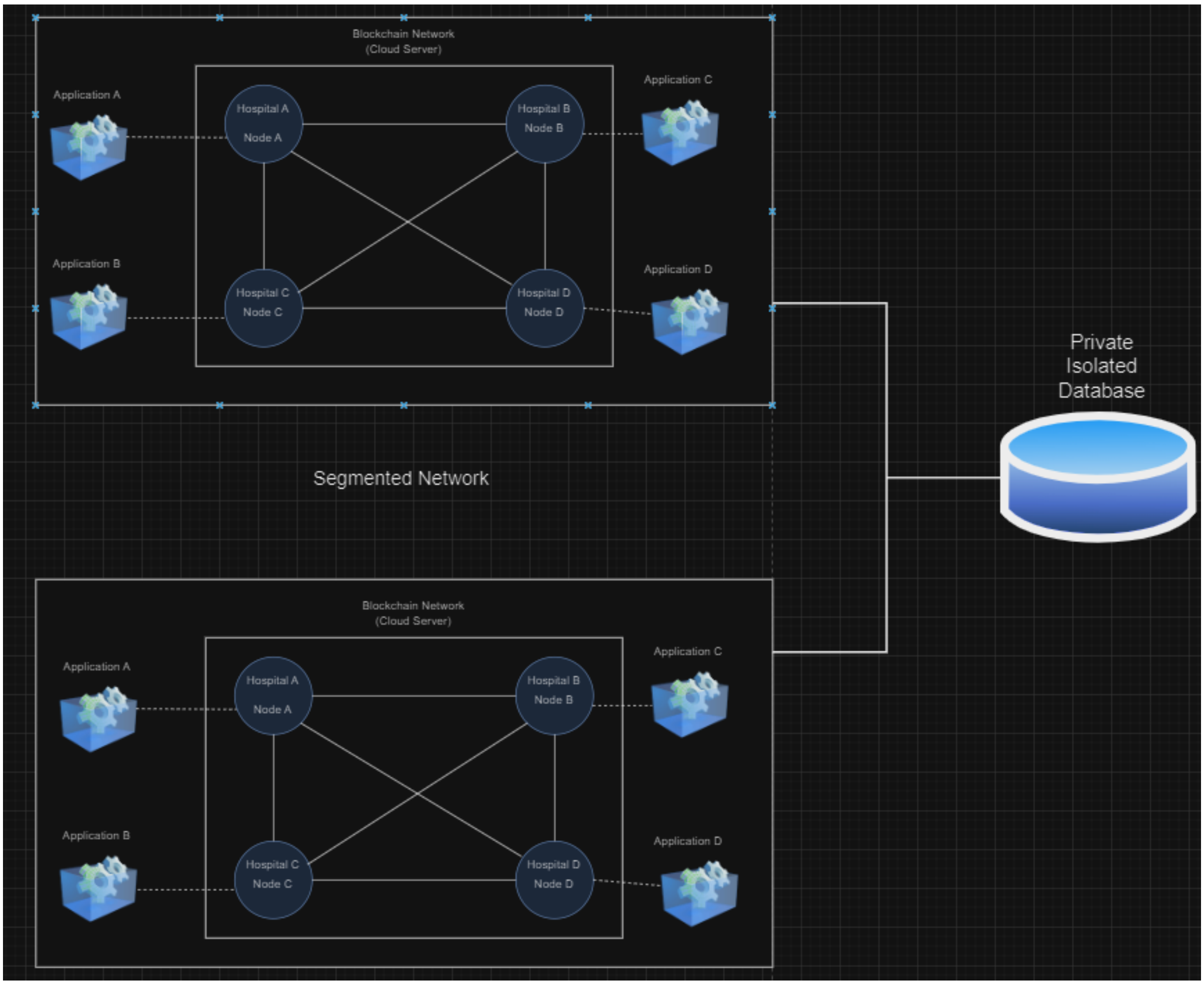

Diagram 1: Blockchain architecture in Cloud

Applications to use:

- Platforms: Hyperledger fabric (LINUX)
- Database: LevelDB/CouchDB/MangoDB
- Applications: Node.js

Objectives

The main objective of this project is to develop a **blockchain-based system** utilizing **Hyperledger Fabric** that integrates a **Mobile Ad-Hoc Network (MANET)** architecture. This system should offer:

1. **Decentralized Data Management**: The application will enable secure, decentralized data storage and sharing among healthcare providers or participants in a permissioned network.
2. **Mobile Ad-Hoc Network (MANET) Integration**: Using MANET allows for dynamic, flexible connections between nodes, especially useful in environments with mobile or constantly changing network infrastructure.
3. **Data Backup & Resilience**: Each blockchain segment will be backed up by isolated physical servers, providing redundancy and ensuring that sensitive information remains secure and retrievable in case of network issues.
4. **Security & Privacy**: By using Hyperledger Fabric, the system aims to maintain strict control over who can access, modify, or store data within the blockchain. Permissioned nodes ensure authorized access only.
5. **Real-Time Data Interaction**: Users can interact with the system through a Node.js-based application to perform transactions, query records, or manage data, providing a real-time experience with decentralized infrastructure.

Challenges

Blockchain Synchronization Across Segments:

- Keeping the blockchain in sync across nodes in different MANET groups can be difficult, particularly when nodes are temporarily disconnected or isolated. Network partitioning or latency in MANET environments could lead to delays in consensus and data replication across nodes.

MANET Implementation and Stability:

- MANETs are known for their dynamic and flexible routing, but ensuring stable communication between the blockchain nodes may be challenging due to high mobility, frequent topology changes, and network partitioning. This can lead to issues like latency, packet loss, and decreased overall network performance.

Data Security and Privacy:

- While Hyperledger Fabric supports permissioned access, ensuring the highest level of encryption and data privacy in a dynamic network like MANET is crucial. The isolated databases need to maintain a high-security level to avoid breaches and data loss

Database Integration and Consistency:

- Each segmented network will have its own isolated database for backup. Ensuring data consistency between these isolated backups and the live blockchain data in real-time can be challenging, especially when dealing with temporary disconnections or conflicts

Scalability:

- As the network grows, scaling the number of nodes within each MANET group and the overall system while maintaining efficient communication and transaction speed can become problematic. This will require optimizing the network's performance and blockchain storage efficiently.