Faculty of Technology

University of Sri Jayewardenepura

ITS 4202

Emerging Technologies

Assignment 1

Name: G.S. Chamika

Index Number: ICT/20/818

Question 1

a) How blockchain and deep learning can work together to improve data security.

Blockchain and deep learning can collaborate to enhance data security in various ways. The article presents a strong combination of blockchain and deep learning for securing healthcare records in Industrial Cyber-Physical Systems (ICPS).

- How blockchain improves data security

Blockchain ensures immutable and decentralized data storage. It enables secure sharing of patient data across IoT devices by validating each transaction using advanced hashing algorithms. This method reduces the risk of unauthorized data access or tampering. In this article, the Pattern-Proof Malware Validation (PoPMV) algorithm is introduced, leveraging blockchain's capability to detect and mitigate cyber-attacks at runtime, even for unknown malware.

- How deep learning improves data security

Some deep learning models like Long Short-Term Memory (LSTM) are utilized for detecting malware patterns and validating workflows. LSTM effectively identifies both known and unknown malware attacks by analyzing sequences and behaviors in real-time. Another method like Reinforcement learning in blockchain network enables adaptive responses to threats by learning from feedback and optimizing the security process.

b) Practical challenges the hospital might face when implementing this solution.

- Many hospitals still rely on outdated systems (Legacy Systems) therefore, it may require significant infrastructure upgrades. Ensuring interoperability across different IoT devices and systems can be challenging.
- In blockchain validation processes, especially with PoPMV, can introduce latency due to high computational demands. And deep learning models like LSTM require more processing power and memory.
- When handling sensitive patient data with decentralized systems raises concerns about compliance with privacy regulations (Government rules and regulations).

- Implementing blockchain and deep learning technologies involves significant initial investment in hardware, software, and training.
- When patient and device numbers grow, the system might face challenges in maintaining performance without scaling resources.
- While blockchain is secure, IoT devices remain vulnerable to cyberattacks, creating weak entry points for malicious actors.

c) Convincing the hospital's management of the long-term benefits of this approach.

- The integration of blockchain and deep learning ensures a robust defense against cyberattacks, reducing risks of data breaches and improving data security.
- User satisfaction: Blockchain's transparency and immutability align with regulatory requirements, fostering trust among patients and stakeholders.
- We can automate administrative tasks like scheduling, billing etc. Automation of data validation and malware detection minimizes manual intervention, saving time and resources.
- While initial costs are high, long-term savings come from reduced data breaches, improved efficiency, and lower system downtime. It saves cost.
- Blockchain's ability to securely share data across systems promotes collaboration between different healthcare entities, enhancing patient care quality and data interoperability.

Question 2

a) How federated learning and blockchain can address the need for secure and efficient data transmission in healthcare IoT.

The article presents the Blockchain-enabled Federated Learning (BFL-hIoT) model, specifically designed to enhance security and privacy in healthcare IoT networks. This model integrates the advantages of federated learning and blockchain to address security and privacy concerns in data transmission.

- Federated learning: Data remains decentralized, ensuring that sensitive patient information is not stored in a centralized server. Each IoT device trains a local model on its data and only shares model updates with the central server. The Federated learning approach maintains patient data privacy while still leveraging collective insights from multiple devices to improve the global model.
- Blockchain: This approach stores encrypted data and model updates, ensuring secure and immutable transactions. Consensus mechanisms (Proof of Work or Proof of Stake) related to the article ensure the integrity of the data and prevent tampering.

b) Two risks associated with using IoT devices in healthcare and how the proposed model minimizes these risks.

1. IoT devices often transmit sensitive patient information, making them targets for cyberattacks and unauthorized access.

How minimizes the risk: Data encryption ensures that patient information remains secure during transmission. Blockchain's immutable ledger prevents tampering, and smart contracts control access, ensuring only authorized entities can retrieve data.

2. Centralized data storage creates a single point of failure, increasing the risk of large-scale privacy breaches.

How minimizes the risk: Federated learning eliminates the need to centralize data by keeping it on local devices, reducing exposure to privacy risks. Blockchain ensures data integrity and secure communication of model updates, minimizing the chance of interception or misuse.

c) Additional features to make the system more user-friendly and secure.

User-friendly features

- Introduce dashboards for healthcare providers to monitor the performance and insights of IoT devices in real-time.
- Develop user-friendly and simple UI designs.
- Develop a mobile application for easier interaction.
- Introduce a feature to notify users or administrators of anomalies detected by the federated model.

Security features

- Require multiple authentication steps for accessing data or interacting with the blockchain.
- Integrate AI models for detecting and responding to unauthorized access attempts or unusual patterns in data usage.
- Integrate AI models for detecting malware attacks.
- Allow computations on encrypted data without decryption, further safeguarding sensitive information.
- Use Zero-Knowledge Proofs (ZKP) to validate transactions without revealing sensitive information.

Question 3

a) Three key challenges the startup might face and suggestions to overcome them.

1. Scalability

Blockchain systems often face limitations in throughput and latency, especially with a high volume of healthcare transactions.

Solution: Implement lightning network or Ethereum plasma, to handle transactions off-chain and only store final states on the blockchain. And employ sharding techniques, as seen in Zilliqa and Ethereum 2.0, to divide the workload across multiple nodes.

2. Interoperability

Existing healthcare systems and IoMT devices may not integrate smoothly with blockchain platforms due to differences in standards and data formats.

Solution: Use frameworks like Health Level 7 (HL7) for healthcare interoperability. And develop APIs and middleware solutions to bridge traditional systems with blockchain networks.

3. Regulatory compliance

Blockchain systems must align with strict healthcare regulations such as HIPAA, which require stringent data protection and user privacy.

Solution: Incorporate smart contracts that enforce access control and ensure compliance. And leverage some patient-centric models (MediBloc), where patients control data sharing permissions, to align with privacy laws.

b) How governments or healthcare organizations could support startups in adopting blockchain technologies.

- Provide financial and technical assistance (Give bank loans and technical knowledge).
- Offer resources such as cloud infrastructure and servers to test their technologies.
- Develop clear guidelines and standards for blockchain implementation in healthcare to reduce legal uncertainties.
- Conduct workshops and provide educational training on blockchain for healthcare providers and startups.
- Share organization's expertise knowledge with startups.
- Introducing new blockchain technologies.
- Encourage collaboration between startups, established healthcare providers, and blockchain developers to accelerate innovation and adoption.

c) Reflecting on a case study from the article and how it addresses these challenges.

1. Scalability

MedRec uses a hybrid storage model where only metadata is stored on the blockchain, while actual data remains in local databases. This reduces the blockchain's storage burden and enhances scalability.

2. Interoperability

MedRec employs modular APIs to integrate seamlessly with existing Electronic Health Record (EHR) systems, ensuring compatibility with diverse healthcare infrastructures.

3. Regulatory Compliance

The system incorporates smart contracts to manage access permissions, ensuring data privacy and adherence to healthcare regulations like HIPAA.

Question 4

a) How blockchain can be used for a digital health passport.

The article explains the use of blockchain to create a secure, decentralized platform for managing COVID-19 vaccination and immunity certificates.

- Use decentralized storage systems like the InterPlanetary File System (IPFS) to ensure data security and accessibility.
- Use Ethereum blockchain automate processes for validating vaccination records, updating immunity status, and granting access to specific entities.
- Blockchain ensures records cannot be tampered with, providing a transparent and trustworthy system for stakeholders, including governments, healthcare providers, and patients.
- Patients control their own data through SSI frameworks, deciding who can access their digital health passports, thus preserving privacy.
- Blockchain enables secure sharing and verification of vaccination certificates globally, aiding in streamlined travel and access control during the pandemic.
- Data is encrypted before being uploaded to IPFS, and access keys are managed through smart contracts, ensuring only authorized users can view sensitive information.

b) Ethical and privacy concerns associated with digital health passports and solutions.

Ethical and privacy concerns

- Digital health passports may reveal sensitive personal and health information, leading to potential misuse.
- Unequal access to vaccines and immunity certificates could marginalize certain populations, creating ethical dilemmas.
- Centralized or poorly secured systems risk exposing patient data to hackers.
- Users may not fully understand how their data will be used, stored, or shared by health passport systems.

Solutions

- Employ SSI frameworks, allowing users to control data sharing and access permissions.
- Use advanced cryptographic techniques and decentralized storage (IPFS) to prevent unauthorized access.
- Align the system with global data protection laws like HIPAA to ensure ethical handling of data.
- Ensure equal access to digital health passports by offering alternative methods for communities with limited digital infrastructure.
- Ensure transparency through user-friendly privacy policies and clear consent processes, explaining data usage in simple terms.

c) Features for a user-friendly and secure interface for the digital health passport.

For ensure usability

- A simple and visually clear dashboard showing vaccination and immunity status.
- Accommodate users across different regions with diverse language preferences.
- Display the latest vaccination and immunity status.
- Ensure the app works on different devices
- Generate scannable QR codes for instant verification by authorities or healthcare centers.
- Provide a secure and lightweight mobile application for convenient and easy access.

For ensure security

- Use fingerprint or facial recognition for accessing the passport.
- Ensure all data exchanges are encrypted to prevent eavesdropping.
- Restrict access to sensitive data based on user roles.
- Leverage blockchain immutability to ensure data integrity and authenticity.