Literature Review on the Integration of Blockchain with Federated Learning (FL) and Homomorphic Encryption (HE) for Credit Card Fraud Detection

Shreyas Vivek
School of Information Technology
Deakin University
Waurn Ponds, VIC, Australia
vivekshreyas01@gmail.com

Literature Review on the Integration of Blockchain with FL and HE

Introduction

The integration of blockchain technology with Federated Learning (FL) and Homomorphic Encryption (HE) aims to enhance the security, privacy, and efficiency of data processing systems, particularly in sensitive applications like credit card fraud detection. FL allows multiple institutions to collaboratively train models without sharing raw data, while HE ensures computations can be performed on encrypted data. Blockchain provides an immutable ledger for secure and transparent data handling.

Key Research Contributions

1. **Efficiency of Federated Learning and Blockchain in Enhancing Credit Card Fraud Detection (CCFD) Systems [1]**

   - **Summary**: This paper explores FL and blockchain integration to enhance CCFD systems. Blockchain ensures data integrity, while FL enables decentralized model training without centralized data storage.

   - **Key Findings**: Improved detection accuracy, enhanced data privacy, and decentralized training.

   - **Challenges**: Real-time performance and scalability.

2. **Blockchain-Based Federated Learning with Homomorphic Encryption and Reputation [2]**

   - **Summary**: This paper examines integrating blockchain with FL using HE and reputation mechanisms to enhance privacy and security in CCF detection.

   - **Key Findings**: Enhanced privacy, secure data processing, reputation-based trust.

   - **Challenges**: Computational complexity, scalability issues.

3. **Secure Data Sharing in Federated Learning through Blockchain-Based Aggregation [3]**

    - **Summary**: This paper discusses using blockchain for secure data aggregation in FL, ensuring data integrity and traceability in CCF detection.

    - **Key Findings**: Secure data aggregation, data integrity, traceability.

    - **Challenges**: Scalability and low-latency communication.

4. **A Privacy-preserving Federated Learning Framework for Blockchain Networks [4]**

    - **Summary**: This framework leverages blockchain to enhance the privacy and security of FL systems in financial applications.

    - **Key Findings**: Enhanced privacy, secure data sharing, use of smart contracts.

    - **Challenges**: Efficient consensus and computational costs.

5. **FL Model Development Using Flower Framework [5]**

    - **Summary**: This research introduces a CCF detection system that integrates FL with blockchain technology using the Flower framework. This framework ensures privacy preservation and data protection while enhancing classification performance and prediction accuracy.

    - **Key Findings**: The Flower framework enables easy integration of FL and blockchain, facilitating efficient and secure model training.

    - **Challenges**: Implementation complexity and managing computational resources.

Integration Analysis

Blockchain can enhance FL and HE integration by providing a secure, immutable ledger for recording and verifying model updates. This integration ensures data integrity and transparency while maintaining privacy through HE. Key mechanisms include:

- **Secure Model Updates**: Blockchain ensures that each model update is verified and immutable.

- **Decentralized Control**: Blockchain reduces the risk of data breaches by eliminating the need for a central authority.

- **Privacy-Preserving Computations**: HE allows computations on encrypted data, ensuring privacy during the processing phase.

- **Secure Data Aggregation**: Blockchain can securely aggregate model updates without exposing raw data.

Potential Use Cases and Implementation

1. **Credit Card Fraud Detection**
    - **Encrypt Transaction Data**: Use HE to encrypt transaction data and analyze it for fraud detection.
    - **Real-Time Fraud Detection**: Train models on encrypted data to perform real-time fraud detection.
2. **Secure Data Sharing**
    - **Collaborative Model Training**: Use FL to allow banks to collaboratively train models while keeping data decentralized.
    - **Secure Aggregation**: Implement secure aggregation to ensure privacy during the model update process.
3. **Blockchain Integration**
    - **Enhancing Security and Transparency**: Research how blockchain can work with HE and FL to enhance security and transparency.
    - **Secure Transaction Logging and Auditing**: Use blockchain for secure transaction logging and auditing.

Application Examples

1. **Credit Card Fraud Detection Systems**:
    - **Integration**: Combining FL with blockchain and HE enhances performance and privacy by enabling decentralized training without data centralization.
    - **Outcomes**: Improved detection accuracy, enhanced data privacy, reduced breach risks.
2. **Suspicious Person List Management**:
    - **Integration**: Using FL to collaboratively update and manage a suspicious person list while maintaining data privacy through HE and ensuring transparency with blockchain.
    - **Outcomes**: Secure and accurate list management, transparent updates, enhanced privacy.

Evaluation of Benefits

1. **Security**:
    - **Data Integrity**: Blockchain ensures immutable records and secure consensus mechanisms.
    - **Privacy**: HE and FL provide robust privacy-preserving mechanisms, keeping raw data encrypted and local.
2. **Transparency**:
    - **Audit Trails**: Blockchain offers transparent, traceable audit trails for compliance and trust.
3. **Efficiency**:
    - **Decentralized Processing**: FL improves efficiency and reduces breach risks by avoiding data centralization.
    - **Computational Overhead**: Advances in optimization can mitigate blockchain and HE's computational demands.

Conclusion

Integrating blockchain with FL and HE significantly enhances the security, privacy, and efficiency of credit card fraud detection systems. This integration provides a robust framework for secure data sharing and processing, essential for maintaining the integrity and privacy of sensitive financial data. Ongoing research and development are necessary to address computational, scalability, and regulatory challenges to fully realize the potential of these technologies in financial applications.

References

[1] Efficiency of Federated Learning and Blockchain in Enhancing Credit Card Fraud Detection (CCFD) Systems. (2023).

[2] Blockchain-Based Federated Learning with Enhanced Privacy and Security Using Homomorphic Encryption and Reputation. (2023).

[3] Secure Data Sharing in Federated Learning through Blockchain-Based Aggregation. (2023).

[4] A Privacy-preserving Federated Learning Framework for Blockchain Networks. (2023).

[5] FL Model Development Using Flower Framework. (2023).

[6] ChatGPT. (2024, August). Generated ideas for the introduction of a paper on blockchain technology. OpenAI. Accessed on 07 August 2024.