Application of Homomorphic Encryption for Financial Services

Students:

- Trần Hữu Đức - 23523021
- Võ Minh An - 23520033
- Nguyễn Gia Bảo - 23520122

Lecturer: Nguyễn Ngọc Tự

Goals

The primary objectives of this proposal are to enhance data privacy and security in financial services while enabling critical financial computations on encrypted data. The specific goals include:

1. **Secure Financial Analytics:** Enable banks and financial institutions to perform computations on encrypted financial data without decrypting it, ensuring data privacy while deriving valuable insights.
2. **Privacy-Preserving Credit Scoring:** Allow credit agencies to compute credit scores using encrypted financial data, eliminating the need to access raw, sensitive information.
3. **Encrypted Financial Transactions:** Securely process financial transactions on encrypted data, ensuring that transaction details remain confidential throughout the process.
4. **Regulatory Compliance:** Ensure compliance with data protection regulations such as GDPR and CCPA by maintaining data privacy during financial computations.

Proposed Solutions

To address the limitations of traditional encryption methods—which require decryption before computation, exposing sensitive financial data—this proposal leverages homomorphic encryption (HE). The proposed solutions include:

1. **Encryption Module:** Encrypt financial data using homomorphic encryption techniques (FHE or SHE), enabling computations without decryption.
2. **Computation Module:** Perform necessary financial operations (e.g., analytics, credit scoring, transaction processing) directly on the encrypted data using selected cryptographic libraries.
3. **Hybrid Encryption for Performance Optimization:**

   While Fully Homomorphic Encryption (FHE) offers strong privacy guarantees, it often suffers from high computational costs. To address this:

   - Combine symmetric encryption (e.g., AES) with HE: Use symmetric encryption for bulk data and apply HE only on sensitive fields that require computation.

- This hybrid model ensures both efficiency and privacy, making it more feasible for real-world financial systems.

4. **Solution Details:**
   - **Algorithm Choice:** Use Fully Homomorphic Encryption (FHE) for general computations or Somewhat Homomorphic Encryption (SHE) for efficiency in specific operations.
   - **Adapted Algorithms:** Modify or design financial computation algorithms to be compatible with encrypted data formats.
   - **Cryptographic Libraries:** Implement using libraries such as:
     - Microsoft SEAL
     - IBM HELib
     - OpenFHE (PALISADE successor)

Outline Deployment

The deployment strategy integrates homomorphic encryption into existing financial systems, with rigorous testing to ensure functionality and security. The steps include:

1. **System Integration:**
   - Incorporate homomorphic encryption into financial analytics platforms, credit scoring systems, and transaction processing frameworks using cryptographic libraries like HElib or Microsoft's SEAL.
2. **Functional Testing:**
   - Simulate real-world financial scenarios (e.g., analytics, credit scoring, transactions) to verify that computations on encrypted data match those on raw data in accuracy and consistency.
3. **Security Testing:**
   - Conduct comprehensive assessments to identify and mitigate vulnerabilities, ensuring data confidentiality and integrity during computations.
4. **Deployment in Practice:**
   - Deploy the solution within financial institutions' analytics platforms and integrate it into credit scoring systems, enabling secure computations without accessing raw data.

References

[1] Bidve, P., et al. (2024). Secure Financial Application Using Homomorphic Encryption. International Journal of Electrical and Computer Engineering Systems, 38(1), 595–602.

[2] Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. International Journal of Science and Research Archive, 12(1), 2942–2949.

[3] Nugent, D. (2022). Privacy-Preserving Credit Card Fraud Detection Using Homomorphic Encryption.

[4] Effendi, F., & Chattopadhyay, A. (2022). Privacy-Preserving Graph-Based Machine Learning with Fully Homomorphic Encryption for Collaborative Anti-Money Laundering. In Privacy and Identity Management. Data for Better Living: AI and Privacy (pp. 45–60).

[5] Landau, J.-P., et al. (2020). Innovative Financial Designs Utilizing Homomorphic Encryption and Multi-Party Computation. MIT Economics
[6] Ramani, A. (2021). Security Enhanced E-Banking Log Management Using Homomorphic Encryption. In Proceedings of the 2021 International Conference on Advances in Computing, Communication, and Control (pp. 123–130). IEEE.
[7] Alabdulatif, A., et al. (2020). A Survey on Fully Homomorphic Encryption: Theory and Applications. IEEE Access, 8, 1–29.
[8] Gong, Y., Chang, X., Mišić, J., Mišić, V.B., Wang, J., & Zhu, H. (2021). Practical Solutions in Fully Homomorphic Encryption: A Survey Analyzing Existing Acceleration Methods. Journal of Cryptographic Engineering, 11(3), 255–272.
[9] Sen, J. (2019). Homomorphic Encryption: Theory & Application. Computer Science Review, 33, 1–15.
[10] Shara, J. (2020). A Survey on Fully Homomorphic Encryption and Its Applications
[11] IBM Research & Banco Bradesco SA. (2019). Towards a Homomorphic Machine Learning Big Data Pipeline for the Financial Services Sector.
[12] Tebaa, M., Zkik, K., & El Hajji, S. (2014). Hybrid Homomorphic Encryption Method for Protecting the Privacy of Banking Data in the Cloud. Procedia Computer Science, 32, 489–496.
[13] Bain, S. (2024). Banks Can Tackle Financial Fraud by Using New Homomorphic Encryption Technology. Financial IT.
[14] Westley, A. (2024). Homomorphic Encryption in Action: From Theory to Practical Implementation. Medium.
[15] Rousseau, S. (2024). Fully Homomorphic Encryption (FHE) in a Banking Quantum Era. Personal Blog.
[16] Jorge Myszne. (2025). Three Homomorphic Encryption Trends for 2025. The Daily Hodl.
[17] Cem Dilmegani. (2025). What is Homomorphic Encryption? Benefits & Challenges. AIMultiple.
[18] James Lloyd. (2022). Homomorphic Encryption: The Future of Secure Data Sharing in Finance? The Alan Turing Institute Blog.
[19] The Alan Turing Institute. (2023). Research Associate in Homomorphic Encryption for Digital Identity. The Alan Turing Institute.