Literature Review about HE in Credit Card Fraud Detection and Suspicious Persons Lists

Homomorphic Encryption (HE) is a form of encryption that permits operations on ciphertexts, generating an encrypted result that, when decrypted, matches the result of operations performed on the plaintext. This property is especially beneficial in scenarios where data privacy and security are paramount. This capability holds significant promise for privacy-preserving data analytics, especially in sensitive domains such as credit card fraud detection and the management of suspicious persons lists.

This review explores recent literature on the application of HE in these areas, evaluating its effectiveness, challenges, and future directions.

Homomorphic Encryption in Credit Card Fraud Detection

Credit card fraud detection involves analysing vast amounts of transaction data to identify patterns indicative of fraudulent activity. Traditional methods rely on plaintext data which raises significant privacy concerns. HE offers a solution by allowing institutions to perform complex analyses on encrypted transaction data without exposing sensitive information.

Key Research Contributions:

- Nugent (2022) dives into the application and techniques of HE in detecting credit card fraud by using encrypted transaction data to train machine learning models. Testing across different models was undertaken and the detection results varied greatly. These included using the ULB Dataset (89% fraudulent transactions correctly identified) which was far more accurate in comparison to using the Vesta Dataset (47% fraudulent transactions correctly identified). Even with such a swing in results, it still showed that HE-enabled models achieved comparable accuracy to those using plaintext data, while preserving data privacy.

Challenges and Limitations:

- The practical implementation of HE in fraud detection is not without challenges. As highlighted by Acar et al. (2017), the computational complexity of FHE operations remains a significant hurdle. They proposed several optimization techniques, such as approximate computing (utilizing smaller, less accurate approximate functions, instead of exact ones) and batching (grouping tasks together, so you do them all at once, instead of switching between tasks that take place in different programs or areas) to mitigate the performance impacts of HE and the current high computational costs.

Homomorphic Encryption and Suspicious Persons Lists

Managing lists of suspicious persons, such as those flagged by security agencies or financial institutions, requires handling sensitive personal information. Homomorphic encryption can enhance the privacy and security of these lists by enabling encrypted data searches and comparisons.

Key Research Contributions:

- Iezzi (2020) explores the development of HE and privacy-preserving search algorithms for suspicious persons lists/fraud within banks. The study went into depth about what methods, libraries and tools are available and how HE could effectively protect privacy while still allowing for accurate and efficient searches.

Challenges and Limitations:

- Despite advancements, challenges remain in deploying HE for managing suspicious persons lists. Issues such as data interoperability and integration with existing systems as can complicate the practical implementation of HE. Additionally, the need for ongoing research to improve the efficiency and scalability of HE systems is crucial for addressing these challenges.

Conclusion

Homomorphic encryption offers promising advancements in privacy-preserving data analysis for credit card fraud detection and managing suspicious persons lists. While the technology has demonstrated potential in maintaining data privacy and security, practical implementation challenges, such as computational overhead and system integration, need to be addressed. Future research should focus on optimizing HE algorithms, enhancing system efficiency, and developing practical frameworks for integrating HE into existing security infrastructures.