Paper Title:
An Accelerated Method for Protecting Data Privacy in Financial Scenarios Based on Linear Operation

Papre Link:
https://www.mdpi.com/2076-3417/13/3/1764

1 Summary

1.1 Motivation

The paper aims to address the dilemma of data privacy and cloud computing in financial scenarios, where massive and sensitive financial data need to be processed efficiently and securely.

1.2 Contribution

The paper proposes a privacy protection model based on cloud computing that can provide four levels of protection according to the users' needs and can accelerate linear operations using GPUs.

1.3 Methodology

The paper uses a scalar-based encryption and decryption scheme to protect the raw data and the user identity, and uses the Freivalds algorithm to verify the intermediate results computed by the cloud server. The paper also designs a multi-user scheduling model to deploy the method in a real scenario.

1.4 Conclusion

The paper shows that the method can improve the speed by 10 times compared to the local computing or the homomorphic encryption, and can effectively prevent the user's privacy from being leaked with minimal delay cost.

2 Limitations

2.1 First Limitation

Assumption of linear operations: The paper assumes that most of the financial algorithms and models are based on linear operations, which may not be true for

some complex and nonlinear scenarios. The paper also does not consider the impact of the encryption and decryption scheme on the accuracy and robustness of the models.

2.2 Second Assumption

Communication overhead: The paper admits that the method has some communication overhead due to the encryption and decryption process, the validation of intermediate results, and the transmission of data between the client and the server. The paper also does not address the potential security risks of data transmission and storage in the cloud environment.

3 Synthesis

The paper discusses the potential of cloud computing in enhancing data privacy in the financial sector, highlighting the dual role of big data and fintech innovations. It also outlines future improvements, including developing more efficient encryption algorithms, reducing communication overhead, and tailoring the method to various financial scenarios and models.