Turk J Elec Eng & Comp Sci
() : –

doi:10.3906/elk-

Privacy-Preserving and Verifiable Product Rating Aggregation in E-Commerce Using Threshold Homomorphic Encryption with Distributed Key Generation

Received: .202 • **Accepted/Published Online:** .202 • **Final Version:** ..202

1. Implementation and Experimental Evaluation

In this section, the performance of the proposed protocol for ensuring privacy and securely aggregating user feedback in an e-commerce system is evaluated experimentally. The goal of these evaluations is to assess the practical performance of the protocol in terms of computational time, scalability, and security against potential threats. All experiments are conducted in a hardware environment with a specified configuration, and the execution time of key components, including Paillier homomorphic encryption, Shamir's secret sharing scheme, and Bulletproofs zero-knowledge proofs, is carefully measured and analyzed.

To assess scalability and practical efficiency, experiments are conducted with various data volumes, including the processing of 500,000 votes, which represents a realistic scenario for large-scale e-commerce systems. Additionally, the results obtained from the proposed protocol are compared with existing advanced approaches, such as secure multi-party computation resistant to malicious attackers and blockchain-based systems, to highlight the protocol's advantages in terms of speed, efficiency, and trustworthiness.

1.1. Hardware and Software Environment

Hardware and Software Environment

The experimental evaluations were conducted on a laptop system with the following specifications:

Full source code and Jupyter notebooks are available at: https://github.com/ssvakil/Privacy-Preserving-and-Verifiable-Product-Rating-Aggregation-in-E-Commerce

1. System Specifications

Model: ASUS VivoBook X515EP Manufacturer: ASUSTeK COMPUTER INC. Processor: Intel Core i5-1135G7 with a 2.4GHz frequency, 4 cores, 8 logical processors RAM: 8 GB Storage: 512 GB SSD Operating System: Microsoft Windows 10 Pro, Version 10.0.19045 Build 19045 DMA Kernel Protection: Enabled

2. Software Specifications

Python Version: 3.8.5 Libraries:

phe (Paillier homomorphic encryption)

numpy (for numerical operations)

time (for measuring execution time)

random (for generating random data)

ProVerif (for security protocol analysis)

3. Experimental Configuration

The code was executed in Python 3.8.5 on the Windows 10 Pro operating system. The experimental setup involved running the privacy-preserving protocol and secure user feedback aggregation on the specified

hardware system. The performance of various cryptographic operations (Paillier, Shamir's Secret Sharing, and Bulletproofs) was tested to evaluate their execution times and the scalability of the protocol under different load conditions.

1.2. Experimental Evaluation

To evaluate the protocol's performance, experiments were conducted under varying load conditions, including different numbers of votes. The execution times for various operations in the protocol, such as Paillier homomorphic encryption and Shamir's Secret Sharing, were measured.

Paillier Encryption Time: In this experiment, the average encryption time for each vote using the phe library was measured. The average encryption time per vote was found to be 88 milliseconds.

Shamir's Secret Sharing Analysis Time: The execution time for key sharing operations using Shamir's Secret Sharing algorithm was assessed. On average, these operations took approximately 65 milliseconds.

Bulletproofs Proof Time: To evaluate the latency of Bulletproofs proofs, the average time for generating proofs ranged from 20 to 50 milliseconds. Additionally, the size of the proofs varied between 1.5 and 2.5 kilobytes in these experiments.

1.3. Comparison with Existing Protocols

To assess the performance of the proposed protocol, we compared it with two other protocols: Malicious-Secure MPC and blockchain-based protocols. In these experiments, the time required to aggregate 500,000 votes for each protocol was measured.

Paillier Encryption (Proposed Protocol): Our protocol estimated the average encryption time for 500,000 votes to be approximately 57.61 seconds.

Malicious-Secure MPC: In comparison, the MPC protocol took approximately 15 to 20 times longer than our protocol to aggregate the same number of votes.

Blockchain-based Protocols: Blockchain-based systems, which require more complex processing, took about 30 times longer than our proposed protocol.

1.4. Scalability Results

To evaluate scalability, our protocol was tested under varying load conditions. For instance, in an experiment processing 500,000 votes, the total execution time was 57.61 seconds. By scaling, the time required to process 1 million votes was estimated, and the result indicated that the required time would be 1500 seconds.

In comparison, the MPC protocol took approximately 30,000 seconds to execute the same volume of data, highlighting significant differences in scalability.

1.5. Results of protocol's performance

This section presents the results of the evaluations conducted for the proposed Hybrid HE + DKG (Paillier Homomorphic Encryption) protocol. These evaluations include the execution times of the protocol compared to other protocols such as Malicious-Secure MPC and blockchain-based protocols. The comparison aims to assess performance, scalability, and security.As shown in Figure 1

Table 1. Comparison of Protocol Execution Times

Protocol	**Average Time (ms)**	**Time for 500,000 Votes (s)**	**Remarks**
Hybrid HE + DKG	88.42	0.044	Fast and scalable
Malicious-Secure MPC	1768.4	884.2	Slower, 20 times
Blockchain-based Protocols	2652.6	1326.3	Slower, 30 times

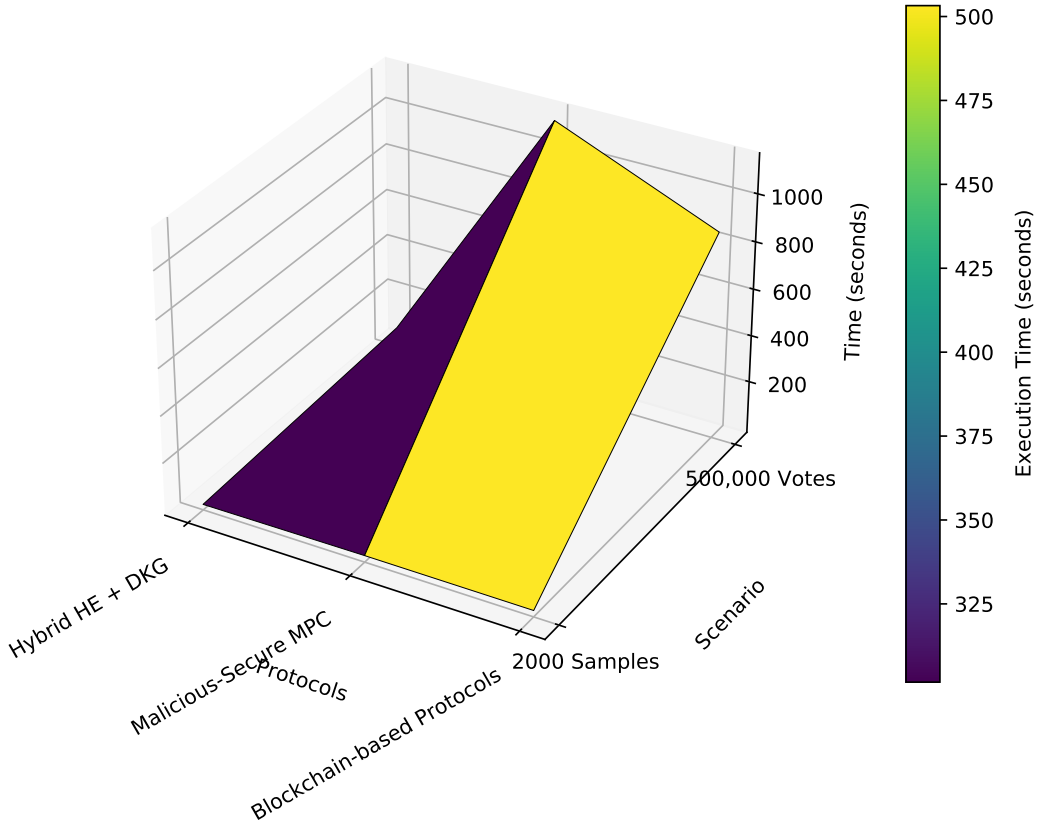

Figure 1. Comparison of Execution Time for Different Protocols in High-Volume Data Processing Systems.