International Journal of Computer Science and Engineering (IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 10, Issue 2, Jul–Dec 2021; 59–72

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

ENHANCED SECURITY IN CLOUD COMPUTING USING SECURE MULTI-PARTY COMPUTATION (SMPC)

Vijaykumar Mamidala

Conga (Apttus), San Ramon, CA, USA

ABSTRACT

A key cryptographic technique that promotes cooperative computing while protecting data privacy is called Secure Multi-Party Computation (SMPC). SMPC stands out as a strong way to improve security in the cloud computing environment without depending on neural networks or conventional encryption techniques. This study explores the algorithms, mathematical underpinnings, and particular performance metrics of SMPC with a focus on cloud environments. The SMPC design entails clients encrypting their data, which is then collected by cloud servers, decrypted from the aggregated result, and averaged. Details are provided for important methods such homomorphic encryption, secure sum calculation, oblivious transfer, and Shamir's Secret Sharing. Highlighted are the secure multiplication using Beaver triples, Lagrange interpolation for data reconstruction, and the homomorphic characteristics of the Paillier cryptosystem. The study shows how several clients can compute the average of their private data securely using a comprehensive secure data aggregation methodology. According to the research, SMPC protocols are effective and safe, which makes them perfect for cloud-based applications where security and privacy of data are critical considerations. This study emphasises how SMPC can be used to protect private information when working together on cloud computing tasks.

KEYWORDS: *Secure Multi-Party Computation (SMPC), Cloud Computing, Homomorphic Encryption, Shamir's Secret Sharing, Oblivious Transfer, Paillier Cryptosystem, Beaver Triples.*

Article History

Received: *06 Aug 2021* | ***Revised:*** *14 Aug 2021* | ***Accepted:*** *19 Aug 2021*