Review on HEROIC Framework: Homomorphically Encrypted One Instruction Computer

Abstract

Outsourcing to cloud brings a new face to computation. In outsourcing, maintenance cost as well as upgrade cost is low to zero. Outsourcing’s features are held back by data privacy concerns. In cloud, privacy of data can be assured by encryption schemes. Common encryption schemes will decrypt the data before processing and re encrypt data after processing, key sharing required. The sensitive data inside the processor are vulnerable to eavesdropping and other attacks. HEROIC Framework (Homomorphically Encrypted One Instruction Computer), a secure architecture for processing data in encrypted form is introduced as a promising solution to the security and privacy concerns. It is single instruction architecture which rules out the need for storing private key inside the processor. In this framework a variant of Paillier encryption scheme is used for homomorphically encrypting both data and instruction.

References

9. HSR Hochschule fr Technik Rapperswil, Homomorphic Tallying with Paillier Cryptosystem, Seminar on e Voting

Index Terms

Computer Science

Information Sciences

Keywords

Outsourcing, Cloud computing, Single instruction architecture