Abstract

Delegating or outsourcing of computation is a prominent feature of cloud computing. It can be made secure through fully homomorphic encryption which allows processing of encrypted data. Verifiability of results is essential where a service-provider cannot be trusted. Since it is mostly used by lightweight devices, so mechanisms are required to verify the results of computations efficiently. In this paper protocols for VDoC are discussed, which focus on verification of aspects of computation other than the results, namely depth and complexity of delegated function which are useful when a user wants to verify amount charged by the service provider. A symmetric-key homomorphic scheme for encryption is being used. The protocols have a real-world relevance and the runtime are small enough for practical feasibility.

References

Verifiable Delegation of Computation through Fully Homomorphic Encryption

- D. Fiore and R. Gennaro. &quot;Publicly verifiable delegation of large polynomials and matrix computations, with applications. &quot;IACR Cryptology ePrint Archive, 2012:281, 2012

- Fangyuan Jin; Yanqin Zhu; Xizhao Luo, &quot;Verifiable Fully Homomorphic Encryption scheme,&quot; Consumer Electronics, Communications and Networks (CECNet), 21-23 April 2012 2nd International Conference Proceedings, pp. 743,746.
- M. Barbosa and P. Farshim. &quot;Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation. &quot;Proceedings of The Cryptographers’aposs; Track at the RSA Conference 2012, San Francisco, CA, USA, February 27 – March 2, 2012. pg 296-312.

Index Terms

Computer Science

Security

Keywords

Homomorphic encryption  symmetric FHE  cloud computing  verifiable delegation of computation  outsourcing computation.