Abstract

The past decade of computing has witnessed a number of new computational models and the most prominent among them is Cloud Computing. Cloud Computing is a paradigm shift that helps a user with internet based computing services that can be accessed from anywhere on any platform. But despite of its advantages, it is yet to gain total trust from users, the primary reason being its security issues. Though some standard organizations have developed a number of security compliance guidelines that need to be followed to ensure security and quality of services in the cloud, security assurance in real terms remains to be undercover. This paper discusses about the two most promising cryptographic techniques, that are, if
implemented correctly can effectively mitigate the security threats and can help in an increased uses of cloud computing.

References

- Peter Mell, Timothy Grance; The NIST Definition of Cloud Computing; NIST Special Publication 800-145, 2011
- Amit Sahai, Brent Waters; &quot;Fuzzy Identity Based Encryption&quot;., Proceedings of Eurocrypt, 2005
- S. Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, Nickolai Zeldovich, Reusable Garbled Circuit and Succinct Functional Encryption, STOC&apos;13, June 1–4, 2013, Palo Alto, California, USA.
- Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully homomorphic
Advanced Cryptographic Techniques for Secured Cloud Computing


Index Terms

Computer Science
Cloud Computing

Keywords

Cloud Computing  Fully Homomorphic Encryption  Functional Encryption