World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:03, 2015

Performance Analysis of Elliptic Curve Cryptography Using Onion Routing to Enhance the Privacy and Anonymity in Grid Computing

Authors : H. Parveen Begam, M. A. Maluk Mohamed

Abstract : Grid computing is an environment that allows sharing and coordinated use of diverse resources in dynamic, heterogeneous and distributed environment using Virtual Organization (VO). Security is a critical issue due to the open nature of the wireless channels in the grid computing which requires three fundamental services: authentication, authorization, and encryption. The privacy and anonymity are considered as an important factor while communicating over publicly spanned network like web. To ensure a high level of security we explored an extension of onion routing, which has been used with dynamic token exchange along with protection of privacy and anonymity of individual identity. To improve the performance of encrypting the layers, the elliptic curve cryptography is used. Compared to traditional cryptosystems like RSA (Rivest-Shamir-Adelman), ECC (Elliptic Curve Cryptosystem) offers equivalent security with smaller key sizes which result in faster computations, lower power consumption, as well as memory and bandwidth savings. This paper presents the estimation of the performance improvements of onion routing using ECC as well as the comparison graph between performance level of RSA and ECC.

Keywords : grid computing, privacy, anonymity, onion routing, ECC, RSA
Conference Title : ICCIT 2015 : International Conference on Computing and Information Technology
Conference Location : London, United Kingdom
Conference Dates : March 14-15, 2015