ABSTRACT

Cloud computing is an architecture for facilitating computing service through the internet on requirement and pay per use access to a group of shared resources namely networks, storage, servers, services and applications, without physically acquiring them Cloud Database management system. Therefore, there is need to secure the data being sent across the architecture. In this project I focus on the security of a Cloud based platform (developed using JavaScript, PHP and all other frameworks by other project colleagues) using Elliptic Curve Cryptography. Elliptic curve cryptography (ECC) is an increasingly popular method for securing many forms of data and communication via public key encryption. The algorithm utilizes key parameters, referred to as the domain parameters. These parameters must adhere to specific characteristics in order to be valid for use in the algorithm. The American National Standards Institute (ANSI), in ANSI X9.62, provides the process for generating and validating these parameters. The National Institute of Standards and Technology (NIST) has identified fifteen sets of parameters; five for prime fields, five for binary fields, and five for Koblitz curves.