Abstract

Ashraf F Tamam

A Novel Approach For Generating One-Time Password With Secure Distribution

Authentication nowadays is an important issue that cannot depend only on static passwords because it is vulnerable and subjected to many types of attacks. Many researchers addressed this problem by introducing a dynamic password framework called a one-time password (OTP). However, this framework still has many limitations. One of these limitations is sending OTP that is done without any encryption. In this paper, we will introduce a new OTP framework that achieves the confidentiality of exchanging the OTP by using a combination of AES-256 bit, RSA, SHA-512. OTP should be delivered to the client in a secure way, as an example is using network traffic to avoid the delay in SMS. In the proposed model the server encrypts OTP using the RSA public-key cryptosystem with the client's public key, in order not to send OTP as a plain text.