

ENHANCEMENT OF ONE TIME PASSWORD

Shashika Boteju

A dissertation submitted in partial fulfillment of the requirements for Bachelor of a

Department of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2020

Abstract

Two-factor authentication is a very common authentication method that is used to secure confidential data. One-time PINs are considered to be an efficient method in securing data but however hackers have figured out ways to bypass this authentication method either using brute-force or hacking of the medium in which the One-time PIN is sent.

The Proposed system provides a secure and reliable one-time PIN generation method. The solution will use techniques such as Steganography and Encryption to secure the one-time PIN methods. The PIN will be generated using TOTP which is considered to be the best algorithm for the generation of a one-time PIN. The PIN will then be encrypted using AES and further hidden using image Steganography techniques.

Testing was conducted on the functional and non-functional requirements and the results were at a satisfactory level. Evaluation was also done by domain-level experts, software engineers, and common end-users. The evaluation results helped in identifying the strengths and weaknesses of the project along with the future enhancements that are required.

Key Words: OTP, Two-Factor authentication, TOTP, Steganography, Encryption