Informatics Institute of Technology

In Collaboration With

University of Westminster, UK

Puzzle Solution

Encryption Algorithm Enhancement

A dissertation by

Mr. G.R.I.S.B.Nishshanka

Supervised by

Mr. Kanishka Yapa

Submitted in partial fulfillment of the requirements for the

MSc Cyber Security and Forensics Masters Department of Computing

July 2021

Abstract

The transmission of the time or location-sensitive data is currently done through getting restricted access. This method is not the best approach for this. The primary purpose of this research is to implement a new way to secure the time and location sensitive data through time lock, geo lock and password lock mechanisms. This system will be focusing on implementing the features to the Advanced Encryption Standard (AES). The best approach for this is, using the time data, password data and location data in the process of key generation. With this newly introduced mechanism, the receiver will not decrypt the ciphertext outside the given time, given password and location.

Adding three layers of unique parameters will provide extra security features to encryption data. For example, Examination, special bank documents and the special of applications could use this extra layer to secure the confidential data. Generated key of the algorithm will only be valid for the given time and given location with the password special API which developed by this project will use own integrated mechanics to get the accurate location and accurate time by connecting to time servers and location satellites and API will internally collect accurate data internally by connecting authorized servers.

Keywords: Encryption, Decryption, Time-Based, Location-Based, AES, Cryptography