A certificateless encryption based on cryptographic concepts to enhance the secure data transfer.

Kurukulasooriya Raveen Lashane Fernando

A dissertation submitted in partial fulfilment of the requirement for
Master of Science degree in Cybersecurity and Forensics

School of Computing
Informatics Institute of Technology, Sri Lanka
in collaboration with
University of Westminster, UK

2023

Abstract

Cybercrime has become one of the major concerns in today business world. Today most of the business systems are looking forward to work with the use of cloud base solutions where due to the business systems available publicly available due to the utilization of cloud services security became a major concern. Therefore, to minimize the security concerns raised when using cloud services, the service providers came up with Encryption as a solution.

In the beginning they performed several research and developments of several models, standards and approaches which had limitations and complexities which allowed cyber criminals to still get hold of the data transferred. After some time, they came to the agreement of using certificate public key cryptography encryption as a solution which to had complexities and limitation when implementing in real world scenarios. On some occasions certificate public key cryptography encryption has proven to be less effective thus changing the research towards certificateless Encryption solutions.

When Certificateless Encryption methods were introduces and followed a problem occurred on how to send the key used to encrypted to the receiver which was known as the key escrow problem. This became one of the major things which became focused when working on a certificateless encryption solution as done by this research.

Lastly with the development of the technology the use of IOT devices which has limited hardware resources has been consumed by many changing the focus to the performance of the encryption solutions used. This is to cater the high demanding usage of IOT. Goal of this research is to provide a conceptual framework on certificateless encryption which will further enhance the ability of using certificateless encryption when performing secure data transfer between business systems and end users.

Keywords: Framework, IOT, Cryptography, Certificate Public Key Cryptographic Encryption, Certificateless Encryption, Encryption, Key Escrow Problem, Cyber Crime, Cyber Security, GDPR.