Enhancing Data Protection and User Verification in Password Management Systems through Integrated Steganography and Cryptographic systems

G.D.M Perera
MS23008250

A THESIS

SUBMITTED TO

SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

IN PARTIAL FULFILMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

December 2024

I certify that I have read this thesis and that in my opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Mr.Amila Nuwan Senarathne- Supervisor

Dr.Nuwan Kuruwitaarachchi –External Supervisor

Approved for MSc. Research Project:

MSc. Programme Co-ordinator, SLIIT

Approved for MSc:

_____

Head of Graduate Studies, FoC, SLIIT

DECLARATION

This is to certify that the work is entirely my own and not that of any other person, unless explicitly acknowledged (including citation of published and unpublished sources). The work has not previously been submitted in any form to the Sri Lanka Institute of Information Technology or to any other institution for assessment for any other purpose.

Sign: ……..

G.D.M Perera

Date: …2024/11/12……

ABSTRACT

Enhancing Data Protection and User Verification in Password Management Systems through Integrated Steganography and Cryptographic systems

Govinnage Dinusha Malshan Perera
MSc. in Information Technology
Supervisor: Mr.Amila Nuwan Senarathne
External Supervisor: Dr.Nuwan Kuruwitaarchchi
December 2024

This research introduces a hybrid authentication system that combines decentralized and centralized security methods, leveraging cryptographic and steganographic techniques to create a secure and user-friendly solution. The system provides users with dual authentication options: a blockchain wallet seed phrase or a novel image-based approach. In registration, a public-private key pair is generated, with the public key stored centrally and private key retrieval enabled through memory-based questions and steganography. The login process offers flexibility, allowing users to either input a seed phrase or answer questions related to an uploaded image. This hybrid model optimizes security by balancing decentralized security with the familiarity of centralized elements, addressing issues like usability, memory retention, and cognitive load. Furthermore, evaluations show that graphical and question-based authentication methods are more intuitive and memorable than traditional passwords, thus reducing recall errors and enhancing security in practical applications. This system provides a significant advancement in secure and adaptable authentication, suitable for various user preferences and ensuring robust data protection.

Key words: *Cryptography, Blockchain Technology, Encryption, Authentication, Security*

ACKNOWLEDGEMENT

While at Sri Lanka Institute Information Technology, I have benefited from having great advisors who seem to agree about very little. Mr.Amila Nuwan Senarathne was a great mentor, providing advice, constant constructive criticism of my ideas and writing, access to his web of contacts and friends, financial support, and the freedom to work on my own projects on his research account's time.

This project could not have been completed without various groups providing financial assistance to fund fieldwork and the inclusion of questions on various surveys in 2024.

Table of Contents

List of Figures

List of Tables