



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entirely my own and not that of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

DECLARATION	iii
ABSTRACT	iv
ACKNOWLEDGEMENT	v
Chapter 1.....	1
1.1 Introduction	1
1.2 Background and Motivation.....	1
1.3 Problem in Brief	3
1.4 Aim and Objectives	4
1.4.1 Aim	4
1.4.2 Objectives.....	4
1.5 Proposed Solution.....	4
1.6 Summary.....	5
Chapter 2.....	6
2.1 Introduction	6
2.2 Related Works	6
2.2.1 Traditional Password-based Authentication Systems	6
2.2.2 Two-Factor and Multi-Factor Authentication (2FA/MFA)	8
2.2.4 Blockchain-Based Decentralized Authentication Systems	10
2.2.5 Transaction Validation Techniques in Public Blockchain	13
2.2.6 Transaction Validation Techniques in Private Blockchain.....	14
2.2.7 Hybrid Authentication Systems (Combining Centralized and Decentralized Approaches).....	15
2.2.6 Comparison Summary of the Selected Authentication Systems.....	16
.....	18
Chapter 3.....	18
3.1 Introduction	18
3.2 Technology Adapted	18
3.2.1 Programming Languages.....	18
3.2.2 Development environment/tools	18
3.2.3 Libraries and Packages.....	19
3.2.5 Version Controlling.....	22

3.3 Summary	22
Chapter 4.....	23
4.1 Introduction	23
4.2 Why Images Are Easier to Remember Than Passwords	23
4.3 Why Security Questions Are Easier to Remember Than Passwords.....	24
4.4 Proposed System.....	25
4.5 Users	26
4.6 Inputs.....	27
4.7 Process.....	27
4.8 Output	30
4.9 Summary	30
Chapter 5.....	31
5.1 Introduction	31
5.2 High-level Service Architecture of the Overall System	31
5.3 Password Based Centralized Authentication	36
5.4 Two Factor/ Multi Factor Authentication	38
5.5 Decentralized Blockchain Authentication	39
5.6 Hybrid Authentication System.....	41
5.7 Summary	43
Chapter 6.....	44
6.1 Introduction	44
6.2 Implemented Code Snippets.....	44
6.3 Implemented User Interfaces for the Proposed System	68
6.4 Summary	74
Chapter 7.....	75
7.1 Introduction	75
7.2 Evaluating the steganography model and private key encryption algorithm	75
7.3 Evaluate ImageHashing Algorithm vs SSIM Algorithm.....	77
7.4 Evaluate SSIM Algorithm by changing the threshold.....	79
7.5 Evaluate Overall System – Feedback Analysis	80
7.6 Summary	84
Chapter 8.....	85
8.1 Conclusion.....	85
8.2 Further Works.....	85
REFERENCES	87

List of Figures

<i>Figure 1 End-to-End Process of the System.....</i>	<i>28</i>
<i>Figure 2 High-Level Architecture of Overall System.....</i>	<i>34</i>
<i>Figure 3 Register a New User.....</i>	<i>35</i>
<i>Figure 4 Login process of a user.....</i>	<i>35</i>
<i>Figure 5: Transaction Operation with asymmetric communication.....</i>	<i>41</i>
<i>Figure 6 Direct Loading API Implementation.....</i>	<i>44</i>
<i>Figure 7Registration API.....</i>	<i>45</i>
<i>Figure 8 Authentication Approach.....</i>	<i>46</i>
<i>Figure 9 Data Encryption.....</i>	<i>47</i>
<i>Figure 10: Environmental Variables.....</i>	<i>48</i>
<i>Figure 11: Smart Contract.....</i>	<i>49</i>
<i>Figure 12Client-side image submission.....</i>	<i>51</i>
<i>Figure 13 Form Submission for Seed Phrase.....</i>	<i>53</i>
<i>Figure 14Image Loading Function.....</i>	<i>54</i>
<i>Figure 15Image Upload Handling Function.....</i>	<i>56</i>
<i>Figure 16 Popup Function.....</i>	<i>57</i>
<i>Figure 17Registering Form Submission.....</i>	<i>58</i>
<i>Figure 18 Defining end-points from the backend.....</i>	<i>60</i>
<i>Figure 19Backend Local Database Structure.....</i>	<i>64</i>
<i>Figure 20JSON object for Security Questions and Answers.....</i>	<i>66</i>
<i>Figure 21 Registering Web Interface.....</i>	<i>68</i>
<i>Figure 22 Uploading section of the favorite image.....</i>	<i>69</i>
<i>Figure 23Direct Login Section with the Seed Phrase.....</i>	<i>70</i>
<i>Figure 24 Direct Login Section with the Seed Phrase.....</i>	<i>71</i>
<i>Figure 25 Login Using Encrypted Image.....</i>	<i>72</i>
<i>Figure 26 Questions that will appear after the login by image.....</i>	<i>73</i>
<i>Figure 27Login Successful Popup.....</i>	<i>74</i>
<i>Figure 28 Evaluating Steganography model.....</i>	<i>75</i>
<i>Figure 29 Evaluating Image Hashing Algorithm.....</i>	<i>77</i>

<i>Figure 30 Evaluation Output</i>	<i>78</i>
<i>Figure 31Evaluating SSIM Algorithm.....</i>	<i>79</i>
<i>Figure 32 Overall Evaluation Bar Chart</i>	<i>81</i>
<i>Figure 33Overall Evaluation Pie Chart.....</i>	<i>83</i>

List of Tables

<i>Table 1</i>	<i>Comparison of Blockchain Integration Approaches</i>	<i>12</i>
<i>Table 2</i>	<i>Comparison Summary of the Selected Authentication Systems</i>	<i>16</i>