Enhancing Cloud File Storage Security through Cryptographic Techniques

K.K.U.M.Hansani
MS23006652

A THESIS
SUBMITTED TO
SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY
IN PARTIAL FULFILLMENT 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 quality, as a thesis for the degree of Master of Science.

Mr.A.N.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work is entirely my own and not of any other person unless explicitly acknowledged (including citation of published and unpublished sources).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: 

…….....

K.K.U.M.Hansani

Date: 10th Sep 2024

……..

ABSTRACT

Enhancing Cloud File Storage Security through Cryptographic Techniques

Kuda Ketiyapege Upeksha Madhu Hansani

MSc. in Information Technology

Supervisor: Mr. Amila Nuwan Senarathne

External Supervisor: Dr.Nuwan Kuruwitaarachchi

December 2024

This project addresses the critical issue of secure cloud storage by developing a system that integrates hybrid cryptography and behavioral biometrics-based two-factor authentication (2FA). As cloud storage is increasingly vulnerable to data breaches and unauthorized access, our research problem focuses on enhancing cloud security through user-adaptive, behavior-based authentication alongside robust encryption.The primary objectives are to (1) secure data through a hybrid cryptographic approach, combining AES for data encryption with RSA for key exchange, and (2) enhance user authentication with behavioral biometrics. Methodologies include local AES encryption of data before cloud upload, ensuring secure access across devices through a web interface. For authentication, machine learning models analyze user-specific interaction patterns, such as mouse movements and scrolling speeds, to develop a behavioral profile for each user. This profile allows the system to detect impersonation attempts effectively. Initial results show a reliable authentication accuracy with a low false rejection rate, balancing security and user experience. Continuous monitoring and regular model updates allow the system to adapt to evolving behaviors, ensuring long-term efficacy. This approach demonstrates a scalable, user-centric solution to cloud storage security, addressing both data protection and adaptive authentication.

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 & Dr.Nuwan Kuruwitaarachchi were great mentors, providing advice, constant constructive criticism of my ideas and writing, access to his web of contacts and friends, and the freedom to work on my own projects on his research time.

Table of Contents

List of Figures

List of Tables