



# **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work is entirely my own and not of any other person unless explicitly acknowledged (including citation of published and unpublished sources).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: 10<sup>th</sup> 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

<b>DECLARATION</b> .....	iii
<b>ABSTRACT</b> .....	iv
<b>ACKNOWLEDGEMENT</b> .....	v
<b>Table of Contents</b> .....	vi
<b>List of Figures</b> .....	viii
<b>List of Tables</b> .....	ix
<b>Chapter 1</b> .....	1
<b>1.1 Introduction</b> .....	1
<b>1.2 Background</b> .....	2
<b>1.3 Research problem</b> .....	2
<b>1.4 Objectives</b> .....	3
<b>1.4.1 Main Objectives</b> .....	3
<b>1.4.2. Specific objectives</b> .....	4
<b>Chapter 2</b> .....	5
<b>2.1 Literature Review</b> .....	5
<b>2.1.1 Cloud Security</b> .....	5
<b>2.1.1.1 Advances Cloud Security Challenges</b> .....	6
<b>2.1.2 Advanced Encryption Standard Algorithm &amp; Rivest Shamir Adleman Algorithm</b> .....	8
<b>2.1.3 Anomaly Detection</b> .....	27
<b>2.2 GAP Identification</b> .....	30
<b>2.2.1 Options for encrypting data stored in the cloud</b> .....	30
<b>2.2.1.1 Cloud storage with zero-knowledge</b> .....	30
<b>2.2.1.2 Cloud Storage Encryption Methodology</b> .....	30
<b>2.2.3 Findings</b> .....	31
<b>2.2.4 Identified Gaps</b> .....	31
<b>2.3 Conceptual framework</b> .....	33
<b>2.4. Research objectives and Hypothesis</b> .....	34
<b>2.4.1 Research Objectives</b> .....	34
<b>2.4.2 Hypothesis</b> .....	35
<b>Chapter 3</b> .....	36

<b>3.1 Research Design.....</b>	<b>36</b>
<b>3.1.2 Proposed System Overview .....</b>	<b>36</b>
<b>3.1.2.1 Encryption System.....</b>	<b>37</b>
<b>3.1.2.2. Anomaly Detection System.....</b>	<b>37</b>
<b>3.1.2.3. System Development .....</b>	<b>39</b>
<b>3.2 Methodology.....</b>	<b>40</b>
<b>3.2.1. Development of the Encryption System .....</b>	<b>41</b>
<b>3.2.2. Implementation of the Anomaly Detection System.....</b>	<b>41</b>
<b>3.2.3. System Development and Integration .....</b>	<b>43</b>
<b>3.3 System Overview .....</b>	<b>44</b>
<b>Chapter 4 .....</b>	<b>56</b>
<b>4.1. Significance and Expected Contributions .....</b>	<b>56</b>
<b>4.1.1 Significance of the Research.....</b>	<b>56</b>
<b>4.1.2 Expected Contributions.....</b>	<b>56</b>
<b>4.2 Justification and Validation of the Proposed Encryption Method.....</b>	<b>57</b>
<b>4.2.1 Justification .....</b>	<b>57</b>
<b>4.2.2 Validation.....</b>	<b>57</b>
<b>4.2.2.1 Testing .....</b>	<b>58</b>
<b>4.3. Ethical Considerations .....</b>	<b>65</b>
<b>4.3.1 Ethical Guidelines .....</b>	<b>65</b>
<b>Chapter 5 .....</b>	<b>67</b>
<b>5.1 Results and analysis .....</b>	<b>67</b>
<b>5.2 Mapping the Results with Research Objectives .....</b>	<b>67</b>
<b>5.2.1 Results for OB1,OB2 &amp; OB3 .....</b>	<b>67</b>
<b>5.2.2 Results for OB 4 .....</b>	<b>70</b>
<b>5.2.3 Results for OB 5 .....</b>	<b>72</b>
<b>5.2.3.1 Performance of File Uploading Across Varying File Sizes.....</b>	<b>72</b>
<b>5.2.3.2 Behavior Detection Efficiency in the System .....</b>	<b>77</b>
<b>5.2.4 User Feedbacks Analysis .....</b>	<b>88</b>
<b>5.3 Conclusion &amp; Future Work .....</b>	<b>89</b>
<b>References .....</b>	<b>91</b>

# List of Figures

Figure 3.1	Flowchart.....	45
Figure 3.2	Usecase Diagram .....	46
Figure 3.3	sequence diagram .....	47
Figure 3.5	app/models.py .....	51
Figure 3.5	routes.py .....	52
Figure 3.6	run.py.....	69
Figure 5.1	AES Key Gereneration.....	69
Figure 5.2	User Logging.....	69
Figure 5.3	Token Generation While Uploading Files.....	70
Figure 5.4	RSA Key Generation.....	71
Figure 5.5	User Behavior Tracking.....	71
Figure 5.6	Track user Activity.....	72
Figure 5.7	Encrypted file in the system.....	73
Figure 5.8	Local database.....	74
Figure 5.9	File Encrypting Speed 1MB - 10 MB.....	74
Figure 5.10	File Encrypting Speed 1MB - 10 MB.....	75
Figure 5.11	File Encrypting Speed upto 10 MB.....	75
Figure 5.12	File Encrypting Speed up to 1000MB.....	75
Figure 5.13	File Encrypting Speed .....	76
Figure 5.14	File Decrypting Speed .....	77
Figure 5.15	Encrypting the AES 256 Key Using RSA Public key .....	77
Figure 5.16	RSA Key Encryption.....	78
Figure 5.17	Start Tracking User Behavior after logging to the system.....	78
Figure 5.18	Suspicious activity Detection & User Locked.....	79
Figure 5.19	User behaviour Detection.....	80
Figure 5.20	User Behavior Tracking Speed .....	80
Figure 5.21	User Mouse movement speed Tracking .....	81
Figure 5.22	User Behavior Tracking Speed .....	81
Figure 5.23	User Behavior Mouse Movement Tracking .....	82
Figure 5.24	User Behavior Mouse Clicks Tracking .....	82
Figure 5.25	Overall system perforamance .....	83
Figure 5.26	Overall system perforamance .....	84
Figure 5.27	AES 256 vs AES 128 .....	84
Figure 5.28	AES used Encrytion systems .....	85
Figure 5.29	Comparison between Different Encrytion systems .....	86
Figure 5.30	Comparison between Different Encrytion systems encrypting speed.....	88
Figure 5.31	User Feedback form.....	89
Figure 5.32	User feedbacks.....	90



## List of Tables

Table 4.1	User logging Testing.....	60
Table 4.2	User registration Testing.....	60
Table 4.3	User registrstion Testing.....	61
Table 4.4	User Token verificationTesting.....	61
Table 4.5	User password reset Testing.....	62
Table 4.6	User password reset Testing.....	62
Table 4.7	User file access Testing.....	63
Table 4.8	User File Uploading Testing.....	63
Table 4.9	User File Encryption Testing.....	64
Table 4.10	User File access Testing.....	64
Table 4.11	User file decryption Testing.....	65
Table 4.12	User file download Testing.....	65
Table 4.13	User file deleting Testing.....	66