



Enhancing OTP Security with Private Blockchain, Geolocation And AI: A Decentralized and Privacy- Preserving Mobile Identity Authentication Framework

G. G. D. SULOCHANA
(MS24016766)

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
(ENTERPRISE APPLICATION DEVELOPMENT)

December 2025

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.



Prof. Dilsham De Silva

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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

G. G .D. SULOCHANA

Date: 25/11/2025

ABSTRACT

Enhancing OTP Security with Private Blockchain, Geolocation and AI: A Decentralized and Privacy-Preserving Mobile Identity Authentication Framework

G. G .D. Sulochana

MSc. in Information Technology (Enterprise Application Development)

Supervisor: Prof. Dilshan De Silva

December 2025

One-Time Password (OTP) authentication is an important tool in protecting online banking, financial services, and online platforms. Nevertheless, the classical OTP systems, which are often based on centralized provision of SMS or email, are becoming susceptible to advanced cyberattacks, including SIM swap fraud, phishing, session jacking, and device spoofing. This study provides an in-depth mobile identity authentication system that would increase the security of OTP by combining the use of private blockchain, artificial intelligence (AI), and contextual verification through geolocation. The framework uses Hyperledger Fabric to decentralize identity verification and user privacy is ensured by a hybrid on-chain/off-chain data model, which is backed by smart contracts. Anomaly detection models based on AI and trained on behavioral patterns of SIM usages and previously known fraud cases have an accuracy rate of 85% when it comes to detecting real-time attacks of SIM swapping. Geolocation authentication, a geo-hashing method-based approach, is a further development of contextual trust by authenticating OTP requests only within defined and trusted geographic areas with an accuracy of 90 percent. Besides that, the system also engages in decentralized Know-Your-Customer (KYC) verification, which can guarantee privacy-preserving mobile identity management. It developed a full-fledged prototype that was tested showing the performance of less than 500 milliseconds latency, high transaction throughput, and proper fraud detection. The APIs that are based on microservices are flexible and interoperable with mobile network operators (MNOs) and service providers. With a combination of these technologies, the framework can augment the reliability and security of the OTP-based authentication considerably. This work describes the severe shortcomings of existing centralized OTPs and a scalable and privacy-sensitive way to provide mobile and digital identity ecosystems in the future.

ACKNOWLEDGEMENT

I extend my heartfelt thanks to all who played a part in the success of this research. I am especially grateful to the Faculty of Graduate Studies and Research, as well as to our lecturers, for equipping us with the knowledge and training essential for completing this project and for gaining meaningful professional experience.

I owe my deepest gratitude to Prof. Dilshan De Silva for his guidance and mentorship. His insightful advice, constructive feedback, and constant encouragement have been invaluable throughout my research journey. I am sincerely thankful for the opportunities and independence he entrusted to me, which have greatly shaped my academic growth and personal development.

TABLE OF CONTENTS

DECLARATION	ii
ABSTRACT	iii
ACKNOWLEDGEMENT	iv
TABLE OF CONTENTS	v
List of Figures	ix
List of Tables	x
Chapter 1 Introduction	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Research Aim and Objectives	3
1.3.1 Research Aim	3
1.3.2 Research Objectives	4
1.4 Research Questions	5
1.5 Justification / Motivation	7
1.6 Thesis Structure	9
Chapter 2 Literature Review	11
2.1 Introduction to the Literature Review	11
2.2 OTP Authentication Mechanisms	13
2.3 Vulnerabilities in Conventional OTP Systems	14
2.4 SIM Swap Fraud: Nature, Impact, and Detection	15
2.5 Detection Blockchain-Based Identity and Authentication	17
2.6 AI for Fraud Detection and Anomaly Identification	18
2.7 Geolocation-Based Authentication and Privacy Concerns	20
2.8 Hybrid and Multi-Factor Authentication Approaches	21
2.9 Research Gap Analysis	23
2.10 Summary of the Literature Review	24
Chapter 3 Research Methodology	27
3.1 Introduction to Methodology	27
3.2 Research Design and Rationale	28
3.3 System Architecture and Conceptual Framework	29
3.4 Blockchain Implementation (Hyperledger Fabric)	31
3.5 AI Model Development and Fraud Detection Algorithms	33
3.5.1 Model Selection	33
3.5.2 Dataset Preparation	33
3.5.3 Training, Testing, and Evaluation	35

3.5.4 Integration with the Framework.....	35
3.5.5 Summary	35
3.6 Privacy-Preserving Geolocation Verification	36
3.6.1 Geolocation Concept and Importance in OTP Authentication.....	36
3.6.2 Privacy Challenges and Risks	37
3.6.3 Privacy-Preserving Geolocation Techniques	37
3.6.4 Integration with the Proposed Framework.....	38
3.6.5 Spoofing and Accuracy Considerations	39
3.6.6 Summary	40
3.7 Dataset, Simulation, and Data Preparation	40
3.7.1 Synthetic Dataset Generation Process and Assumptions for SIM Swap Detection.....	40
3.7.2 Data Simulation for Fraud Scenarios	41
3.7.3 Data Preprocessing and Preparation.....	43
3.8 Tools and Performance Evaluation	45
3.8.1 AI Model Development and Testing.....	45
3.8.2 Blockchain Implementation	46
3.8.3 Geolocation Verification.....	46
3.8.4 Integrated Framework Evaluation.....	47
3.8.5 Summary	47
3.9 Ethical, Legal, and Regulatory Considerations.....	47
3.9.1 Ethical Considerations	48
3.9.2 Legal and Regulatory Compliance.....	48
3.9.3 Responsible AI Practices	49
3.9.4 Summary	49
3.10 Summary of the Methodology	49
Chapter 4 System Implementation.....	52
4.1 Introduction.....	52
4.2 System Implementation Overview.....	52
4.3 Blockchain Implementation and Evaluation	54
4.3.1 Private Blockchain Architecture	54
4.3.2 Smart Contracts for Identity and OTP Lifecycle Management.....	55
4.3.3 Tamper-Proof User Mobile Identity Management.....	55
4.3.4 Hybrid On-/Off-Chain Storage	56
4.3.5 Performance Evaluation with Hyperledger Caliper	56
4.4 AI Model Implementation and Evaluation.....	56
4.4.1 Model and Environment.....	57
4.4.2 Feature Set	57

4.4.3 Data and Preprocessing	57
4.4.4 Training Protocol	57
4.4.5 Outputs and Decisioning	57
4.4.6 Latency and Throughput Impact	58
4.4.7 Limitations	58
4.5 Geolocation Layer: Privacy-Preserving Contextual Verification	58
4.6 Integration of Blockchain, AI, and Geolocation Modules	60
4.6.1 Workflow Integration	60
4.6.2 Interoperability Across Stakeholders	61
4.6.3 Performance of Integrated System	62
4.7 Microservices and API-Based Interoperability	62
4.8 Prototype Development and Deployment Environment	66
4.9 Summary of System Design and Implementation	67
Chapter 5 Results and Evaluation	68
5.1 Introduction	68
5.2 Blockchain Performance Results	68
5.2.1 Latency Performance	69
5.2.2 Throughput	69
5.2.3 Resource Utilization	69
5.2.4 Scalability and Consensus Overhead	69
5.2.5 Summary of Blockchain Results	69
5.3 AI Model Evaluation Results	70
5.3.1 Classification Performance	70
5.3.2 Probability-Based Risk Mapping	71
5.4 Geolocation Verification Results	71
5.4.1 Validation Accuracy	71
5.4.2 False Rejection and Spoofing Resistance	71
5.4.3 Latency of Location Verification	72
5.4.4 Privacy Preservation	72
5.4.5 Summary of Geolocation Results	72
5.5 Integrated System Performance Results	72
5.5.1 End-to-End Latency	72
5.5.2 Scalability and Load Handling	73
5.5.3 Fraud Detection Impact	73
5.5.4 System Interoperability	73
5.5.5 Summary of Integrated Performance	74
5.6 Comparative Analysis with Existing Approaches	74

5.6.1 Conventional OTP Systems	74
5.6.2 Blockchain-Based Approaches	74
5.6.3 AI-Driven Fraud Detection Approaches	74
5.6.4 Geolocation-Based Approaches	75
5.6.5 Integrated Hybrid Approaches	75
5.6.6 Comparative Summary	75
Chapter 6 Conclusion and Future Work	76
6.1 Conclusion	76
6.2 Limitations	77
6.3 Future Work	78
REFERENCES	79

List of Figures

Figure 3-1 Conceptual framework	29
Figure 3-2 Key Components of the Proposed OTP Authentication Framework	30
Figure 3-3 Conceptual Framework of Geolocation in OTP Authentication	36
Figure 3-4 Representation of GeoHash Grid Encoding	37
Figure 3-5 GeoHash Precision vs. Location Match Confidence.....	38
Figure 3-6 OTP Verification Flow Incorporating Cross-Validated Geolocation Signals.....	39
Figure 3-7 Confusion Matrix of Random Forest Model	45
Figure 4-1 High Level Architecture for Enhancing OTP Security and Mobile Identity Authentication Framework	53
Figure 4-2 Transaction Origination and Mobile Device Location Verification through MNO Triangulation	60
Figure 4-3 Interaction sequence of OTP verification with The User Identity Management System, MNO, AI, and blockchain	61

List of Tables

Table 2.1 Overview of research papers discussed in the study.....	12
Table 3.1 SIM Swap fraud detection Model training dataset structure	34
Table 3.2 Classification Report and of Random Forest Model	46
Table 5.1 Evaluation Report of Model Performance Across Classes	70
Table 5.2 Actual vs Predicted Class Distribution for Evaluation Set	70