



Optimizing Multi-Factor Authentication Protocols to Bolster Corporate User Security

B.G.P. Indika
MS23017238

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 (CYBERSECURITY)

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.



Prof. Anuradha Jayakody

Supervisor's name and surname

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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

B.G.P. Indika

Date: 10th November 2024

ABSTRACT

Optimizing Multi-Factor Authentication Protocols to Bolster Corporate User Security

Indika Gamage

MSc. in Information Technology - Cybersecurity

Supervisor: Prof. Anuradha Jayakody

December 2024

In today's cybersecurity landscape, where corporate entities face sophisticated threats, robust authentication measures are essential. This research focuses on designing a contextual and risk-based Multi-Factor Authentication (MFA) model to enhance corporate security. Unlike traditional static MFA, the proposed model incorporates dynamic, context-sensitive factors such as user behavior, location data, and risk levels, strengthening defenses in environments handling sensitive information.

This study highlights the need for adaptable authentication solutions capable of responding in real-time to evolving threats. By integrating biometric and adaptive authentication technologies, the research aims to enhance both security and user experience. The proposed scalable MFA model offers a multi-layered defense mechanism tailored to the demands of corporate environments, contributing to improved data protection and organizational trust.

While this approach advances secure authentication practices, it also presents challenges, such as privacy concerns stemming from extensive data collection, high implementation complexity, and the need for accurate, real-time data. Scalability may lead to system delays, and frequent verification prompts risk frustrating users. Balancing security, usability, and privacy is critical for long-term success.

In conclusion, this research demonstrates the potential of contextual and risk-based MFA models to effectively mitigate cybersecurity threats. By providing a more adaptive and responsive framework, the study contributes to the development of improved corporate cybersecurity practices, addressing the growing need for solutions that safeguard data assets and maintain trust with stakeholders.

ACKNOWLEDGEMENT

While at Sri Lanka Institute Information Technology, I have benefited from having great advisors who seem to agree about very little. Prof. Anuradha Jayakody 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. I am especially grateful to the Mahapola Trust, which funded the fieldwork in 2024.

TABLE OF CONTENTS

| | |
|---|------|
| DECLARATION | ii |
| ABSTRACT..... | iii |
| ACKNOWLEDGEMENT..... | iv |
| TABLE OF CONTENTS..... | v |
| List of Figures | viii |
| List of Tables | viii |
| Chapter 1 Introduction | 1 |
| 1.1 Overview | 1 |
| 1.1.1 Historical Background | 1 |
| 1.2 Motivation and benefits for risk and context base MFA | 4 |
| 1.3 Research Question..... | 4 |
| 1.4 Objectives..... | 5 |
| 1.5 Scope and Limitations:..... | 6 |
| 1.5.1 Specific Scope..... | 6 |
| 1.5.2 Boundaries and Limitations | 7 |
| 1.6 Significance of the Study..... | 7 |
| 1.6.1 Importance in the Field of Cybersecurity..... | 8 |
| 1.6.2 Potential Industry Impact | 8 |
| 1.6.3 Contributions to Academic Research..... | 9 |
| 1.6.4 Influence on Policy Making | 9 |
| 1.7 Methodological Approach | 10 |
| 1.7.1 Quantitative Methods for Security and Performance Evaluation | 10 |
| 1.7.2 Qualitative Methods for Usability Testing and User Experience | 10 |
| 1.7.3 Combining Both..... | 11 |
| 1.8 Structure of the Thesis..... | 11 |
| 1.9 Definitions of Key Terms | 12 |
| 1.10 Summary | 14 |
| Chapter 2 Literature Review | 16 |
| 2.1 Review of Existing Literature | 16 |
| 2.2 The Evolution of Multi-Factor Authentication (MFA)..... | 16 |
| 2.2.1 Emergence of Dynamic and Risk-Based MFA | 16 |
| 2.2.2 Contradictions in Findings..... | 17 |
| 2.2.3 Areas of Consensus | 17 |
| 2.3 Risk-Based and Contextual MFA | 18 |

| | |
|--|----|
| 2.3.1 Strengths of Risk-Based and Contextual MFA..... | 18 |
| 2.3.2 Weaknesses of Risk-Based and Contextual MFA | 19 |
| 2.3.3 Contradictions in Findings..... | 20 |
| 2.3.4 Areas of Consensus Among Researchers..... | 20 |
| 2.4 Behavioral Biometrics for Implicit Authentication..... | 21 |
| 2.4.1 Behavioral Biometrics for Implicit Authentication..... | 21 |
| 2.4.2 Contradictions in Findings..... | 23 |
| 2.4.3 Areas of Consensus Among Researchers..... | 24 |
| 2.5 Blockchain-Based Authentication Schemes..... | 25 |
| 2.6 The Role of AI and Machine Learning in Authentication | 25 |
| 2.7 Enhancing Detection of Anomalies..... | 27 |
| 2.8 MFA on Cloud Computing..... | 27 |
| 2.9 Dynamic MFA Smart Phones..... | 28 |
| 2.10 MFA for IOT..... | 29 |
| 2.11 Gap Identification in Multi-Factor Authentication (MFA) Systems | 32 |
| 2.12 Effectiveness of Risk-Based and Contextual MFA..... | 34 |
| 2.13 Adaptive Authentication and Its Challenges..... | 36 |
| Chapter 3 Methodology..... | 38 |
| 3.1 Enhance MFA Security with Contextual-Based and Risk-Based Authentication | 38 |
| 3.1.1 Define Objectives and Scope | 38 |
| 3.2 Detailed Description of Methodological Framework..... | 38 |
| 3.3 Incorporate Literature References..... | 39 |
| 3.4 Contextual-Based Authentication..... | 39 |
| 3.5 Risk-Based Authentication | 40 |
| 3.6 Implementation and Testing..... | 41 |
| 3.6.1 Quantitative Approach: Testing Scenarios for System Performance and Security Effectiveness | 42 |
| 3.6.2 Qualitative Approach: Usability Testing and User Feedback Scenarios..... | 43 |
| 3.6.3 Ethical Considerations..... | 45 |
| 3.6.4 Feedback Mechanism for Continuous Improvement | 45 |
| Chapter 4 Conceptual Framework..... | 46 |
| 4.1 Definition of Key Concepts..... | 46 |
| 4.2 Use of Visual Aids..... | 47 |
| 4.3 Theoretical Foundations | 48 |
| 4.4 Components of the Conceptual Framework..... | 48 |
| 4.5 Justification for Component Selection..... | 50 |

| | |
|---|-----|
| 4.6 Dynamic Nature of the Framework | 51 |
| Chapter 5 System Design | 56 |
| 5.1 System Architecture..... | 56 |
| 5.2 Spring boot application service..... | 56 |
| 5.2.1 Purpose of Micro services..... | 56 |
| 5.2.2 Spring Boot frameworks for Microservices Development..... | 57 |
| 5.2.3 Additional Services of Spring Bood Application Service | 61 |
| 5.2.4 Entities used in our Spring boot application service..... | 67 |
| 5.2.5 API uses management in the Spring boot application service..... | 69 |
| 5.3 Flask Application Service..... | 74 |
| 5.3.1 Purpose of choose Flask..... | 74 |
| 5.3.2 Features of Flask. | 75 |
| 5.3.3 APIs implemented in the Flask application..... | 76 |
| 5.3.4 Logic in that API. | 77 |
| 5.3.5 Random Forest..... | 79 |
| 5.3.6 Purpose of choose Random Forest | 81 |
| 5.4 Face Matching API..... | 82 |
| 5.4.1 Angular framework | 83 |
| 5.4.2 Purpose of Choose Angular..... | 85 |
| Chapter 6 Result..... | 86 |
| 6.1 Existing research paper analysis. | 86 |
| 6.1.1 Evaluation of how improves current MFA systems. | 89 |
| 6.2 Evaluation of Developed MFA System..... | 92 |
| 6.2.1 User Feedback on Contextual and Risk-Based MFA Prototype | 92 |
| 6.2.2 Improved Security through Contextual and Risk-Based MFA..... | 92 |
| 6.2.3 Importance of User Awareness and Education..... | 93 |
| 6.2.4 Summary of User Feedback and Recommendations | 95 |
| 6.2.5 Testing Scenarios summary | 96 |
| Chapter 7 Discussion..... | 97 |
| 7.1 Interpretation of Results..... | 97 |
| 7.1.1 Effectiveness | 97 |
| 7.1.2 Impact the field of security and MFA systems..... | 99 |
| 7.1.3 Limitations and constraints..... | 103 |
| Chapter 8 Conclusion | 106 |
| References | 108 |

List of Figures

| | |
|--|----|
| Figure 9: High-level diagram for contextual base authentication | 52 |
| Figure 10: High level work floor of the MFA Process..... | 54 |
| Figure 11: Architecture Diagram of a Spring Boot Application..... | 61 |
| Figure 12: Architecture Diagram of a Spring Boot Application..... | 64 |
| Figure 13: User Information Table | 67 |
| Figure 14: Login attempt table..... | 68 |
| Figure 15: User history table..... | 68 |
| Figure 16: Password forget table | 68 |
| Figure 17: Password history table..... | 69 |
| Figure 18: API for registration..... | 69 |
| Figure 19: API for Login..... | 70 |
| Figure 20: User risk analysis..... | 71 |
| Figure 21: Forgot password | 71 |
| Figure 22: Password rest API | 71 |
| Figure 23: Validate Email API | 71 |
| Figure 24: Validate password rest | 72 |
| Figure 25: Flow chart of the login | 73 |
| Figure 26: Architecture diagram of a Flask micro-service application..... | 75 |
| Figure 27: User login history table | 76 |
| Figure 28: Behavior user login history | 76 |
| Figure 29: Coding for login history API..... | 77 |
| Figure 30: Coding for user risk analysis..... | 78 |
| Figure 31: Coding for location behavior | 78 |
| Figure 32: Coding for location risk analysis..... | 79 |
| Figure 33: Coding for Random Forest | 79 |
| Figure 34: The diagram illustrates the working of the Random Forest algorithm..... | 80 |
| Figure 35: sample of diagram for random forest..... | 81 |
| Figure 36: Coding for Random Forest classification risk behavior..... | 82 |
| Figure 37: High-Level Architecture | 83 |

List of Tables

| | |
|---|-------------------------------------|
| Table 1.1 Style Table | Error! Bookmark not defined. |
| Table 2: Summary of Testing Scenario..... | 96 |
| Table 3: Summary of Conclusion | 107 |