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is entirely my own and not of any other person, unless explicitly acknowledged (including citation of published and unpublished sources).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

List of Figures

List of Tables