EFFECTIVENESS OF MULTI FACTOR AUTHENTICATIONS TO ENSURE INFORMATION SECURITY ON CUSTOMER DATA STUDY ON THE INSURANCE INDUSTRY IN SRI LANKA

Dinesh Samarasekara

219151V

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

July 2023

EFFECTIVENESS OF MULTI FACTOR AUTHENTICATIONS TO ENSURE INFORMATION SECURITY ON CUSTOMER DATA STUDY ON THE INSURANCE INDUSTRY IN SRI LANKA

Dinesh Samarasekara
219151V

The dissertation was submitted to the Department of Computer Science and Engineering of the University of Moratuwa in partial fulfilment of the requirement for the Degree of Master of Business Administration in Information Technology.

Department of Computer Science and Engineering

University of Moratuwa
Sri Lanka

July 2023

DECLARATION

I declare that this is my own work, and this thesis does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

……. ……31/07/2023……..

Dinesh Samarasekara

(Signature of the candidate) Date:

The above candidate has carried out research for the Masters thesis under my supervision.

31/07/2023

…….. ……

Dr. PDJB Karunarathne Date

Signature of the Supervisor

…… ……

(Co-supervisor Name) Date

Signature of the Co-Supervisor

COPYRIGHT STATEMENT

ABSTRACT

Organizations face new challenges in securing their networks and systems due to the growing threat of cybersecurity attacks and the shift towards remote work due to the COVID-19 pandemic. Traditional username and password authentication methods are no longer sufficient to protect against increasingly sophisticated attacks. Multi-factor authentication (MFA) provides an added layer of security by combining two or more authentication factors to enforce access policies. MFA is a security feature that requires submitting two or more than two items of information to confirm that they are the actual user. This can include items such as passwords, One Time Password (OTP)s sent to their registered mobile phones or emails, or biometrics such as face recognition or fingerprint scan. These hardened methods are more difficult to interpret by attackers since the actual user biometrics are involved, therefore they do not have much support even if they steal an OTP or a password. For instance, a typical user might be required to enter their username and password, as well as a code sent to their phone. As a result, even if an attacker has the user's login and password, accessing their account will be far more challenging. MFA can employ a wide variety of various sorts of elements. The following are some examples of common factors: something you know, like a login and password; something you have, like a security token or a smartphone; and something you are, like a fingerprint or face recognition. There are many challenges and opportunities associated with implementing MFA in various contexts. Some of the challenges include cost, complexity, and user acceptance. However, there are also many opportunities associated with implementing MFA. Some of the opportunities include increased security, reduced risk, and improved compliance. Overall, MFA is a valuable tool that can help organizations to improve their security posture. With all above in hand, it is more important to consider the challenges over opportunities while implementing MFA solutions before finalizing the decision.

Keywords: multi-factor authentication, MFA, security, remote workforce, authentication factors, technology, usability, regulatory compliance, application readiness, end device readiness, implementation challenges, organizational behavior

ACKNOWLEDGEMENT

I would like to extend my heartfelt appreciation to everyone who helped finish this research book.

First and foremost, I want to express my gratitude to Dr. Buddika Karunarathne, my supervisor, for all of his or her advice and assistance during this study project. Your invaluable feedback, encouragement, and expertise have helped me immensely in shaping my ideas and presenting them in a coherent and structured manner.

I would also like to extend my thanks to the participants who have generously given their time and shared their insights, without whom this research would not have been possible. Your contributions have provided a rich and diverse perspective that has enriched the findings and conclusions of this study.

Additionally, I would like to thank my friends and coworkers for their encouragement and aid during the study process. Even when things were tough, your constant encouragement and support kept me going.

Finally, I want to thank my family from the bottom of my heart for their unwavering love and assistance. Without your unfailing encouragement and support, I would not have been able to do this. Your belief in me has been a continual source of strength and inspiration.

I sincerely appreciate each and every one of your contributions, without which this study book would not have been feasible.

Dinesh Samarasekara

TABLE OF CONTENTS

DECLARATION I
COPYRIGHT STATEMENT II
ABSTRACT III
ACKNOWLEDGEMENT IV
TABLE OF CONTENTS V
LIST OF FIGURES VIII
LIST OF TABLES IX
LIST OF ABBREVIATIONS X
1. INTRODUCTION 1
1.1. Background 1
1.1.1. The need for MFA 2
1.1.2. Risk-based identification and authentication 3
1.1.3. Key Benefits 4
1.2. Motivation 5
1.2.1. The challenges 6
1.3. Research Scope 7
1.4. Problem Statement 8
1.5. Research Objectives 9
1.6. Research Significance 9
1.7. Research Questions 10
1.8. Outline 10
2. LITERATURE REVIEW 12
2.1. Chapter Overview 12
2.2. Multi-factor Authentication (MFA) Overview 15
2.3. Human Factor (User Experience) in MFA 16
2.4. Technology of MFA 19
2.5. Application Readiness in MFA 22
2.6. End Device Readiness in MFA 24
2.7. Regulatory Compliance in MFA 26
2.8. Types of Authentication Factors 28
2.9. Password based authentication 29
2.10. Authentication with Certificates 30
2.11. Two Factor Authentication (2FA) 30
2.12. Authentication Mechanisms in Development 31

2.13. Issues in data protection mechanisms 31
2.14. Synthesis of Literature 32
2.15. Theoretical Framework Background 34
2.16. Theoretical Framework 35
2.17. Variable Operationalization 36
2.18. Conclusion 39
3. RESEARCH METHODOLOGY 43
3.1. Introduction 43
3.2. Research Design and Approach 43
3.3. The Research Methodology Implementation 47
3.4. Constructing and Administering Questionnaire 47
3.5. Study Population and Sample Selection 49
3.6. Dealing with Ethical Issues 50
3.7. Validity of Research 52
3.8. Research Outcome 53
3.9. Problems Encountered 53
4. DATA ANALYSIS 55
4.1. Introduction 55
4.2. A Summary of Data Analysis Techniques 57
4.3. Preparation for Data Analysis 58
4.3.1. Dealing with Missing Data in the data set 58
4.3.2. Handling Outliers 59
4.3.3. Questionnaire Reliability 60
4.4. The Statistical Data Overview 60
4.5. Sample profile 62
4.5.1. Gender 62
4.5.2. Age 63
4.5.3. Occupation 64
4.5.4. Experience 66
4.5.5. Education 67
4.5.6. Descriptive Statistics 68
Table 4.7: Descriptive statistics 69
4.6. Reliability Analysis 69
4.6.1. User experience with MFA 69
4.6.2. The technology used for MFA 70

4.6.3. Application readiness for MFA 70
4.6.4. End device readiness for MFA 71
4.6.5. Regulatory compliance for MFA 71
4.6.6. Effectiveness of MFA 71
4.7. Correlation analysis 72
4.8. Regression analysis 73
4.9. Hypotheses Testing 77
4.10. Objective Analysis 78
4.10.1. Impact of user experience 78
4.10.2. Relationship between technology of MFA 78
4.10.3. Influence of application readiness 78
4.10.4. The role of end device readiness 78
4.10.5. Effect of regulatory compliance 79
4.10.6. Impact of implementing MFA on customer data security 79
4.11. Limitations and future directions 79
5. RECOMMENDATIONS AND CONCLUSION 81
5.1. Recommendations 81
5.2. Conclusion 89
REFERENCES 91
APPENDIX A: RESEARCH QUESTIONAIRE 98

LIST OF FIGURES

Figure 2.1: Theoretical Framework 35

Figure 2.2: Series of reflective hypotheses 39

Figure 3.1: Conceptual Model for Research 45

Figure 4.1: Analysis of the Gender Distribution 63

Figure 4.2: Analysis of the Age Distribution 64

Figure 4.3: Analysis of the Occupation Distribution 65

Figure 4.4: Analysis of the Experience Distribution 67

Figure 4.4: Analysis of the Education Distribution 68

Figure 4.5: Frequency Histogram 76

Figure 4.6: Residual scatterplot 76

LIST OF TABLES

Table 2.1: Variable Declaration 36

Table 2.2: Operationalization of Variables 36

Table 4.1: The Statistical Data Overview 60

Table 4.2: Analysis of the Gender Distribution 63

Table 4.3: Analysis of the Age Distribution 64

Table 4.4: Analysis of the Occupation Distribution 66

Table 4.5: Analysis of the Experience Distribution 66

Table 4.5: Analysis of the Education Distribution 67

Table 4.7: Descriptive statistics 69

Table 4.8: Reliability of User experience with MFA 69

Table 4.9: Reliability of The Technology used for MFA 68

Table 4.10: Application readiness for MFA 70

Table 4.11: Reliability of End device readiness for MFA 70

Table 4.12: Reliability of Regulatory compliance for MFA 71

Table 4.13: Reliability of Effectiveness of MFA 71

Table 4.14: Correlation analysis 72

Table 4.15: Model summary 73

Table 4.16: ANOVA 73

Table 4.17: Coefficient Table 74

Table 4.18: Hypotheses Testing 77

LIST OF ABBREVIATIONS

2FA	Two Factor Authentication
MFA	Multi-Factor Authentication
VPN	Virtual Private Network
IAM	Identity and Access Management
OTP	One Time Password
IT	Information Technology
AI	Artificial Intelligence
IP	Internet Protocol
COVID-19	Corona virus Disease of 2019
PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
PIN	Personal identification number
SMS	Short Message Sender
HIPAA	Health Insurance Portability and Accountability Act
RFID	Radio-frequency identification
API	Application programming interface
SPSS	Statistical Package for Social Sciences
URL	Uniform Resource Locator
UE	User experience with MFA
TU	Technology used for MFA
AR	Application readiness for MFA
EDR	End Device readiness for MFA
RC	Regulatory compliance for MFA
EM	Effectiveness of MFA