

The Impact of Digitalization on Fraud Prevention and Detection in the Sri Lankan Banking Industry

Makesalinkam Suja

239119B

Degree of Master of Business Administration in Information Technology

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

August 2025

The Impact of Digitalization on Fraud Prevention and Detection in the Sri Lankan Banking Industry

Makesalinkam Suja

239119B

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

August 2025

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).

.....

Makesalinkam Suja

...11-08-2025...

Date:

The above candidate has carried out research for the Master's thesis under my supervision.

Name of the supervisor:

Dr R.M. Sunimal Rathnayake

.....

Signature of the Supervisor

12-08-2025.....

Date

COPYRIGHT STATEMENT

I hereby grant the University of Moratuwa the right to archive and to make available my thesis or dissertation in whole or part in the University Libraries in all forms of media, subject to the provisions of the current copyright act of Sri Lanka. I retain all proprietary rights, such as patent rights. I also retain the right to use in future works (such as articles or books) all or part of this thesis or dissertation.

ABSTRACT

The banking industry in Sri Lanka has been rapidly digitalized and this has completely revolutionized the way through which financial services are delivered and at the same time introduced new unprecedented fraud risks, which have not been equally met by the older strategies of preventing them. The study researches the effects of digitalization on the effectiveness of fraud prevention and detection in Sri Lankan commercial banks via identification of vulnerabilities and formulation of strategic recommendations regarding improved security capabilities.

With quantitative research methodology, the study gathered data of 518 customers with digital banks and 300 working with the banking sector in major commercial banks using structured surveys. This study employed the Technology-Organization-Environment (TOE) model to review the complex relationships between digital transformation programs and fraud prevention efficiency through lenses of technology capacity, organization preparedness, and an environment.

The important findings explain that there is an urgent gap between the rate of digital banking adoption and the ability to protect it, and it means that even traditional rule-based fraud detection systems are only 45 percent effective against modern threats and have a false positive rate of 15 percent. The study also sees considerable room to be improved with improved technologies, as the artificial intelligence and machine learning systems performed 85 percent better in terms of detection as well as biometric authentication can prevent account takeover fraud by 99.9 percent.

The research has concluded that the organizational elements, such as staff training and customer education, are rather important factors of successful fraud prevention, and well-trained institutions achieve better results than institutions found only on technological afterthoughts by 50 percent better. When done with privacy protection and an optimal user experience, 94 percent of customers accept increased security precaution.

Research recommendations suggest the following: multi-factor authentication and AI-enabled detection systems should be implemented right away, medium-step installation of end-to-end biometric-based authentication and predictive analytics systems, and long-term implementation of the capability to share information across banks in a cross-bank environment. The presented three-phased implementation framework will systematically guide the process of improving fraud prevention by ensuring the efficiency of operations and customer satisfaction.

This study will add practical evidence-based solutions that can be adopted in Sri Lankan banks in order to face the fraud prevention issue and keep on with the digital development and achieve the competitive edge in the new financial services scene.

Keywords: Digital Banking, Fraud Prevention, Fraud Detection, Banking Security, Sri Lankan Banking, Digitalization, Artificial Intelligence, Machine Learning, Biometric Authentication, Multi-Factor Authentication, Cybersecurity, Financial Technology, Risk Management, Customer Authentication

ACKNOWLEDGEMENT

I also would like to thank all the people who helped with the successful completion of the research project.

First, I would like to express my greatest gratitude to my supervisor at the University of Moratuwa MBA in IT special programmed and the insights, knowledge and never-ending support provided in this study. Their keen response and critical comments were useful in this research.

I would like to thank the relevant commercial banks and its management bodies who gave me a chance in reaching their institutes and help with data collection. Thanks, especially to the 300 banking professionals who so generously gave their time and expertise in the participation of the surveys and who were key to giving insightful information on the various challenges and possibilities of fraud prevention.

I would like to thank the 518 digital banking clients who identified and participated in this study to assure them of their role and contribution to my research that empowered the results of my research. The fact that they were ready to talk about controversial issues related to security helped them a lot in the research findings.

I also want to thank the Central Bank of Sri Lanka and other industry associations who gave me access to appropriate documentation and regulatory directions that helped me arrive at this study.

Due to members of the University of Moratuwa faculty who have offered methodological guidance and academic support during the undertaking of the research work. They gave invaluable experience in research design and analysis of the data.

I would also like to thank my friends and family for being patient, encouraging and understanding during the challenging time of my research work. They supported me and gave me the motivation that was required to make this work materialize.

Lastly, I agree to mention all researchers and practitioners whose publications have formed the theoretical base of this work and made up the larger knowledge novelty in the area of digital banking security and fraud prevention.

TABLE OF CONTENTS

1. INTRODUCTION	1
1.1. Background	1
1.2. Motivation	2
1.2.1. The Growing Digital Banking Adoption Crisis	2
1.2.2. Inadequacy of Traditional Fraud Prevention Methods.....	3
1.2.3. Severe Consequences of Fraud on Banking Sector Stability	3
1.2.4. The Imperative for Advanced Fraud Detection Systems	3
1.2.5. Critical Research Gap in Sri Lankan Context	4
1.2.6. Strategic Goal of Practical Solution Development	4
1.3. Research Scope	4
1.3.1. Digitalization Impact Analysis.....	5
1.3.2. Comprehensive Vulnerability Assessment	5
1.3.3. Current Fraud Prevention Method Evaluation	5
1.3.4. Advanced Technology Investigation.....	6
1.3.5. Practical Strategy Development.....	6
1.3.6. Sri Lankan Banking Sector Focus.....	6
1.3.7. Stakeholder Integration	6
1.4. Problem Statement	7
1.4.1. The Core Problem: Misaligned Digital Transformation and Security Evolution 7	
1.5. Research Gap Hindering Effective Solution Development	7
1.6. Research Objectives	8
1.6.1. Research Significance	11
1.6.2. Practical Significance for Banking Industry	12
1.6.3. Academic and Scientific Significance	12
1.6.4. Policy and Regulatory Significance	13
1.6.5. Economic and Social Significance.....	14
1.6.6. Strategic and Competitive Significance	14
1.7. Outline.....	15
2. LITERATURE REVIEW	20
2.1. Introduction	20

2.2.	Digital Banking Security Regulatory Framework in Sri Lanka.....	20
2.2.1.	Regulatory Directives of Sri Lankan Central Bank	20
2.2.2.	Risk and Controls Governance Structure	21
2.2.3.	Convention Integration.....	21
2.3.	Banking Security Background Technology Acceptance Model	21
2.3.1.	Theory on Risk Perception and Security Behavior	22
2.3.2.	Demographic factors to security behaviour	22
2.4.	The Adoption of Online Banking.....	23
2.5.	Mobile Banking Uptake	24
2.6.	Adoption Trends in Sri Lanka.....	27
2.7.	Comparison of the World.....	29
2.8.	Customer Satisfaction in Web-based Banking.....	31
2.8.1.	Service Quality Ricketts.....	31
2.9.	Effect of E-Banking Services.....	34
2.10.	Gender and Demographic Factor	36
2.11.	Advances in Technology in Banking	38
2.12.	Blockchain Technology	38
2.13.	Machine Learning and Artificial Intelligence	40
2.14.	Business Big Data Analytics.....	42
2.15.	Some of the high-growth areas are Fraud Detection and Prevention.	44
3.	RESEARCH METHODOLOGY.....	48
3.1.	Introduction.....	48
3.2.	Research Philosophy and Design	48
3.2.1.	Philosophical Foundation.....	48
3.2.2.	Research Design Framework	48
3.2.3.	Mixed-Methods Integration	49
3.3.	Theoretical Framework and Hypothesis Development.....	49
3.3.1.	Conceptual framework	49
3.3.2.	Theoretical Foundation	49
3.3.3.	Research Questions and Hypotheses.....	50
3.4.	Population and Sampling Strategy	52
3.4.1.	Target Population Definition	52
3.4.2.	Sampling Framework and Strategy	53

3.4.3.	Sample Size Determination and Power Analysis.....	54
3.5.	Data Collection Instruments.....	54
3.5.1.	Customer Survey Instrument	54
3.5.2.	Professional Survey Instrument	55
3.5.3.	Instrument Validation and Reliability.....	55
3.6.	Data Collection Procedures.....	56
3.6.1.	Data Collection Timeline	56
3.6.2.	Data Collection Platforms and Quality Controls	56
3.6.3.	Response Enhancement Strategies.....	57
3.7.	Ethical Considerations	57
3.7.1.	Ethical Approvals.....	57
3.7.2.	Participant Protection.....	57
3.8.	Data Analysis Plan	58
3.8.1.	Quantitative Analysis Strategy.....	58
3.8.2.	Qualitative Analysis Framework	58
3.8.3.	Mixed-Methods Integration	59
3.9.	Validity and Reliability Considerations	59
3.9.1.	Internal Validity	59
3.9.2.	External Validity	59
3.9.3.	Construct Validity	60
3.10.	Summary	60
4.	DATA ANALYSIS.....	61
4.1.	Introduction.....	61
4.2.	Data Quality Check and Validation	61
4.2.1.	Missing Values Analysis.....	61
4.2.2.	Variable Mapping and Operationalization	62
4.2.3.	Variable Classification and Relationships	65
4.2.4.	Data Distribution Analysis.....	66
4.2.5.	Preliminary Relationship Exploration.....	67
4.2.6.	Data Visualization and Patterns	68
4.2.7.	Data Quality Validation Summary.....	70
4.3.	Data Preparation and Sample Validation	70
4.3.1.	Data Quality Assessment	70

4.3.2.	Sample Representativeness Verification.....	71
4.4.	Descriptive Statistics and Exploratory Analysis	72
4.4.1.	Customer Sample Descriptive Statistics	72
4.4.2.	Professional Sample Descriptive Statistics	73
4.5.	Hypothesis Testing Results	73
4.5.1.	Overview of Hypothesis Testing Outcomes	73
4.6.	Detailed Hypothesis Analysis	76
4.6.1.	Introduction	76
4.6.2.	Overview of Hypothesis Testing Framework	76
4.7.	Detailed Hypothesis Testing Results	76
	H1: Age and Digital Banking Adoption Relationship	76
	H2: Security Awareness and Fraud Experience Relationship	78
	H3: Professional Experience and Digital Maturity	79
	H4: Security Budget and Fraud Detection Effectiveness	81
	H5: Channel Diversity and Security Vigilance	82
	H6: Password Strength Variations Across Age Groups.....	83
	H7: Digital Transaction Volume and Infrastructure Adequacy	85
	H8: Security Technology and Detection Time Efficiency	86
	H9: Professional Role Level and Budget Decision Authority	88
	H10: Fraud Experience and Security Vigilance Enhancement	89
	H11: Security Technology and Detection Rate Performance	90
4.8.	Summary of Hypothesis Testing Results	92
4.8.1.	Overall Success Rate.....	92
4.8.2.	Effect Size Distribution.....	92
4.8.3.	Statistical Power Achievement	92
4.8.4.	Theoretical Implications.....	93
4.8.5.	Practical Implications.....	93
4.9.	Limitations and Considerations	93
4.9.1.	Statistical Limitations	93
4.9.2.	Methodological Considerations	93
4.10.	Conclusion	94
4.11.	Qualitative Analysis and Theoretical Integration	94
4.11.1.	Thematic Analysis Framework	94

4.11.2.	Primary Themes and Theoretical Integration.....	94
4.11.3.	Professional Insights Integration.....	97
4.12.	Mixed-Methods Integration and Convergence Analysis.....	97
4.12.1.	Convergent Findings	97
4.12.2.	Divergent Insights	97
4.12.3.	Theoretical Model Validation	98
4.13.	Statistical Power and Effect Size Interpretation.....	98
4.13.1.	Achieved Statistical Power	98
4.13.2.	Effect Size Distribution and Interpretation	98
4.14.	Limitations and Methodological Considerations	99
4.14.1.	Statistical Limitations	99
4.14.2.	Sample Representativeness	99
4.15.	Summary of Key Findings	99
4.15.1.	Primary Research Contributions	99
4.15.2.	Mixed-Methods Integration Value.....	100
4.15.3.	Implications for Theory and Practice	100
5.	RECOMMENDATIONS AND CONCLUSION.....	101
5.1.	Interpretation of Key Findings	101
5.1.1.	Security Awareness and Fraud Prevention Effectiveness	101
5.1.2.	Device Usage and Security Behavior Relationship	102
5.2.	Practical Implications for Banking Industry	102
5.2.1.	Customer Segmentation and Targeted Security Programs.....	102
5.2.2.	Platform-Specific Security Enhancements.....	102
5.2.3.	Organizational Security Culture Development	103
5.3.	Policy Recommendations for Regulatory Authorities	103
5.3.1.	Enhanced Regulatory Framework.....	103
5.3.2.	Industry Collaboration Initiatives	103
5.4.	Study Limitations and Future Research Directions	104
5.4.1.	Methodological Limitations	104
5.4.2.	Future Research Opportunities.....	104
5.5.	Contributions to Knowledge and Practice	104
5.5.1.	Theoretical Contributions.....	104
5.5.2.	Methodological Contributions	105

5.6.	Summary of Key Findings	105
5.7.	Implications for Theory and Practice	106
5.8.	Recommendations for Stakeholders.....	106
5.9.	Final Conclusions.....	106
REFERENCES		108
APPENDIX A: SUEVERVEY FOR PROFFSSONALS		110
APPENDIX B: CUSTOMERS SURVEY		116
APPENDIX C: ANAYISIS EVIDANCE		120

LIST OF FIGURES

Figure 3. 1	Conceptual framework.....	49
Figure 4 . 1	Missing Values Analysis Summary	61
Figure 4 . 2	Data Visualization and Patterns	68
Figure 4 . 3	Digital Banking Adoption Distribution.....	69
Figure 4 . 4	Relationship Visualizations.....	69
Figure 4 . 5	Data Quality Validation Summary	70
Figure 4 . 6:	Age vs Digital Banking Adoption Scatter Plot.....	78
Figure 4 . 7	Security Awareness vs Fraud Experience	79
Figure 4 . 8	Professional Experience vs Digital Maturity Correlation Plot	80
Figure 4 . 9	Security Budget vs Fraud Detection Rate Analysis.....	82
Figure 4 . 10 :	Channel Diversity vs Security Vigilance Relationship.....	83
Figure 4 . 11	Password Strength by Age Groups Box Plot.....	85
Figure 4 . 12	Digital Transactions vs Infrastructure Score	86
Figure 4 . 13	Security Technology vs Detection Time Analysis	87
Figure 4 . 14	Role Level vs Security Budget Allocation	89
Figure 4 . 15	Fraud Experience vs Security Vigilance Comparison.....	90
Figure 4 . 16	Security Technology vs Fraud Detection Rate.....	92

LIST OF TABLES

Table 3.1: Key Variable Operationalizations	Error! Bookmark not defined.
Table 3.2 Data Collection Timeline	Error! Bookmark not defined.
Table 3.3 : Target vs. Actual Response Rates.....	Error! Bookmark not defined.
Table 4.2: Customer Sample Descriptive Statistics (N = 518)	Error! Bookmark not defined.

Table 4. 1 Customer Sample Descriptive Statistics (n = 518).....	72
Table 4. 2 Professional Sample Descriptive Statistics (n = 300).....	73
Table 4. 3 Summary of Hypothesis Testing Results	75
Table 4. 4 Effect Size Classification Distribution	75
Table 4. 5 Statistical Test Distribution and Effectiveness	76
Table 4. 6 Effect Size Classification Summary	99

LIST OF ABBREVIATIONS

List of Abbreviations

Banking and Financial Terms

ATM - Automated Teller Machine
CBSL - Central Bank of Sri Lanka
CRM - Customer Relationship Management
EFT - Electronic Funds Transfer
KYC - Know Your Customer
LKR - Sri Lankan Rupee
NEFT - National Electronic Funds Transfer
POS - Point of Sale
RTGS - Real Time Gross Settlement

Technology and Security Terms

AI - Artificial Intelligence
API - Application Programming Interface
AML - Anti-Money Laundering
BaaS - Banking as a Service
CI - Computational Intelligence
DLT - Distributed Ledger Technology
IoT - Internet of Things
IT - Information Technology
ML - Machine Learning
MFA - Multi-Factor Authentication
NFC - Near Field Communication
OTP - One Time Password
PIN - Personal Identification Number
QR - Quick Response
RFID - Radio Frequency Identification
SMS - Short Message Service
SSL - Secure Sockets Layer
TLS - Transport Layer Security
2FA - Two-Factor Authentication

Research and Academic Terms

ANOVA - Analysis of Variance
CEO - Chief Executive Officer
CTO - Chief Technology Officer
MBA - Master of Business Administration
PhD - Doctor of Philosophy
R&D - Research and Development
ROI - Return on Investment
SPSS - Statistical Package for the Social Sciences
TAM - Technology Acceptance Model
TOE - Technology-Organization-Environment
TPB - Theory of Planned Behavior

Digital Banking Terms

CAGR - Compound Annual Growth Rate
CISO - Chief Information Security Officer
CX - Customer Experience
FinTech - Financial Technology
GDP - Gross Domestic Product
ICT - Information and Communication Technology
RegTech - Regulatory Technology
SaaS - Software as a Service
UI - User Interface
UX - User Experience

Security and Fraud Prevention

ATO - Account Takeover
CCTV - Closed Circuit Television
CVV - Card Verification Value
DDoS - Distributed Denial of Service
EMV - Europay, Mastercard, and Visa
HTTPS - Hypertext Transfer Protocol Secure
IDS - Intrusion Detection System
IPS - Intrusion Prevention System
SIEM - Security Information and Event Management
SOC - Security Operations Center
VPN - Virtual Private Network

Regulatory and Compliance

AML - Anti-Money Laundering
CFT - Combating the Financing of Terrorism
FATF - Financial Action Task Force
GDPR - General Data Protection Regulation
ISO - International Organization for Standardization
PCI DSS - Payment Card Industry Data Security Standard

Statistical and Analytical Terms

ANOVA - Analysis of Variance
CI - Confidence Interval
KMO - Kaiser-Meyer-Olkin
PCA - Principal Component Analysis
SEM - Structural Equation Modeling
SPSS - Statistical Package for the Social Sciences

Organizational Terms

CEO - Chief Executive Officer
CFO - Chief Financial Officer
CIO - Chief Information Officer
CISO - Chief Information Security Officer
CRO - Chief Risk Officer
CTO - Chief Technology Officer
HR - Human Resources

Geographic and Institutional

ASEAN - Association of Southeast Asian Nations

EU - European Union

SAARC - South Asian Association for Regional Cooperation

UK - United Kingdom

US - United States

USA - United States of America

Miscellaneous

B2B - Business to Business

B2C - Business to Consumer

COVID-19 - Coronavirus Disease 2019

FAQ - Frequently Asked Questions

P2P - Peer to Peer

QR - Quick Response

SLA - Service Level Agreement