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).

……. …11-08-2025...

Makesalinkam Suja 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

…….. 12-08-2025……

Signature of the Supervisor Date

COPYRIGHT STATEMENT

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

LIST OF FIGURES

LIST OF TABLES

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