Usability-Security Trade-off: Quantifying Swiftness-Driven Risk Behaviors Among Mobile Financial Services (MFS) Users in Bangladesh

by

Shihab Shahriar Shanto
22299538
Sadnan Hossain
21301092
Humaira Bushra Tamim
24141114
M. Naphew Siddique
24141111
Umama Tasnuva Aziz
21301570

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
Brac University
December 2025.

Declaration

It is hereby declared that

1. The thesis submitted is our own original work while completing our degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material that has been accepted or submitted for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Humaira Bushra Tamim
24141114

M. Naphew Siddique
24141111

Sadnan Hossain
21301092

Shihab Shahriar Shanto
22299538

Umama Tasnuva Aziz
21301570

Approval

The thesis/project titled "Usability-Security Trade-off: Quantifying Swiftness-Driven Risk Behaviors Among Mobile Financial Services (MFS) Users in Bangladesh" submitted by:

1. Shihab Shahriar Shanto (22299538)
2. Sadnan Hossain (21301092)
3. Humaira Bushra Tamim (24141114)
4. M. Naphew Siddique (24141111)
5. Umama Tasnuva Aziz (21301570)

of Summer, 2021 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science in Fall, 2025.

Examining Committee:

Supervisor:
(Member)

Md. Sabbir Ahmed
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Md. Aquib Azmain
Senior Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Mobile Financial Services (MFS) applications represent a critical intersection between security and usability, where extremely smooth user experiences can lead to overconfidence and hard security measures can lead to user frustration. Both conditions have the potential to affect risky behavior among users. Existing MFS studies focusing on general technology adoption and usage intention are not entirely empirical enough to understand the self-reported or anticipated risky behavior of users. In order to fill this gap, this research expounds the Technology Acceptance Model (TAM) to include two additional variables, namely Swiftness (SWF) and Risky Behavior (RB).

A quantitative study was carried out on user speed, risk-related behaviors, perceived usefulness, perceived ease of use, perceived security, and some supplementary variables like usage experience, confidence in identifying frauds, training, etc., exploring the idea of usability-security trade-off in the security-usability-functionality triangle. The empirically analyzed relationships are based on the results collected from 707 MFS users in Bangladesh through a cross-sectional survey. It determines how risk-taking propensity in high-frequency financial environments is influenced by the different variables mentioned above. The study uses Python to clean and pre-process the collected data and applies SPSS and JASP to statistically analyze the collected responses. Structural Equation Modeling (SEM) was used to evaluate and validate the relationships, our five hypotheses, and some other variables claims to have.

The obtained results validates our four hypotheses and rejects one, findings like positive relationship between swiftness and risky behaviour suggests users who prefer swiftness tends to take risky actions more, additionally, negligible impact of training on reducing risky actions irrespective of what years of app usage experience a user holds then encouraging swiftness through making the app more easy to use etc indicates risky-actions are more impacted by situational-based decisions rather than being less-aware.

Based on these reflections, the paper suggests a more dynamic security approach rather than the existing static ones. Some future research implications include a dynamic MFS user interface design based on risk-based authentication and context components of risk indicators at major points of interaction. This empirical solution is intended to develop secure-by-design MFS interactions that are usable and fast, and help to minimize risky user behaviors.

Keywords: Mobile Financial Services, Technology Acceptance Model, Usability-Security Trade-off, Swiftness, Risky Behavior, Structural Equation Modeling, Bangladesh

Dedication

We dedicate this work to the millions of Mobile Financial Services users in Bangladesh who entrust their financial security to digital platforms daily. May this research contribute to creating safer, more user-friendly financial technologies that serve the needs of all citizens, from urban professionals to rural farmers, in our journey toward comprehensive digital financial inclusion.

We also extend our sincere appreciation to our families and to our friend Alamgir for their continued support and encouragement throughout this research.

Acknowledgment

We extend our sincere gratitude to the Department of Computer Science and Engineering at BRAC University for providing the academic environment and resources necessary for conducting this research. We are particularly thankful to the faculty members who reviewed our work at various stages and provided invaluable feedback that enhanced the quality of this thesis.

We are deeply grateful to the 707 Mobile Financial Services users who participated in our survey, sharing their experiences and behaviors candidly. Without their willingness to contribute their time and insights, this empirical investigation would not have been possible.

We acknowledge the Mobile Financial Services providers in Bangladesh, bKash, Nagad, Rocket, and others, whose platforms form the technological infrastructure that has transformed financial accessibility in our country. While we critically examine security-usability trade-offs, we recognize the transformative impact these services have had on financial inclusion across diverse demographic segments.

Our sincere indebtedness goes to everyone who ensured the quality and integrity of our research process through their diligent efforts.

Table of Contents

List of Figures

List of Tables

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

2FA Two-Factor Authentication

AMOS Analysis of Moment Structures

AVE Average Variance Extracted

CFA Confirmatory Factor Analysis

CFI Comparative Fit Index

CR Composite Reliability

HTMT Heterotrait-Monotrait Ratio

MFS Mobile Financial Services

OTP One-Time Password

PEOU Perceived Ease of Use

PIN Personal Identification Number

PS Perceived Security

PU Perceived Usefulness

RB Risky Behavior

RMSEA Root Mean Square Error of Approximation

SEM Structural Equation Modeling

SPSS Statistical Package for the Social Sciences

SRMR Standardized Root Mean Square Residual

SWF Swiftness (Speed/friction-reduction preference)

TAM Technology Acceptance Model

TLI Tucker-Lewis Index

Chapter 1

Introduction

1.1 Background

Mobile Financial Services (MFS) have fundamentally transformed Bangladesh's financial landscape. As of 2025, 89.38 million users 51.5% of the population actively use MFS platforms, processing approximately 450 million transactions monthly with a combined value exceeding BDT 800 billion. This represents one of the world's highest MFS penetration rates among developing economies.

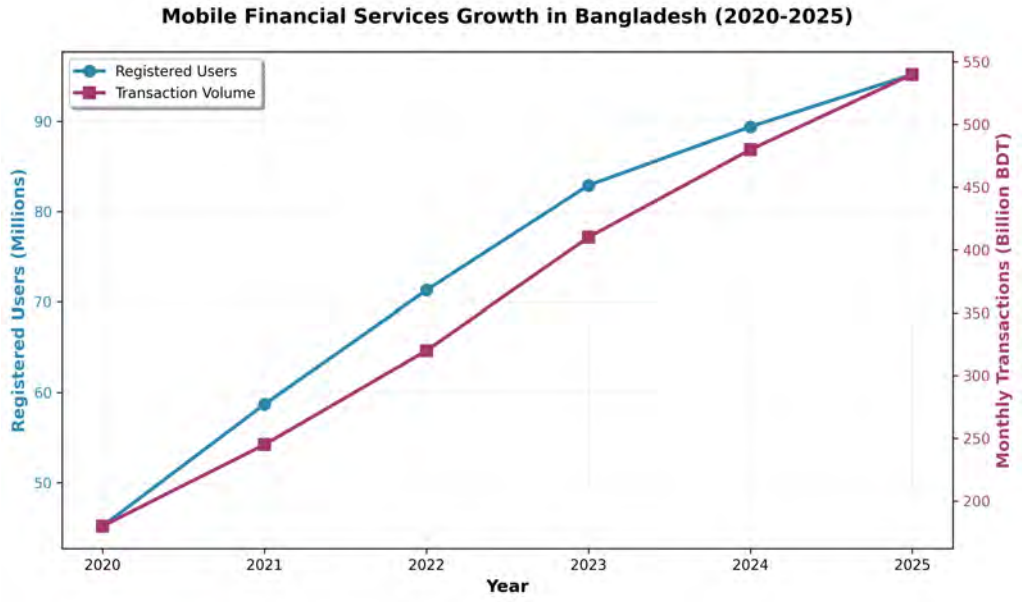

Figure 1.1: Mobile Financial Services Growth in Bangladesh (2020–2025).

The MFS ecosystem emerged following Bangladesh Bank's 2011 regulatory framework, permitting banks and mobile network operators to provide financial services via mobile platforms. Introduced in 2011, bKash was the first in the market to meet the urgent demands of the financial services in a country where the traditional banking infrastructure used in the country was still concentrated in the urban centers. Later new competitors, including Nagad (2019), Rocket (Dutch-Bangla Bank) and others, developed a competitive ecosystem that spurred ongoing innovation and reached more and more of the underbanked demographic.

The financial inclusion has been revolutionized. MFS services allow people such as farmers, their small businesses, domestic workers and migrant workers to send money, pay their bills, buy goods, get salaries and even manage finances without necessarily going to physical banks. due to lockdowns limiting physical interactions during the COVID-19 pandemic, when digital transactions were treated as unnecessary convenience, the adoption of MFS increased exponentially.

Yet, the rapid development has left a design problem with an urgent and vital aspect: how to maintain the security requirements in the balance with the demands of user experience. The software of a financial application should ensure that the user assets and personal information is secured with a strong level of security. But the high level of security will irritate consumers, delay the adoption process, lead to a high number of verification processes and cause abandonment. On the other hand, the use of simplified interfaces with the primary aim of achieving speed and convenience can accidentally foster unsafe user practices: not paying attention to security warnings, sharing of authentication credentials, and not completing the verification steps before transacting.

This security-usability-speed triangle is one of the major conflicts in the design of MFS. Customers are increasingly demanding frictionless transactions, and in many cases they will want to do financial transactions without entering PINs or waiting to receive One-Time Passwords (OTPs). Research in the industry shows that above 30 seconds transaction abandonment rates increase dramatically placing a strain on providers to reduce security friction. Though speed will increase user satisfaction and perceived utility, speed can result in a reduced level of security since users will want to by-pass security precautions that could stop fraud and unauthorized access.

These are complicated relationships between usability, security and speed that must be understood in order to create an MFS interface that is not compromised in its security but provides the user experience that contemporary users desire.

1.2 Rationale and Motivation

There are many notable findings and voids in the collection of recent literature that can be called the driving forces of this investigation. Although much research has been directed on the technology adaptation using the Technology Acceptance Model (TAM), many empirical studies objectively measure the actual risky behaviors instead of simply imagined risks or behavioral intentions [4], [24]. Most of the available studies are anchored on adoption purposes and overall consumption patterns, which do not properly explore the effectiveness of certain usability features, especially speed and ease of use, which make users adopt observable risky behaviors that undermine the security.

The theoretical framework of Bangladesh offers a fairly strong and applicable theoretical basis to our research. Due to the fact that the country is a developing economy that is rapidly expanding its digital financial base, it faces special challenges in the establishment of a balance between access and security demands. Since MFS is deployed by a large number of demographic groups with wildly different degrees of digital literacy, in some cases, the decisions motivated by usability have direct and apparent security implications [46]. Also, the presence of informal financial practices

and the cultural nature of trust-based finance can affect how customers think and react to the security features implemented in the digital platforms in a fundamental way.

There is an indication that MFS users in Bangladesh often prefer transaction speed to security verification, based on early findings of industry research, media reporting, and data on security incidents. Most common behaviors, which have been reported many times, are sharing of authentication credentials with people whom you trust (family members, business partners), routinely neglecting transaction review screens to save time, and using PIN based on personal information (birthdays, phone numbers, identification numbers), which is easily guessed [45]. Security concerns are on the upsurge, such as advanced phishing attacks that take advantage of user confidence and social engineering techniques that play on the customer's desire to have a fast transaction. By 2024, the Bangladesh Bank had registered more than 12,000 cases of fraud on MFS platforms, and the total financial damage had been estimated at more than BDT 850 million [Bangladesh Bank, 2024]. This is a twenty-three percent growth over the last year, as the security issues in the fast-growing digital financial environment continue to rise. These numbers highlight the demand to conduct empirical studies on the behaviors of users who could pose security threats.

Although the previously noted behavioral patterns minimize the mental load and shorten the time spent on transactions, there are high susceptibility areas that can be utilized by the malicious. Nevertheless, these behavioral patterns have not been sufficiently measured in previous studies, nor has this been empirically demonstrated to relate to usability factors, such as perceived ease of use and speed preferences [50]. None of the MFS providers or governments can make well-informed and evidence-based choices about how to trade off user experience optimization and critical security needs without reliable empirical data regarding the actual behavior of users, and not speculation.

Practically, this knowledge of such relationships may help designers create MFS interfaces that make use of data-driven methods to strike a skillful tradeoff between security and usability. Rather than traditional security solutions that may annoy users during every transaction or interfaces that are too easy to use to the detriment of security, evidence-based design approaches can include dynamic and context-based security controls [27]. These methods may involve risk-based authentication where security requirements are varied according to the context of the transaction (amount, recipient, location, time, and device), progressive disclosure of security knowledge, which helps users without overloading them with technical information, and context risk indicators, which cause no material disruption to workflows but alert users to possible security dangers.

The theoretical motivation is rooted in the fact that the current technological acceptance models cannot accommodate security-sensitive applications, especially in high-frequency transaction scenarios. The perceived ease of use and the perceived utility were the major determinants of uptake and continued use in classical TAM [4]. The time dimension of the interactions of users remains a poorly researched aspect, and whereas the dimensions of trust and perceived risk have been integrated into a number of extensions, they measure perceptions instead of actual actions [25].

Users can complete tasks faster, which has been operationalized as a measure of swiftness in this study but has not been addressed with much systematic focus, though it is clear that this is important in high-frequency transaction scenarios where users have to complete numerous operations in a day [32]. The users who make dozens of transactions weekly might become strongly oriented to the speed of completion, which nullifies the importance of the security considerations, despite the fact that such a dimension has not been directly featured in technology acceptance frameworks as a specific construct with significant effects on behaviors.

This study tries to fill these theoretical and practical gaps by operationalizing risky behavior as a quantifiable construct separate from perceived risk, introducing swiftness as a direct variable that measures speed preferences in transaction completion, and empirically investigating the relationships amongst these variables to known constructs of the TAM using strong statistical tools. The primary objective is to provide empirical evidence that will be useful in advancing the theories in the study of technology acceptance and its practical implementation in the design of mobile financial services, which will eventually lead to safer financial technology that will not lead to loss of user satisfaction.

1.3 Problem Statement

A critical knowledge gap still exists as to how usability features, especially speed and ease of use, can make people adopt risky behavior that puts their financial security at risk continuously, yet mobile financial services have been extensively utilized and have produced a transformational effect in Bangladesh. Recent studies of MFS are mainly focused on adoption objectives and risk perception instead of examining real risk behavior by analyzing user experience with financial sites [24], [33]. This state of research gap poses a great challenge to MFS providers and interface designers when these two competing goals (i.e., high security implementation and enhancement of user experience) are concerned in the context of the lack of suitable empirical support.

It is an intrinsically complicated issue with many other factors that are connected to it. To begin with, the conventional Technology Acceptance Model applications fail to address the speed aspect of user-interaction, which has grown to be more crucial in frequency-based financial dealings as customers anticipate almost real-time turnaround [4]. The users expect transactions to take a few seconds, and even minor delays caused by the need to make required security checks cause friction, which can lead to abandoning the adoption or creating workaround behavior, which often undermines security. Nevertheless, recent studies on TAM mainly focus on usability through the prism of the ease of use instead of explicitly assessing how temporal efficiency influences the initial adoption choices and future usage patterns.

Second, perceived risk and actual risky behavior denote different constructs that may not necessarily correlate, regardless of the fact that the majority of studies measure perceptions through the self-report measurement tools and not through observable behaviors [26]. A user can share PINs even when s/he realizes that sharing threatens his/her security based on his/her convenience, time, or even necessity. Equally, the users can report serious concerns over the security in the survey forms, but often fail

to do security checks in the practical use environment. Attitude and risk perception studies alone can often create a distortion of the actual security process and do not help to establish the actual causes of the activities that endanger security due to this perception-behavior gap.

Third, it is still challenging to quantify the relationship between usability-driven design features and security-compromising user behavior, making it impossible to make evidence-based interface design decisions with measurable outcomes [14]. MFS providers make crucial design choices on a daily basis, such as how to strike a balance between transaction speed and security review opportunities, whether to permit biometric authentication as a stand-alone security mechanism, how many authentication steps to include in login flows, and whether to require OTP verification for all transactions or just those that exceed specific thresholds. However, these judgments are made in the absence of reliable empirical evidence about how specific design choices consistently affect user security behaviors. Due to the lack of quantitative data linking specific usability characteristics to quantifiable security effects, design decisions must unavoidably rely on intuition, industry customs, or user satisfaction metrics that may overlook significant security implications.

MFS providers may inadvertently offer user experience enhancements that unintentionally encourage risky behaviors at scale. For instance, one-tap transaction confirmations may increase user satisfaction scores and completion rates, but they may also increase the amount of fraudulent transactions that users approve without carefully examining the transaction details. Users may become less watchful and more vulnerable as a result of smooth, flawless experiences that give them false trust in system security. When apps are regularly easy to use, and transactions flow swiftly without security disruptions, users may internalize incorrect assumptions that the system is inherently secure against all threats. Because of this complacency, consumers are more susceptible to phishing attempts, social engineering attacks, and other human-centered exploitation techniques.

Moreover, during the design and execution of security, it wasn't possible to properly take into account the usability factors that influence the compliance of the user to the security measures in the practical usage context [49]. In spite of the fact that multi-factor authentication is theoretically and technically sound, sometimes users might bypass it because it is too cumbersome. To avoid this, users might come up with unsafe workarounds that greatly compromise the security benefits that these techniques are intended to offer, e.g., storing OTPs in unprotected note apps, forwarding SMS to common devices, or writing down authentication codes. Luckily, the designers will not be able to develop mechanisms that the users will follow regularly and properly unless these designers understand the effects of speed preferences and ease of use on the security protocol measures among the different classes of users.

There is also the possibility that legal regulations and system security in the MFS are never in unity with the ability and realities of user activities [40]. When regulations or standards requiring particular security attributes fail to address the implications on usability and reaction to user behavior, the consequences are that the user unwillingly opts for non-conforming workarounds, alternative financial solutions that are not permitted, or they altogether reject electronic financial services and switch

to less secure channels. Nonetheless, regulations that put usability and accessibility before sufficient security considerations can unintentionally introduce structural vulnerabilities that place the lives of whole user communities at risk of exploitation.

It is more importantly critical and contingent in the developing nations of the globe, including Bangladesh, where MFS is employed by vastly heterogeneous people with radically different digital literacy, economic, and cultural backgrounds in the context of financial services [48]. An effective design solution and security solution applied to well-educated urban users will not be efficient and effective with rural users who might lack the necessary technology skills and have a different mental model of what digital security is all about. The security systems that presuppose some basic knowledge, behavioral patterns, or risk perceptions can be inefficient or even harmful in the case when users can be described as having fundamentally different constructs of meaning and management of digital security.

Based on an enlarged TAM concept emphasizing on a specific integration of usability and behavioral security concepts, this paper quantitatively examines the degree of swiftness preferences and perceived ease of use versus risky behaviors amid MFS users in Bangladesh. The study attempts to give evidence that may guide interface design decision-making processes, security policy formulation, and user education programs towards strategies that effectively balance usability, speed, and security in a manner that is both theoretically well supported and practically achievable through defining empirical relations between the three variables through the use of rigorous statistical analysis.

1.4 Research Objectives

The primary objective of the study is to quantitatively explore and verify the relationships between risky behavior and usability factors (perceived rapidity and convenience of use) among the Bangladeshi mobile money users. This general purpose is operationalized by six detailed research objectives, which methodologically cover different facets of the study topic:

Objective 1: Behavioral Characterization and Measurement

To measure and systematize the risky practices of MFS users in Bangladesh, such as the trends of poor verification of transactions, ineffective authentication practices, and sharing of credentials. In order to establish empirical baseline data on the security behavioral landscape that has been largely unrecorded in previous research, this objective aims to quantify the prevalence and distribution of security-compromising behaviors throughout the user community [45].

Objective 2: Validation of Core TAM Relationship

to measure the correlation between perceived usefulness (PU) and perceived ease of use (PEOU) with respect to MFS apps utilized by Bangladeshi customers. In order to determine whether the fundamental relationship between usability perceptions and functional value assessments is as strong in financial technology contexts as it is in other technology domains, this objective validates the TAM relationship in the particular context of mobile financial services [4], [24].

Objective 3: Security as a Value Proposition

To measure the correlation between perceived security (PS) and perceived usefulness (PU) in order to comprehend how functional value assessments in financial technology contexts are influenced by security perceptions. In order to determine whether financial technology contexts necessitate treating security as a core value proposition rather than just a background concern, this objective looks at whether security plays a crucial role in how users assess the utility of MFS applications [25], [26].

Objective 4: Core Hypothesis Testing

To determine the statistical significance and practical magnitude of the association between swiftness preferences (SWF) and hazardous behavior (RB) among MFS users through empirical testing. This is the main contribution of the study, which examines whether the need for quick transaction completion consistently motivates security-compromising actions and, if so, quantifies the strength and impact of this relationship on security outcomes.

Objective 5: Upstream Driver Identification

To investigate whether swiftness preferences (SWF) are positively impacted by perceived ease of use (PEOU), as well as whether streamlined interfaces consistently promote speed-oriented user behaviors and higher expectations for quick engagement. In order to determine whether usability improvements unintentionally generate temporal expectations and preferences for quick completion that could subsequently jeopardize security, this goal looks into the upstream elements that influence swiftness preferences [27].

Objective 6: Evidence-Based Design Recommendations

To develop experimentally validated, evidence-based recommendations for MFS interface design to effectively balance security, speed, and usability based on the use of contextual risk indicators, dynamically authenticating designs, and theoretically-founded design principles. This objective will make sure that the research results have a substantial practical influence through translating the empirical results into practical recommendations to the practitioners, incorporating theory and practicality [14].

These objectives combined address the research problem in a multi-faceted manner, considering the influence of usability on security behaviors and those practical implications of the study that can minimize risks without compromising the quality of the user experience.

1.5 Key Research Contributions

The contributions to the literature of technology acceptance modeling, behavioral security, and mobile financial services design in this study are categorized as follows:

1. **Theoretical Contributions**

   Extension of the Technology Acceptance Model (TAM): Swiftness (SWF) and Risky Behavior (RB) are two new constructs added to the existing

TAM. Unlike past extensions focused on perceptual variables like trust and perceived risk, this study operationalizes behavioral security as a measurable variable. By shifting the focus to observable security-compromising behavior, this represents a significant theoretical enhancement of TAM's application to security-related scenarios.

Conceptualization of Swiftness as a Distinct Construct: Unlike literature, which perceives speed as a sub-construct of usability or perceived ease of use, this study supports swiftness as a construct on its own according to the display of preferences by users towards speedy transactions. This difference allows for the more efficient modeling of time efficiency on behavioral patterns, excluding the confounding influence of general usability beliefs.

Empirical Quantification of the Usability-Speed-Risk Pathway: The study offers, for the first time, empirical data of the mediated relationship between perceived ease of use, preferences to speed, and risky behaviors ($PEOU \rightarrow SWF \rightarrow RB$). With Structural Equation Modeling (SEM), the quantification of effect sizes and confidence intervals may be performed and used to make evidence-based interface design choices.

2. **Methodological Contributions**

Behavioral Measurement Instruments: The researchers design and provide psychometric validation of measures in order to measure actual risky behavior (e.g., credential sharing, weak authentication, verification skipping, and phishing susceptibility) as opposed to perceived risk or behavioral intentions. This fills a major loophole in the behavioral school of security studies.

Context-Specific Validation in Emerging Economies: The paper gives tested measurement tools and structural equations to suit new market settings, whereby the demographic factors, the level of financial literacy, and cultural values vary greatly in the developed economies.

3. **Practical Contributions**

Evidence-Based Design Guidelines: The study elicits empirical evidence to MFS providers on the specifications of operational designs, risk-based authentication models, context-based security indications, and friction-suiting interface techniques. These guidelines also associate particular usability features with quantifiable behavioral results.

User Segmentation for Targeted Interventions: Targeted Interventions: The study shows that the speed and risky behavior are different in each demographic (age, education, frequency of a transaction) by identifying user risk portfolios. These results allow individual security training and interface specifics.

Policy Implications for Financial Inclusion: Financial Implications of Policymaking on Financial Inclusion: The security-usability-speed triangle analysis offers regulators a guide on how to balance between innovation and consumer protection, especially in situations where MFS is used as the main financial tool amongst the underbanked citizens.

It is expected that this combination of contributions will enhance both theory and practice regarding *secure-by-design* principles in mobile financial services and other security-sensitive digital platforms operating under resource constraints.

1.6 Research Questions

The operationalized theoretical framework is used in a methodical way, and the methodical approach of the proposed research addresses the following research questions that guide the empirical research:

RQ1: Characterization of behavior

Which specific risky behaviors do MFS users in Bangladesh have, and which activities of risky behavior are practiced by the users of MFS across the different user groups, depending on their experience level, use patterns, and demographics? Identifying the most prevalent dangerous behaviors, whether they are distributed systematically depending on user attributes, and the distribution of risk-taking behavior in the user population at large, this question would describe the behavioral security environment completely.

RQ2: Usability-Value Relationship

What is the scale and statistical significance of the correlation between the perceptions of the utility of MFS applications and the perceived ease of the Bangladeshi users? To establish the significant effects of usability perceptions on functional value judgments and measure the intensity of the effect, this question will explore the strength of the basic TAM relationship in the MFS setting.

RQ3: Security-Value Relationship

How do security perceptions relate to usability perceptions in overall value judgments and how does the perceived security influence judgments of users of MFS usefulness? This question investigates the existence of security as one of the key value propositions in financial technology, whether its influence on usefulness ratings is comparable, superior, or inferior to the influence of the usability attributes, and the interaction between the two mechanisms.

RQ4: Speed-Risk Relationship (Core Question)

Is the need/want to use transactions quickly a strong predictor of the tendency to engage in risky behaviors, and what is the size, direction, and practical implications of this relationship? This is the primary research question, which will examine whether speed preferences are a serious and consequential determinant of security-compromising behaviors and measure the intensity of the relationship to be used in the development of an intervention.

RQ5: Usability-Speed Relationship

How far, how, and what is the practical value, and can the tendency to make transactions fast be greatly predictive of the tendency to engage in dangerous activities? It is the primary research question, and it will be tested whether the speed preferences are a meaningful and consequential cause of security-compromising behavior,

and will measure the extent of this relationship to determine how to design the interventions.

RQ6: Design Principles and Interventions

Based on the empirical relationships identified in this study, which design principles and interface interventions can effectively balance usability, speed expectations (swiftness), and security in Bangladeshi MFS systems—reducing swiftness-driven risky behaviors without undermining perceived usefulness and overall user experience?

This question translates the validated behavioral mechanism (swiftness → risky behavior) into actionable design guidance. It examines how MFS platforms can introduce risk-proportionate safeguards (e.g., adaptive friction, contextual security cues, and segment-sensitive interventions) that control speed-driven shortcuts while preserving usability and perceived value for routine, legitimate transactions.

All the study questions outlined above are supposed to be theoretically justified, experimentally justified by quantitative methods, and practically significant to the stakeholders, including MFS providers, interface designers, policymakers, and users themselves.

1.7 Scope, Constraints, and Challenges

This paper has the tenacity of scope to provide analytical depth, as well as the systematic coverage of key methodological considerations. The scope of the research is chosen to address the usability-security trade-off for the specific study population, which is Bangladeshi MFS users, with behavioral outcomes as the subject of study, instead of technical security practices and platform specifics. The narrow-purpose design allows for its strict quantitative analysis and preserves the practical application to interface design decision-making.

Geographical Scope

The research is confined to Bangladesh and concentrates on the clients of the leading MFSs in the country. Even though this geographic focus ensures that findings can be directly applied to a specific ecosystem and applied to gain deep contextual insight, it inevitably limits the overall ability to generalize the results to other national settings with different regulatory frameworks, cultural norms, economic situations, and technical infrastructures. However, the theoretical framework and practical approach presented here can be used by other developing countries that have similar financial technology ecosystems and challenges.

Population Scope

The target population is made up of active MFS users aged 18 years and above who have conducted at least one transaction within the three months before taking part in the survey. This research compiled information on 707 participants during the period August 2025 to October 2025, and there were 89.38 million active users of MFS in Bangladesh. Following the rigorous data cleaning procedures, 703 valid responses were achieved. To ensure that it is representative enough and to be able to investigate how the associations are different between the attributes of the user,

the sample includes users who represent a wide range of demographic groups, such as age, education, income, geographical location, and others.

Construct Scope

The five key characteristics that have been operationalized on the basis of validated multi-item scales are Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Swiftness (SWF), Risky Behavior (RB), and Perceived Security (PS). Other demographic variables, including age, gender, education level, monthly income, geographic area, and MFS using experience, are presented as contextual factors in case the moderation studies are to be conducted, and multi-group comparisons are to be made. It is this targeted construct set that allows maintaining analytical tractability and enables making depth of measurement possible.

Methodological Scope

The research design is a quantitative study design based on the cross-sectional survey design and validated measuring instruments that have been adapted to the previous research and tailored to the MFS environment. The data cleaning, preprocessing, and transformation are carried out using Python 3.9, the descriptive statistics, reliability assessments, and preliminary analysis are conducted using SPSS 28.0, whereas the proposed relationships are tested using AMOS 26.0. Despite the fact that it does not enable tracking behavioral changes during a specific time, the cross-sectional approach enables a strong measure of hypothesized correlations, as it is able to measure perceptions and self-reported behaviors at a specific time.

Behavioral Scope

Frailty or foreseeable authentication credentials based on personal data (birthdays, phone numbers) or simple codes (1234, 1111); (1) sharing PINs or passwords with trusted people to facilitate a transaction; (2) clicking on unverified links or attachments purporting to be MFS applications; (3) always following a speedy transaction completion rather than following security guidelines; and (5) invariably having a tendency to follow the preferred action of making transactions, as opposed to adherence to security measures, are all risky. A rigorous literature review, engagement with industry stakeholders, and initial qualitative research identified the following behaviors as typical and secondary security risks in the MFS environment.

Temporal Scope

In this cross-sectional study, the user views and self-reported behaviors were documented during the period of August-October 2025 as the survey was administered. The selected period was well selected as it was to record a stable usage trend once MFS adoption had gone normal after the COVID-19 lockdowns, when the usage had reached a stable point, though longitudinal behavioral tracking would provide more information on how behaviors change.

Technology Scope

The study concentrates on smartphone-based MFS applications as opposed to USSD-based services or feature phone implementations. Such focus is based on the fact that app-based services comprise most of the transactions in Bangladesh and offer much richer interface design solutions, which are relevant to exploring trade-offs

between usability and security. More sophisticated security functions and user interactions that are needed in the questions of the study are also possible with app-based systems.

Constraints and Limitations

The research acknowledges several methodological weaknesses that affect the meaning of the findings. To start with, self-reported data on behavior is vulnerable to social desirability bias, the problem of which consists of the willingness of respondents to report socially undesirable behavior. Even though measurement procedures included the softening of language and nonjudgmental framing to minimize this bias, survey methodology is incapable of eliminating this bias entirely.

Second, the limitation on causal inference is also inevitable, as the research design does not permit the longitudinal monitoring of behavioral changes or experimentation with the features of the interface. A cross-sectional approach is incapable of either establishing causality or dismissing reverse causation or unmeasured confounding variables, although hypothesized causal linkages can be tested using structural equation modeling.

Third, real fraud incidents and technical security vulnerabilities (including the security of the code, encryption, and security of the infrastructure) are not measured. Instead of concentrating on technical issues, the research still points to user behaviors as a cause of security risks that are caused by human factors. The reason behind this limitation of the scope is that behavioral security is a distinct and understudied condition of MFS security.

Fourth, even though the users located in various regions of Bangladesh are represented in the study, the selection of the sample primarily relied on urban networks and Internet-based methods of recruitment, which could have not captured the rural users with different patterns of use and a lower level of digital access. This sample bias was not achieved because not all the demographic variables were fully represented, but this is known and solved with the help of specific recruiting strategies aimed at different sectors.

Fifth, rather than focusing on platform-specific behaviors, the study looks at generic behavioral patterns across MFS platforms. Although platform-specific security features and interface designs may result in subtle variances not reflected in general measurements, a preliminary study indicated that behavioral patterns were mainly constant across major providers (bKash, Nagad, Rocket), supporting this aggregation.

Challenges and Mitigation Strategies

During the execution of the research, a number of difficulties were found and methodically resolved. Targeted outreach through community groups and professional networks with a rural reach was necessary to recruit a variety of user segments through online channels, especially rural and less educated consumers. Extensive pilot testing, iterative question wording modification for clarity, and the use of attention checks to detect inattentive responses were all necessary to ensure data quality from respondents with different levels of digital literacy.

Questionnaire design techniques, such as construct item randomization, varied re-

sponse formats when appropriate, and ex-post statistical testing (Harman's single-factor test) to determine whether common method variance systematically inflated relationships, were used to manage potential common method bias inherent in single-source survey data.

Despite such limitations and challenges, the research is important in that it provides the first comprehensive empirical investigation of the connections between swiftness and risky behavior within the context of Bangladeshi MFS, generates validated measurement instruments of new constructs (primarily swiftness), and provides sound empirical data that impact both theoretical and practical progress.

1.8 Research Methodology Overview

The quantitative and theory-testing methodology applied to this study relates to the positivist tradition of epistemology and is founded on the assumption that constructs have objective relationships that can be measured with the help of methodical empirical studies (Creswell & Creswell, 2018). The method consists of a series of interrelated components that are supposed to be cautious in verifying suggested connections and maintaining scientific integrity.

Theoretical Framework

Besides the traditional TAM constructs (Perceived Usefulness, Perceived Ease of Use), the researcher implements the concept of perceived security, which is relevant to the domain, and introduces two new constructs, Swiftness (SWF) and Risky Behavior (RB). The wider paradigm enables the investigation of the impact of the usability traits on value perceptions and behavioral security outcomes both directly and indirectly.

Data Collection

Primary data were collected with the help of a structured online survey between August and October of 2025 with the help of Google Forms among 707 MFS customers in Bangladesh. The survey tool contained items related to the patterns of usage and demographics, besides the previously tested multi-item scales assessing every construct through 5-point Likert scales. Although the authors acknowledge the natural limitations of non-probability sampling to make statistical generalizations, sampling approaches like purposeful and snowball sampling were employed to maximize demographic diversity.

Analytical Framework

Complementary statistical methods were used in several levels of data analysis. The sample and variable distributions are described via descriptive statistics. By evaluating construct reliability, convergent validity, and discriminant validity, confirmatory factor analysis verifies the measurement model. Equation of Structure Modeling provides path coefficients, significance levels, and model fit evaluations when testing hypothesized correlations between constructs. Additional analyses look at latent class structures in behavioral patterns, moderation by demographic factors, and mediation effects.

Software and Tools

Data transformation, preparation, and cleaning were accomplished using Python 3.9. Descriptive statistics, reliability evaluations, correlation analyses, and exploratory research were carried out using SPSS 28.0. AMOS 26.0 used the maximum likelihood estimate for Confirmatory Factor Analysis and Structural Equation Modeling.

Quality Assurance

Data quality and analytical rigor were guaranteed by several processes: 30-user pilot testing improved the clarity of the instrument; attention checks found inattentive respondents; completion time monitoring identified suspiciously fast responses; duplicate detection stopped multiple submissions from a single person; and thorough data cleaning addressed missing data, outliers, and violations of assumptions.

Ethical Compliance

In the course of the research, informed consent of every respondent was received, the respondent's anonymity was maintained during the data collection process, and data protection measures helped to keep the information confidential.

This is a methodological system that produces empirical data that can be immediately applied in the practical design and policy making in the field of MFS, thereby facilitating the testing of theoretical hypotheses in a rigorous manner.

1.9 Thesis Organization

The six major chapters, which constitute this thesis, are carefully organized in such a way that they slowly unfold the study story, beginning with problem identification and moving on to empirical research and workable conclusions and prospects.

Chapter 1: Introduction sets the background of the study, presenting background information on mobile financial services in Bangladesh, giving a clear picture of the problem and motivation of conducting the research, specifying the specific research questions and objectives, and describing the scope of the study, its limitations, and challenges. This chapter reveals why this study is required, the objectives of the study, and the contribution it will make to the theoretical and practical knowledge.

Chapter 2: This richly themed synthesis of the literature provides a thorough review of the research and usability-security trade-offs, the adoption of mobile financial services, behavioral security, the impact of digital literacy, and aspects of adoption determined by context are all provided in Chapter 2. The chapter builds up theoretical foundations and the intellectual significance this research would bring to the field by systematically surveying the related previous research, pinpointing major gaps in research by comparative analysis, and locating this study within the existing body of scholarly debate.

Chapter 3: Design and Needs of the Research elaborates on the research design from different angles required to have an in-depth assessment. The chapter introduces the theoretical framework and the development of the hypothesis, explains how the project will be planned, risk management strategies, explains the economy of the research carried out, and potential interventions, assesses the environmental and sustainability issue, and considers how the societal impacts will be viewed, final specification and requirements, and systematically assesses the ethical point.

Chapter 4: Design process overview, survey instrument design and development process, data collection strategy and implementation, analytical framework design, defining statistical techniques and validation processes that ensure quality of measurement are all discussed in detail in Design Methodology. There is sufficient methodological information presented in this chapter to enable a critical evaluation of the rigor of the research and to facilitate potential extension or replication.

Chapter 5: Analysis, Assessment, and Outcomes systematically gives empirical results using different analytical lenses. The performance evaluation framework is outlined, the analysis of the measurement model is used to support the construct reliability and construct validity, the structural model is tested to test the hypothesized relationships, the results of the statistical analysis and hypothesis test are reported, the comparative analysis is conducted to examine the relationships between the user segments and the discussions based on the empirical evidence are made to recommend the design arrangements.

Chapter 6: Conclusion and Future Directions summarize the research contributions, discusses theoretical implications on TAM and behavioral security literature, describes practical implications to different stakeholder groups (MFS providers, designers, policymakers, and users), identifies research limitations and their implication on the interpretation, gives specific recommendations of future, research based on the same foundation, and comments on the research findings.

The thesis is included after the main chapters and also has a comprehensive reference list. The survey instrument in its entirety, further statistical outputs endorsing the primary chapter analyses, ethical approval documentation, and project timeline documentation materials, including Gantt charts, are found in its appendices.

This organizational structure ensures a logical development from problem identification through rigorous empirical study to practical findings while adhering to accepted rules for engineering and computer science theses. Every chapter builds methodically on the one before it while retaining enough autonomy to allow readers interested in certain topics to interact with each chapter in a meaningful way.

Chapter 2

Literature Review

2.1 Introduction

Mobile Financial Services adoption, usage, and behavior patterns have been widely explored by various theoretical models, with the Technology Acceptance Model being an underlying paradigm that has been repeatedly proven and applied under various technological settings [4]. This literature review will integrate the current academic literature on MFS adoption dynamics, usability-security trade-offs in financial technologies, and behavioral security practices to define the theoretical basis that supports the current research study, in addition to providing gaps that warrant the current empirical research.

The review is structured thematically in seven interrelated areas that give rise to the research problem and methodology as a whole. To begin with, technology acceptance in mobile financial situations focuses on how technology acceptance has already been deployed and justified, and expanded specifically to financial technologies to create a base of knowledge about the factors leading to adoption. Second, security perception and trust: examination of the impact of security judgments and institutional trust on adoption decisions and continuance usage behavior is conducted. Third, the usability issues and user behavior explore the design properties of interfaces and how the characteristics of the interface design influence the usage patterns and behavior. Fourth, there is the usability-security trade-off, which looks at the underlying dilemma of convenience versus protection that designers have to face. Fifth, behavioral security and risk-taking reviews Empirical research on the objective risky behaviors and not just perceptions. Sixth, digital literacy and cybersecurity awareness determine how knowledge by users moderates security-usability links. Seventh, contextual factors in Bangladesh specifically analyze peculiar environmental factors that form the basis of MFS use in the study environment.

This is a review of the literature that includes about 30 major academic publications that were published during 2017-2025, which means that the study includes up-to-date information regarding the technological possibilities, user demands, and threats to security. The review presents regular patterns as well as reveals serious gaps that are filled by this research: namely, the scarcity of empirical measurement of real risky practices (as opposed to perceptions), the lack of explicit inclusion of the concept of speed/swiftness as a specific theoretical construct, and the lack of context-specific

studies within developing economies such as Bangladesh, where distinctive cultural, economic, and infrastructural conditions determine the technology adoption and usage.

2.2 Theoretical Foundations: Technology Acceptance Model

The Technology Acceptance Model (TAM), developed by Davis **davis1989**, provides the foundational framework for understanding technology adoption decisions. TAM proposes that two cognitive beliefs, *Perceived Usefulness* (PU) and *Perceived Ease of Use* (PEOU), are primary determinants of technology acceptance and subsequent usage behavior.

Perceived Usefulness is the beliefs that users have that a system can improve their performance and productivity in the tasks. **Perceived Ease of Use** reflects the evaluation of users on the mental effort needed to use the system. The essence of **TAM** proposition is that an easy-to-use system is one that is perceived to be easy to use, and thus, **less cognitive effort** is needed, leading to an increase in the **perceived usefulness** which motivates positive attitudes, behavioral intentions and actual use.

Within the mobile financial services setting, **TAM** has always been confirmed by the scholars and the model extended to include domain-specific aspects of financial technologies, especially **trust, security, and risk perception** [25]. **Hossain et al.** [24] established that the **perceived usefulness** is a strong predictor of adoption intentions ($\beta = 0.48, p < 0.001$) in mobile commerce in Bangladesh, and **perception risk** has a strong negative effect ($b = -0.32, p < 0.01$). It proves that the adoption choices in the financial context are made with a parallel evaluation of the **functional benefits** and the **problem of security**.

Incorporating **TAM** with **Innovation Resistance Theory**, **Rahman et al.** [33] found that, even though **Perceived Usefulness** ($b = 0.41$), **Perceived Ease of Use** ($b = 0.36$), and **Perceived Trust** ($b = 0.29$) have a positive effect on the attitudes towards using MFS, **risk-related barriers**, **security concerns**, **fear of financial loss**, and **technological uncertainty** adversely affect attitudes ($\beta = -0.38$) and usage intentions ($\beta = -0.24$). This two-sided view of vision proves that successful promotion of **MFS** needs to increase perceived benefits as well as resolve the **resistance factors** in a systematic manner.

The evidence of the emerging economies in the recent past supports the cross-cultural applicability of **TAM** with significant **moderating factors**. According to **Islam et al.** [47], dimensions of **speed and reliability**, which are attributes of **system quality**, have significant effects on usage intention ($\beta = 0.43, p < 0.001$), and significant **gender moderating effects**. **Female users** demonstrated greater sensitivity to **system quality** ($\beta = 0.51$ vs. 0.36 for males), while **male users** weighted **perceived usefulness** more heavily ($\beta = 0.47$ vs. 0.33 for females).

These extensions demonstrate that mobile financial services adoption is determined by multiple interacting factors beyond the traditional usefulness-ease of use dyad. However, existing TAM literature focuses predominantly on adoption intentions and

perceptions rather than actual usage behaviors and security practices, a gap this research addresses.

2.3 Security and Trust in Mobile Financial Services

Security perceptions and institutional trust have become important predictors of mobile banking and MFS adoption choices that tend to act as moderators or mediators, intensifying or weakening the impacts of usability factors on behavioral intentions and actual use [26].

Khan and Amin [26] particularly concentrated on the security aspects of dimensions that influence the adoption of mobile banking in Bangladesh as an extension of TAM by integrating methodologically with Principal Component Analysis to reduce dimensionality and logistic regression to predict. Their study indicated that the perceived security is critical and cannot be substituted in the willingness of consumers to adopt mobile banking to carry out financial transactions, with the users rating perceived security as a significant factor ($oddsratio = 2.34, p < 0.01$). In particular, perceived high security indicators of visible encryption, clear two-factor authentication, and transparent security policies were rated highly and 2.34 times more likely to adopt mobile banking than users with low security perceptions, even after other factors of adoption, such as usefulness and ease of use, were controlled.

This observation places security as a technical necessity or a background characteristic, but as a core value proposition to mobile financial services, especially in emerging markets, where institutional cybersecurity facilities might be viewed as relatively undeveloped compared to developed economies and where trust in digital financial facilities is weak. The scale of security impact indicates that even the most usable applications with rich features might not gain mass adoption when there are security concerns among the users, and security communication and demonstration are considered strategic requirements and not common compliance regulations.

Baabdullah et al. [25] developed a complex theoretical model that incorporates both TAM and the aspects of the Unified Theory of Acceptance and Use of Technology (UTAUT) and the specifics of perceived security, privacy protection, and institutional trust. Their Structural Equation Modeling result of 295 mobile banking users in Saudi Arabia indicated that the perceived security ($\beta = 0.31, p < 0.001$) and perceived privacy ($\beta = 0.27, p < 0.001$) were essential independent predictors of their continued mobile banking intention and actual usage behavior, whose effects extended beyond and in addition to the core factors of usability.

High perceptions of security and privacy have a positive relationship with usage intentions, which means that the concern regarding information safety, the integrity of transactions, and data confidentiality affect the adoption choices regardless of moderate or high usability. The mediating variable ($indirecteffect = 0.18, p < 0.01$) that facilitates the transformation of positive perceptions of usability into actual sustained use is trust, which implies that in the financial technology setting, unlike less productive but mostly universally applicable productivity applications, security and privacy cannot be considered a secondary consideration and, instead,

they have to be included as core value propositions that directly influence whether users gain utility through technological capabilities.

The research by Lallie et al. [49] is thorough and based on UTAUT2 with extensions of security, risk, and trust constructs, and surveyed 315 mobile banking users and tested the hypothesis with the help of Covariance-Based Structural Equation Modeling. As they have found out, demographic variables, especially income and age, play a significant role in their moderating effect on the extent to which the users consider security requirements relative to the ease of use (effort expectancy) in their calculation of the adoption.

Security perceptions were found to have a significant influence on adoption decisions among older users (45+ years; $\beta = 0.44, p < 0.001$) but a smaller influence among the young users (18-34) ($\beta = 0.22, p < 0.01$), and effort expectancy played a stronger role when compared to younger users ($\beta = 0.51$ among young users and $\beta = 0.31$ among older users). Income earners were more willing to use more complicated security measures, which they felt were more suitable to protect valuable financial resources, and lower-income earners preferred easier-to-use interfaces despite expressly recognizing that they were dealing with insecure situations, potentially because time is a more significant factor, with work schedules being a limitation on transaction speed.

The authors found that institutional trust, trust in the overall competence and benevolence of the financial institution, is a decisive mediator between the perceived security features and the behavioral intention ($indirecteffect = 0.24, p < 0.001$). This implies that the intention to use security measures is heavily based on the trust that users have in the institution that introduces the security measures. The security measures provided by trusted institutions are seen as cues of protective competence, whereas the same measures provided by less-trusted providers might be seen as unnecessary barriers that are driven by an institutional motive instead of protecting the users.

In their study, Adrian-Tupas and Mendoza investigated the moderating role of trust in the relationship between performance expectancy and adoption through the survey of 518 mobile money users. Their results showed that concerning the paradoxical trend: within the environment of high levels of trust, the user forms a sense of complacency, which results in the negligence of performance discrepancies and an ordered neglect of system warnings. High institutional trust users (as measured by agreement with statements such as I trust my mobile money provider completely) were much more likely to skip transaction checks ($\beta = 0.34, p < 0.001$) and disregard security warnings ($\beta = 0.29, p < 0.01$) than users with medium levels of institutional trust.

This blindness of trust then results in the development of risky habitual patterns where users avoid the security checks due to the implicit trust in the system, and this creates the vulnerability of fraud once the trust is compromised by the attackers posing as legitimate institutions. The researchers found that the users who supported statements like I trust the system enough not to read the security warnings were 3.2 times more likely to perform risky behavior like sharing credentials and using weak PINs (odds ratio = 3.2, 95% CI [2.1, 4.8], $p < 0.001$).

This result implies that too much trust without the necessary critical consideration creates a paradoxical security weakness; the same institutional trust that allows initial adoption and continues to be used may also lead to weakened security practices among habitual users who have come to develop unwarranted belief in system infallibility. Security education can thus be required to foster trust with verification as opposed to blind trust, which, in particular, requires users to adopt protective behavior even when utilizing trusted services.

Ali et al. [29] examined hedonistic motivation as a mediating variable between trust and perceived risk based on Structural Equation Modeling of a survey. Their results have shown that the pleasure obtained as a result of the use of a digital financial application (measured with the items that estimate pleasure, fun, and positive affect during use) decreases the perceived salience and seriousness of security risks (mediation effect = -0.21, $p < 0.01$). Users with high hedonic motivation also scored much lower on perceived risk measures despite the experimental vignettes showing the same level of security threat information, indicating that the development of positive effective reactions to visually appealing interface design can lead to hazardous overconfidence in system security.

Users in flow states or enjoying the experience of using financial applications were much more prone to discount or ignore security warnings ($\beta = 0.28, p < 0.01$); hedonic motivation partially mediated the relationship between trust and risk perception. Ali et al. hypothesize that aesthetically pleasing, enjoyable interfaces cause positive affect to produce cognitive spillover so that good feelings about the interface inappropriately spill to security assessments, which causes users to underestimate threats. This process implies that very smooth, pleasant user experiences, though advantageous in adoption and satisfaction, may need counter-measures in terms of security to avert complacency due to the effects.

All these studies show that perceptions of security and institutional trust and effective responses are interrelated in a complex web that helps to affect initial adoption decisions as well as continued security behavior. The factors, however, have been the focus of most studies, but in connection to adoption intentions as opposed to real security-compromising behavior when used in normal contexts. Little has been done on the relationship between trust-induced complacency and certain risky actions and the issue of whether interface usability features that elicit positive affect could indirectly decrease security vigilance via hedonic processes that circumvent rational risk evaluation.

2.4 Usability Factors and User Behavior Patterns

Although the perceptions of security affect the decisions to adopt the technology and the formation of an initial trust, the usability factors essentially determine the continuity of usage, behavioral patterns, and user preferences that will remain the same during the life-cycle of the technology [37]. Various empirical studies have investigated the impacts of perceived ease of use and corresponding usability constructs on user behavior in mobile financial settings in which there are complex relationships between interface design and security practices.

The study that compared user-perceived security of mobile banking applications in

terms of integrated UTAUT2 and TAM constructs revealed that perceived security is a significant predictor of the behavioral intention ($\beta = 0.36, p < 0.001$) and actual usage behavior ($\beta = 0.28, p < 0.01$). Nevertheless, usability-related constructs such as effort expectancy (the equivalent of perceived ease of use in UTAUT) and habit showed the same or even stronger impact on intention ($\beta = 0.42, p < 0.001$ to effort expectancy) and usage behavior ($\beta = 0.51, p < 0.001$ to habit) which demonstrate that ease of use and familiarity have the same or even stronger influence on intention and usage behavior.

Importantly, the findings showed that the expectation of the perception of security moderates the expectancy-intention relationship (interaction $\beta = 0.19, p < 0.05$), meaning that usability is not enough to facilitate long-term usage without an adequate level of perceived security. The positive impact of ease of use on adoption intention is significantly smaller when the perceived security is low, whereas it is a significantly stronger influence on adoption when the perceived security rises beyond the threshold levels. This interdependency implies that the two aspects, security and usability, are not trade-offs but work in synergy where the best results are achieved once both aspects rise above acceptable levels.

To evaluate mobile banking adoption in Uganda, Zikmund [35] adopted TAM2, a further development of TAM that consists of the constructs of subjective norm and voluntarism (retained with perceived risk). The researchers observed that the actual mobile banking use is positively related to perceived usefulness ($\beta = 0.38, p < 0.001$) and perceived ease of use ($\beta = 0.47, p < 0.001$), with the latter having the greatest direct effect, which is stronger than that of usefulness. This means that systems that are seen to be easy, not complex, and need minimal learning are the most actively used. The perceived risk was found to have a negative relationship with usage intention ($\beta = -0.31, p < 0.01$) and had an indirect relationship with actual usage through the intention pathway (indirect effect = -0.14, $p < 0.05$).

Intriguingly, the research found that time risk, apprehension of transaction delays, or lengthy authentication procedures that waste precious time, was seen to be more detrimental than security risk by frequent MFS users who transact most of their daily transactions. The time risk is of greater concern than the fraud risk to users engaging in transactions that are time-sensitive due to the nature of the transactions, such as wage payments that have time constraints or bill payments that are near the due date, as damages are directly and immediately felt in high-rate transaction situations where delays have direct, concrete costs. The result of this finding implies that usability-security trade-offs can be addressed in different ways based on the context of the use and urgency of the transactions.

The study of Generation Z mobile banking use in Indonesia supported the positive, significant impact of feeling easy to use by showing that the simplicity of the system design and low complexity of operations are key factors that support the use of mobile banking among technologically advanced young users ($\beta = 0.53, p < 0.001$). Another predictor was trust ($\beta = 0.34, p < 0.001$), which means that even digitally native users take reliability, protection of privacy, and safety of data into account when using mobile banking services, even though they feel very comfortable with digital technologies in general.

Interestingly, the effects of social influence and prior experience with technology were

weaker and non-significant ($\beta = 0.12$ and 0.15, respectively, $p > 0.05$), which means that personal judgments formed due to first-hand experience with the available system usability and trustworthiness are more determinative among young users than peer influence or experience with similar technologies. This is contrary to that of older demographics, where social influence can frequently be more prominent, and it implies that younger users make independent evaluations based on direct interaction with the interface, not necessarily depending on social validation or using knowledge gained through the use of other technology.

In the study by Nguyen et al. [51], the specific testing variable was the digital self-efficacy that was analyzed as a potential moderator in reference to the Generation Z users of mobile banking, particularly focusing on their confidence in their skills to effectively complete digital tasks. They have found that the usability-behavior relationship has a significant moderator of digital self-efficacy (interaction $\beta = -0.27, p < 0.01$). Low digital self-efficacy users showed strong interest in speed-oriented interfaces over security verification procedures ($\beta = 0.41, p < 0.001$), and often based their choices on peer-to-peer recommendations instead of carrying out their own security evaluations of applications.

Users who overtly expressed low self-efficacy often supported the assertions such as I use my peers to inform me whether the app is safe without personally assessing security features such as encryption indicators or authentication measures which is a vulnerability in that peer assessment might be inaccurate or peers themselves might have a low level of security awareness which is required to make a judgment as to the quality of such features. This reliance on social confirmation instead of technical assessment introduces systematic vulnerabilities where users can take up risky behaviors normalized by their peer groups, including the use of PIN sharing to be convenient or the use of credentials in the note-taking application, not realizing the risk of such behavior and why such actions can be risky.

Dewi et al. [37] investigated the quality of the system and the behavior of users using UX/UI evaluation frameworks, providing focus group discussions and pre-post testing on 120 participants to determine the effects of visual cues and system feedback on user behavior and the number of errors. Their experimental results showed that apparent visual stimuli, such as color-coded warnings of risks, iconographic warnings, and gradual revelation of security information, increased significantly in preventing user error by 35 percent (mean errors before intervention = 4.2 per series of transactions, after intervention ($\beta = 2.7, p < 0.001$).

Therefore, risky behavior frequency was reduced since the situational awareness of the users performing transactions increased with the improved interface design. According to post-experiment interviews, users reported that having clarity in the feedback during the purchase is what makes them feel safe and confident (mean agreement 4.3/5.0), implying that properly designed interface elements may be used to serve two functions simultaneously to make the user both easy to use and security-conscious instead of introducing trade-offs between them.

Dewi et al. discovered that immediate, clear, contextually relevant feedback on the status of transactions, security checks underway, and possible threats identified results in users showing increased voluntary interaction with security measures as opposed to perceiving security measures as opportunity costs to the completion of

tasks. It implies that the perceived friction due to security measures can be caused in part by bad interface design, miscommunication, vague feedback, and upset workflow, but not necessarily by security requirements. Properly integrated security measures that have obvious value indicators can be tolerated or even embraced by the users.

All these findings indicate a strong relationship between the usability factors and the initial adoption as well as the continuation of the use patterns, habits, and security practices. Nonetheless, the majority of the studies have investigated these factors as direct predictors of general usage frequency or satisfaction instead of investigating how usability attributes may intersystematically promote speed preferences, which in turn may stimulate certain security-compromising behaviors. Little is known about the potential development of temporal expectations through usability optimization in an unintentional manner, which decreases adherence to security protocols. Also, even though the moderating effect of digital self-efficacy has been found, its interplay with the swiftness preferences in shaping the risky behavior patterns was not explored by rigorous empirical research.

2.5 The Usability-Security Trade-off

The conflict between usability and security is an inherent design problem of mobile financial services that applies to both user satisfaction and security results.

Tarale and colleagues [52] investigated the underlying conflict of security needs and user-friendliness in the adoption of digital technology, using such advanced analytics as logistic regression, decision trees, and comparison between models. Their analysis of 1,247 users of digital services on different platforms found that there are astonishing differences between the generations in the manner in which users make trade-offs involving security and usability.

A younger group (18 to 34 years) was always more convenience-oriented, being more tolerant of features such as Remember Me features (72% regularly use vs. 43% of 45+ users, $\chi^2 = 156.3, p < 0.001$) and more paradoxical with Two-Factor Authentication (68% regularly use 2FA vs. 51% of 45+ users, $\chi^2 = 89.7, p < 0.001$), which they tend to feel comfortable with.

The older participants (45 and above years) on the other hand portrayed more data privacy concerns (mean privacy concern score 4.2/5.0 compared to 3.4/5.0 of younger users, $t = 12.3, p < 0.001$) and the readiness to forsake the convenience in favor of greater security measures (61% vs. 38% willing to tolerate longer authentication processes, $\chi^2 = 132.4, p < 0.001$).

One of the most interesting findings was that the level of educational attainment is strongly related to digital literacy ($r = 0.58, p < 0.001$), with a significant level of education associated with increased confidence in settings and the use of digital tools in regard to security. The more educated users exhibited a more advanced knowledge of security-usability trade-offs, as they were able to make context-specific decisions of how and when to put security or convenience first, and the less-educated users were more binary in their thinking, perceiving security and usability as incompatible instead of a dimension to trade off.

Uddin and Begum [40] integrated the Theory of Reasoned Action with TAM to study the adoption of mobile banking using the prism of financial inclusion goals. Their findings validated that the effects of Perceived Risk ($\beta = -0.34, p < 0.001$), Relative Advantage ($\beta = 0.41, p < 0.001$), Trust ($\beta = 0.29, p < 0.01$), and Convenience ($\beta = 0.38, p < 0.001$) are combined to create individual propensities to mobile banking adoption.

The introduction of Convenience as an independent construct that exists apart from Perceived Ease of Use is a conceptual improvement, as it accepts that convenience covers the temporal (time savings), spatial (transacting anywhere), and procedural (fewer steps) aspects of interface usability. Uddin and Begum discovered that convenience and security/trust constructs have some autonomy in adoption decisions; users can adopt even in the presence of security concerns when convenience benefits can be high enough (especially in low-value transactions) or reject convenient and insecure services when transaction values are great.

This difference is important in acquiring the multidimensional of user experience in the financial environment and implies that security-convenience trade-offs can be addressed in various ways based on the nature of transactions.

The perceived ease of use, security, and privacy in mobile banking as regards their relationship with adoption intention showed that the positive correlation between ease of use and adoption intention ($\beta = 0.45, p < 0.001$) exists; however, security and privacy concerns also moderate this positive relationship (interaction $\beta = -0.23, p < 0.01$). In particular, ease of use is not a credible indicator of higher adoption intention in cases where the security and privacy concerns are more significant among users.

Positive influence of usability on intention is only when there are low security and privacy problems, or when it is perceived to be taken care of appropriately. Statistical analysis showed that ease of use has no effect on adoption intention ($\beta = 0.08, p = 0.23$) among users with a high degree of security concerns (top quarter), and it has a strong effect among users with a low degree of security concerns ($\beta = 0.52, p < 0.001$). This means the benefits of the usability can be dwarfed by unaddressed issues of information safety and security of transactions.

In order to assess the trade-offs between task effectiveness and security in the mobile transaction management systems, Braz et al. [14] introduced the framework of Security Usability Symmetry (SUS). Their metrics-based model used in three various mobile banking applications noted that usability errors that resulted in wrong entries of inputs due to complex security implementation measures tended to show security vulnerabilities.

In one form, where users had to manually enter the multifaceted transaction codes, consisting of 16 characters, to be verified, errors of 23% (users typed the wrong codes) occurred, failing to place a transaction and user frustration and frustration leading to workaround behavior such as writing down the codes in note applications. According to the users, it is complex security steps that lead them to commit more input errors (mean agreement 4.1/5.0), a paradoxical scenario whereby the more the security, the more vulnerable because of a human factor and workaround.

The experiment showed that an adequate security-usability tradeoff needs to take

into account quantity-versus-quality aspects: the number of security checkpoints is minimal and should be well-designed as opposed to the number of security steps, which are poorly combined. Applications that had 2-3 loosely integrated security checks (such as biometric and transaction confirmation with risk-based OTP in high-value transactions) demonstrated stronger security results (lower fraud rate, higher compliance with security protocols) than applications with 5-6 poorly integrated checks that end users easily circumvented or compromised.

Stewart and Jurjens [27] have made a literature synthesis of the topic of usability-security trade-offs and have elaborated on the design principles of financial apps. According to them, security and user satisfaction can work in harmony only when the former is considered at early design phases and not as an addition. The study found that users like easy interface with minimal barriers (this term was found in 73 percent of user interview transcripts), but security measures that do not seem like an obstacle but as part and parcel of the system have greater compliance (78 percent compliance with integrated security feature versus 43 percent compliance with bolt on security features, $\chi^2 = 245.7, p < 0.001$).

Stewart and Jurjens suggest that during normal operation, security is supposed to be invisible, and during emergency times, it should be obvious; users are supposed to have a smooth sail in regular operation, but clear security messages when suspicious activities are detected. The principles of their design are contextual security (setting the level of security according to the level of risk), progressive disclosure (providing security information in layers instead of all at once), and security feedback loops (assuring security measures without the need to use extra effort on the side of the user).

Aker and Mbiti [28] focused on accessibility-security trade-offs within the particular context of financial inclusion objectives. In their analysis of MFS implementations in Kenya, Tanzania, and Uganda, they found that very high security requirements tend to prevent access by users who are either marginalized or have low digital literacy. The complicated password regulations, repeated re-authentication, and verification processes that need a literate individual are barriers that lock out the very groups that MFS intends to reach.

The critical design question that was asked in the study was, "Is the security mechanism a hindrance to using the service?" and discovered that security measures with an assumption of literacy (reading security warnings, typing complicated passwords, going through multi-step authentication) can be used to screen out large groups of users in situations where 40-60 percent of target users are limited by their level of formal education. Their results indicate that every MFS platform with a diverse group of target customers must seek a common solution between holistic security and open accessibility to ensure that such a direction is the main policy goal in the developing economies.

Aker and Mbiti suggest security that is context-sensitive, offering high security to high-value transactions and simplified to low-value, high-frequency transactions, which form the bulk of the transactions in low-income customer transactions.

All these studies prove that there is tension between security and usability, and improvements in one aspect of design can negatively affect the other. Nevertheless,

the literature also suggests that this trade-off is not definitive; the objective security mechanisms designed in the initial phases of the design processes can achieve the goal of security and usability. The only aspect that is not studied thoroughly is how the demand for speed/swiftness contributes to this trade-off and how time efficiency considerations generate pressure that defuses the security-usability conflict towards the privilege of convenience at the cost of security practices.

Synthesizing Divergent Perspectives on the Usability-Security Relationship

The literature contains potentially contradictory views of usability and security as inevitable trade-offs or possible synergies. To reconcile these points of view, it is important to realize that the relation between the two approaches to design and the quality of the implementation is contingent but not necessarily hostile or complementary.

Researchers who claim that trade-offs are inevitable [45], [52] tend to study situations in which security is introduced as an addition to existing interfaces, such as the introduction of multi-step authentication to interfaces originally designed to be smooth to use. Security mechanisms in these conditions present both cognitive and time costs which are directly in conflict with predetermined usability expectations. The observation made by Braz et al. [14] that complex verification codes made input errors 23% is typical; security requirements are added on top of the existing design, and users feel that the security requirement is a "hump".

On the other hand, studies indicating relations of synergy [27], [37] consider situations where security is encompassed at early design stages and not applied afterwards. The principle of "invisible security" in normal operation and "conspicuous security" in anomalies introduced by Stewart and Jurjens [27] is an expression of design-first thinking in which protective measures do not interfere with user work processes. The experimental results provided by Dewi et al. [37] show that contextual security cues decreased error rates by 35% without negatively affecting workflow efficiency indicate that properly integrated security can actually contribute to a more positive user experience.

It seems that the implementation quality and design philosophy are the key influencing factors. Measures of security can be implemented as

- **Add-on constraints**: Invent zero-sum trade-offs where stiffer security leads to decreased usability.
- **Integrated affordances**: Develop possible synergies where security facilitates task accomplishment.

By looking at the situation, not of whether the trade-off between usability and security is in principle or not, but of *when* (speed preferences, traits of users, condition of transactions) users perceive and react to security-usability interactions, this study has helped address this theoretical tension. Operationalizing swiftness as a mediating construct, the study offers a mechanism for explaining when usability gains bring security benefits through error reduction and facilitative interaction, and when they bring security threats through the development of speed expectations that discourage verification.

2.6 Behavioral Security and Risk-Taking in MFS

Although a lot of research has been conducted on perceptions and intentions, there is limited empirical research that can be used to quantify actual risky behavior in mobile financial settings.

The study of the usability and security trade-offs in mobile financial services critically assessed the effectiveness of trade-offs between ease of use and security in undermining the trustworthiness and confidence of users in financial applications. The research found that with the assistance of empirical survey data on 698 MFS users, the vast majority of users voluntarily reduced security for time and comfort and resorted to risky behaviors such as sharing authentication data (47% of respondents reported sharing PINs with people they trust at least once) or leaving credentials in an insecure place like a note application or messaging application (38% of respondents reported doing so).

This trend illustrates a significant usability-security trade-off: when usability and convenience are the key factors to adoption, the latent vulnerability of oversimplified security controls can be introduced, and when users suffer a security breach or even learn that there are risks they were not previously aware of, trust is destroyed. The research determined that the protection of one's services was rated highly by the users when compared to the mere ease of use (even when users were asked to rank, 62% chose security over ease of use), yet at the same time, some wanted security measures not to be too complex and intrusive (71% of the respondents agreed that security measures should not make transactions very slow).

Remarkably, post-incident security prioritization (84% post-incident) compared to overall security prioritization (62% overall) was significantly higher in those users who had security incidents (fraud, unauthorized transactions) and, as a result, prioritized security over ease of use more.

Relative importance of usability, trust, and contextual variables, such as cost and social influence, are used to investigate the variables that influence the adoption of mobile money services, based on the study by Kelly [32] using TAM. The study established that the perceived ease of use is a decisive factor in the attitudes ($\beta = 0.48, p < 0.001$) and continued use of mobile money services, simplicity and convenience being the focal point of adoption decisions.

Even though trust and security perceptions also impact positively ($\beta = 0.31$ and 0.27, respectively, $p < 0.01$), the direct effects of these perceptions on actual usage are not as considerable as the effects of ease of use, which means that the user has other concerns (convenience) when conducting daily financial transactions as opposed to the security level. Kelly discovered that in the case of routine, habitual transactions, users tend to work in a cognitive economy mode where they do not engage in a minimum of mental effort or time investment, and as a consequence, they tend to involve themselves less in security mechanisms that involve cognitive processing.

This implies a trade-off with the users being willing to work with a lower perceived security as long as the mobile money services are fast, convenient, and easy to operate. The researchers found that transaction frequency is a moderator; those

who made 20+ transactions per month exhibited comparatively low levels of security practice relative to those who made fewer than 20 transactions per month, indicating that frequent use would develop the habitual nature that did not involve deliberate security practices.

A research study on the contribution of perceived risk, perceived security, and perceived trust to the adoption of smart mobile banking through Structural Equation Modeling came up with the conclusion that, perceived security ($\beta = 0.37, p < 0.001$) and perceived trust ($\beta = 0.42, p < 0.001$) have strong positive predictive values of adoption, which is in line with the notion that user trust in ability of a system to hold financial and personal information safe are key factors in mobile banking contexts.

Perceived risk, on the contrary, has negative and significant effects on trust ($\beta = -0.44, p < 0.001$) and attitudes ($\beta = -0.28, p < 0.01$); that is, high vulnerability or risk of loss may offset the influence of a positive usability belief. Whereas the aspects of usability, such as ease of use ($\beta = 0.34, p < 0.001$) and usefulness ($\beta = 0.39, p < 0.001$), have a positive influence on adoption, they cannot overcome the barriers that high perceived risk introduces to the process.

The authors of the study have concluded that both trust and attitude mediate the negative influence of perceived risk on adoption intention, which indicates that risk concerns run in more than one psychological mechanism to affect behavior.

Al-Hujran et al. [39] used Process Virtualization Theory to investigate continuance intention in mobile banking and surveyed 484 users with the help of SEM analysis. Their results showed that the fear of transaction failure in the process of execution because of technical defects, connection loss, or system malfunctions could be the main obstacle to long-term use ($\beta = -0.41, p < 0.001$).

Users who shared worries in phrases such as "I fear the transaction will fail in the process" had an overall higher abandonment of mobile banking services (abandonment rate 34 and 8 with a high level of concern and low level of concern, respectively, $\chi^2 = 78.4, p < 0.001$) despite being satisfied with usability features. This implies that reliability perception is a separate dimension to the conventional security issues (fraud, data breaches) and that users' risk evaluation is based on both security risk and operational risk.

Surprisingly, users who had encountered failures in processes (transactions failed, systems crashed in the course of transactions) acquired much greater perceived risk of virtual process failure, which remained despite system improvements, indicating that the issue of reliability once acquired is hard to overcome, and may be more durable than the issue of security.

Hassan et al. [38] examined the change in security perceptions and risk acceptance during MFS adoption during the COVID-19 pandemic with the use of extended UTAUT. According to their results, the aftermath experience of dependence on digital financial services following the pandemic has made users relinquish increased risk levels to gain access to the required expediency and accessibility. A high number of respondents said they felt that something in the statement "I have no choice but to use this app even though I am concerned about my security" (57% agreed or strongly agreed) suggests that situational influence might supersede personal risk

preference and create situations in which users are being forced to do risky things, not because they want to do so.

The research resulted in sustained use even in the face of high-security concerns on the part of users, who adopted the necessity-driven adoption yet showed a higher level of stress (using the Technology Anxiety Scale) and reduced trust, which resulted in psychological costs of forced adoption of perceived risk. The authors suggest that forced adoption due to the pandemic could have resulted in creating a user base with varying risk tolerance profiles compared to those who adopted voluntarily, and the consequences of forced adoption on behavioral patterns of security in the long run.

These studies reveal that behavioral security in MFS situations entails a complicated interaction of perceptions, habits, situational necessities, and real risky practices. However, several gaps remain. To begin with, the majority of studies have studied perceived risk of various threats and not the actual risky behavior; the rate and trends of certain security-compromising behaviors are not quantified. Second, there has not been a systematic study on the relationship between speed preferences and risky behaviors. Third, it is not fully understood how the usability features can be transformed into behavioral security outcomes.

2.7 Digital Literacy, Cybersecurity Awareness, and User Behavior

A new source of research is exploring the role of digital literacy and cybersecurity awareness in the security-usability-behavior relationship in MFS.

Kumar and Rani [48] used PLS-SEM to consider the moderating effect of cybersecurity awareness on the connection between digital literacy and trust in digital banking using a moderation analysis. In their findings, they showed that digital literacy is a kind of filtering mechanism: highly-literate users have calculated risks and make informed security choices; low-literate users have blind-faith in systems and thus are more vulnerable to fraud and security breaches.

Active risk assessment was found in users with high digital literacy (measured using validated scales to assess technical knowledge, internet proficiency, and security awareness): users with high literacy (4.4/5.0) agreed that "my knowledge of digital threats affects my trust in the app" ($t = 15.7, p < 0.001$) whereas low-digital literacy users (2.8/5.0) did not. Meanwhile, passive trust in low-literacy users was found to rely on interface aesthetics or brand recognition as opposed to security features (correlation interaction between app looks professional and trust = 0.58 with low-literacy users, and 0.21 with high-literacy users, $z = 4.3, p < 0.001$).

Kumar and Rani discovered that there was a moderation of the relationship between perceived ease of use and risky behavior with digital literacy (interaction $\beta = -0.31, p < 0.01$). The ease of use among low-literacy users was a strong predictor of risky behavior, whereas it was non-significant among high-literacy users. This implies that digital literacy offers such protective benefits that help users ensure security practices in cases where interfaces reduce friction.

On the same note, the data of Afzal et al. [41] also explored how digital literacy influences Fin-tech adoption by using moderated SEM analysis. Their result has shown that literacy is both enabling and protective: the higher the digital literacy, the higher will be the adoption rates ($\beta = 0.36, p < 0.001$), but at the same time, the less risky behaviors will be engaged in ($\beta = -0.29, p < 0.01$).

The paper reported that the technologically advanced users are capable of negotiating security-usability trade-offs better, accepting the required security friction but refusing to encounter superfluous verification procedures. Highly literate users were able to discriminate between security measures that offer true protection (which they accepted with only slight objection) and those offering only slight protection benefits compared to inconvenience (which they complained about and sometimes avoided).

It is proposed that digital literacy will allow metacognitive awareness of security, because people can not only determine whether security is available but also whether a given security mechanism is adequate and capable, resulting in more rational decisions regarding security behavior [41].

Nagari and Rahararja [50] surveyed 200 users who participated in SmartPLS 4 to differentiate between cybersecurity awareness, knowledge, and behavior. Their results showed that there is an alarming lack of connection: awareness does not always translate into safe behavior. A large number of users approved such statements as "I know the risks; however, I do not always change my behavior" (63% approval), which proves that even informed users have gaps in their knowledge and behavior.

The researchers found that knowledge ($\beta = 0.47, p < 0.001$), which was the perception of specific threats, vulnerabilities, and specific protective measures, and not mere awareness ($\beta = 0.18, p = 0.12$), which is represented by general knowledge that there is a security risk, is the main motivator of actual risk reduction behavior. Nagari and Raharar have discovered that users might know that mobile banking is vulnerable to social engineering attacks (awareness), and they do not know that their use of birthdays as PINs exposes their accounts to social engineering attacks (knowledge), and this is what defines them as adopting protective behaviors.

This implies that the educational interventions should go beyond awareness campaigns ("be careful about your mobile banking") to full knowledge building (here's how attackers can use weak PINs, and here are detailed PIN creation strategies that can withstand these attacks).

To come up with a qualitative resilience model, Ali and Shah [45] carried out semi-structured interviews with 22 mobile users of banking services. In their investigation, they discovered human behavior as the weakest link in cybersecurity and that users feel that multifactor authentication and other security solutions are complex and unnecessary obstacles to the speed of the transaction. The respondents noted that I find multi-factor authentication as a hindrance to my speed (18 out of 22 participants said the same thing), and this is an example of the perceived clash of the security need and the usability preference.

The study noted that cybersecurity resilience should be reinforced by focusing on user attitudes and developing proactive security attitudes instead of applying technical controls. Ali and Shah have outlined various mental models: (1) security is the

responsibility of the system, not mine; (2) if something were wrong, the app would tell me; and (3) I will deal with security after I experience a problem. The result of these cognitive models is that the users lose interest in security concerns and move on to automatic safeguards, leaving them vulnerable to attacks that use the social aspect of social engineering.

The systematic literature review included 2019-2025 articles to summarize the research on mobile transaction security and adoption [46] by Debora (2025). The analysis of 67 empirical studies found that 42 percent of adoption failures are caused by the barrier of digital literacy and not by security, and ease-of-use and affordability are the most important factors influencing user choices. Security was at a lower priority compared to cost and usability, especially for poor people.

This observation highlights the multidimensional nature of interactions between socioeconomic variables, digital literacy, and security-usability preferences in the formation of the MFS adoption and usage patterns. The synthesis of Debora is that in a context with limited resources, users can consciously or unconsciously search for immediate availability and affordability, rather than the abstract issue of security, specifically when security threats are perceived as probable and remote, whereas usability and cost threats are perceived as immediate and certain.

The overall consequence of these studies is that digital literacy and cybersecurity knowledge play a major role in how users go about the security-usability-speed trade-offs. Nevertheless, the exact interplay in relation to the level of literacy, rapidity attitudes, and risky behavior is not well-investigated. Even though literacy has protective effects, it is still unclear how it works, whether by diminishing swiftness preferences, by allowing users to hold onto security practices despite swiftness preferences, or by other mechanisms that still need to be studied further.

2.8 Contextual Factors in Bangladesh MFS Ecosystem

A number of studies have concentrated on Bangladeshi MFS in particular, showing peculiar trends that apply to this study.

Rouf et al. [43] used the Expectation Confirmation Model to examine the continuance intention of rural users to MFS in Bangladesh. Their PLS-SEM analysis of 384 rural users showed that perceived trust was found to be the strongest predictor of satisfaction ($\beta = 0.52, p < 0.001$), which, in its turn, mitigates the feeling of security anxiety (indirect effect = -0.28, $p = 0.01$).

The trust was greatly boosted by government support and endorsement ($\beta = 0.34, p < 0.001$), and the users indicated that they felt safe when using MFS because of government endorsement (mean agreement 4.2/5.0). This indicates that institutional legitimacy is a significant factor in security perceptions in the Bangladeshi setting, in which the reliance on trust in regulatory systems can replace the conduct of personal examination of security.

Rouf et al. discovered that rural users with low financial literacy and little economic means depend on third-party validation (government approval, peer use, agent rec-

ommendation) as opposed to independent security review. This dependency results in opportunities and threats. Although government approval can help initiate usage among the reluctant users, the same can lead to overconfidence, where the user does not think that the government endorsement will provide a full degree of security.

The report also found that the rural customers had varied usage patterns as compared to the urban customers, who used it more often in agent-assisted transactions (where the agency runs the app on behalf of the customers) instead of having to run the application independently. This presents special security concerns, since the users have to trust that agents will not misuse access to their accounts or credentials, a trust relationship that goes beyond trust in the technology platform itself.

Cham et al. [30] compared the Fin-tech adoption trends in Malaysia, which gave valuable information in the context of developing economies comparable to Bangladesh. As their SEM analysis showed, competitive advantage based on speed is a more important driver of adoption than risk aversion, especially in the urban clusters.

Those who ranked statements such as using this service puts me at an advantage over the traditional ways as highly significant (odds ratio = 2.7, $p < 0.001$) were the ones with higher adoption rates despite having a high risk awareness. This implies that a relative advantage in speed and efficiency can be used to surpass security concerns when users feel that they are having definite advantages over other financial services.

In environments where doing business with traditional banking involves physical commuting, queuing, and filling paperwork, which can take hours to complete, the time-saving associated with mobile financial services offers dramatic competitive advantages that overwhelm issues of security, especially for time-limited customers (small business owners, employed individuals). The competitive advantage mechanism can be especially relevant in developing economies where the traditional financial infrastructure is inefficient or inaccessible.

Other background studies about Bangladesh have investigated the impact of MFS agents on the behavior of users and their security habits. Agents are the mediators that facilitate transactions to users, and this is especially so in rural and less-educated users. Although the agents can make things more accessible, they also create security weaknesses. The users who utilize the services of the agents can share credentials, monitor PINs, or even do no transactions at all, thus leaving room to abuse them.

Research has established that about 35 percent of rural MFS users are dependent on agent-assisted transactions as opposed to independent use of apps, which is a completely different model compared with the independent user model used by most security models. This agent-mediated pattern of usage needs to employ security strategies that take into consideration the existence of trusted intermediaries as well as safeguard against likely agent violations.

Security perceptions and behaviors in Bangladesh are also determined by cultural issues. Financial practices that rely on trust, which are common in informal economies, where verbal contracts, family-based lending, and peer-to-peer networks are used in place of formal contracts, result in a set of expectations that do not necessarily conform to the requirements of formal security provisions of the digital systems. Users who have been used to trust-based transactions will view the security checks

as measures of lack of trust and not as security measures.

Functional needs. Family members might require the sharing of credentials to access shared accounts, where the household is required to make financial transactions pose a conflict with the models of credit security on individual accounts. Security models that imply individual ownership of accounts might not be suitable or feasible in settings in which collective household financial management is social.

These contextual analyses determine that the Bangladeshi MFS ecosystem possesses its own specifics, which can have a certain impact on the security-usability-behavior relations. Nevertheless, there is little systematic empirical research on the role of these contextual elements in determining preferences in swiftness and risky behavior in Bangladesh in particular.

2.9 Research Gaps and Study Positioning

The reviewed literature reveals several critical gaps that this research addresses.

Gap 1: Behavioral Measurement vs. Perceptual Measurement

Although considerable studies have been conducted on perceived risks and security perceptions, very little research has conducted on a quantitative study of actual risky behaviors that are undertaken by users instead of their perceived risks or intentions. Literature is currently mostly concerned with adoption intentions [24], [25], [33] or perceived risks [26], [40] instead of operationalizing and measuring the actual behavioral patterns that are damaging to security.

The difference between the perceived risk and the risky behavior is very important, as there may be users who are aware of risks but at the same time practice a risky behavior, or users who are not aware of the risks involved in their practices. Attitudes are only measured by research that includes perceptions, which does not allow applying them practically, such as to interface design or security policy that needs to encompass real behaviors.

Gap 2: Swiftness as an Explicit Construct

Despite significant research carried out on the perceived risk and security perceptions, scarce research has carried out on actual risky behavior taken by users rather than perceived risks or intentions taken by them. The intention to adopt [24], [25], [33] or the perceived risks [26], [40] are mostly the subject of literature now, rather than the actual patterns of behavior, which are harming security.

The gap between the perceived risk and the risky behavior is very critical since there could be users who are aware and at the same time, practice a risky behavior, or there could be users who are not aware of the risks involved in their practices. Research that includes perceptions only measures attitudes, and this does not permit them to be applied in practice, e.g., interface design or security policy that must cover actual behaviors.

Gap 3: Quantification of Usability-Security Behavioral Linkages

The relationships between the design features of usability and the security-threatening user behaviors remain to be undermeasurable, which precludes evidence-based inter-

face design decisions. The literature at hand theorizes the usability-security trade-off [14], [27], [52] and lacks empirical quantification of the connection between the enhancement of specific usability aspects and the measurable risky behavior.

The information needed by designers will answer questions like, "Under what circumstances can we reduce the number of authentication steps by one and still make risky behavior increase by what percentage?" or What are the correlations between credential sharing behaviors and interface simplicity? The decision-making process depends on the assumptions that are not always true until we have the quantitative data that will help to correlate the usability features and the behavioral security outcomes.

Gap 4: Interaction of Digital Literacy with Swiftness and Risk

Although digital literacy has been determined as a moderating factor [41], [48], [50], the interaction between it and the swiftness preferences and risky behavior regarding the high-frequency mobile financial transactions is not investigated. The knowledge-behavior gap that Nagari and Rahararaj [50] target should also be researched further in the settings where the time constraints can potentially widen the gap between the security awareness and the actual behavior.

Is there a protective effect of digital literacy in terms of increasing or decreasing swiftness preferences or in facilitating the use of security practices in the face of swiftness preferences or through other mechanisms? What is the interaction between the temporal pressures and the literacy levels in affecting the security behaviors? These are some of the questions that have not been answered.

Gap 5: Context-Specific Behavioral Investigation in Bangladesh

Bangladesh studies have concentrated on the adoption intentions and overall usage patterns but have not sufficiently considered the impact of the specific usability features, especially swiftness and ease of use, on the provable risky behaviors in this regard [24], [26], [33], [43].

Although usability-security trade-offs have been identified internationally [14], [49], [52], there are not many context-specific studies in developing economies with distinct financial ecosystems, cultural behaviors, and agency-induced usage patterns. The culture of Bangladesh, with a high penetration of MFS, heterogeneous user bases, agency-mediated transaction frameworks, and tendencies towards trust-based finance, might also have certain specific trends that are not reflected in international studies.

Gap 6: Post-Pandemic Risk Behavior Dynamics

The effect of the pandemic on forced adoption and risk acceptance [38] creates new dynamics that can have permanently changed the security-usability-behavior relationship, especially in situations where MFS shifted its status from optional convenience to a necessary infrastructure. This change necessitates a need to study the role of necessity-driven adoption in shaping long-term behavioral patterns and practices related to security.

The risk tolerance profile, level of security knowledge, and behaviors of users who embraced MFS due to the need to seek security during the pandemic may not be

the same as those of voluntary early adopters, and no study has systematically been able to study how this segment of the population manages to cope with security usability trade-offs.

Research Positioning

The gaps that this research addresses are:

1. Measuring risky behavior as a construct that quantifies the degree of risky behavior, not the degree of perceived risk, and by validated scales, on the actual security-compromising behavior that is part of a security-compromising behavior scale and not the assessment of perceived risk.
2. The addition of the rapidity as an explicit variable that indicates preferences related to speed in completion of transactions, theorizing it as a source of risky behavior and an outcome that depends on usability variables.
3. Efforts to empirically test the relationship between usability constructs and behavioral security outcomes through the use of strong statistical techniques (CB-SEM) and present quantitative information regarding the strength and direction of the relationships.
4. With areas of high penetration rates (89.38 million active users), a wide range of user demographics, and a special socioeconomic profile, the Bangladeshi MFS context is proposed, and the direct implications of the empirically based research on the interface design and security policy making in the area of developing digital financial ecosystems are offered.
5. Looking at the security usability speed triangle as a whole, understanding that they are not in bilateral trade-offs but in a dynamic interaction.

The combination of behavioral measurement, rapidity construct, and situation-specific inquiry fills the given gaps but also adds to both theoretical and practical knowledge on the subject of usability-security-speed relations in mobile financial services. The research enables the establishment of empirical relationships between these constructs and thus provides evidence that can be used to inform a process of designing interfaces to adopt strategies that are effective in balancing usability, speed, and security in situations where all three constructs are of paramount importance.

Chapter 3

Requirements, Impacts and Constraints

Ethical issues such as informed consent, privacy rights and participant rights were attentively handled, and approval of the ethics committees was gained beforehand.

3.1 Final Specifications and Requirements

It was a quantitative empirical study that was developed by this research project to assess. The tradeoff between usability, security and speed in the Bangladeshi Mobile Financial System (MFS) environment.

3.1.1 Methodological Requirements

- **Analytical Framework:** The research makes use of a long Technology Acceptance Model (TAM) that was merged with definite behavioral constructs: Swiftness (SWF) and Risky Behavior (RB).
- **Structural Modeling:** Covariance-Based Structure is used to test hypotheses. Complex path Multivariate and Bivariate Path Analysis (CB-SEM) to mentally examine complex path relations whilst considering the error of measurements.
- **Psychometric Integrity:** The measurement scales had to satisfy the requirements developed credible levels of reliability, namely, **Cronbach's** $\alpha \geq 0.70$ and **Composite Reliability (CR)** ≥ 0.70.

3.1.2 Resource and Technical Requirements

- **Data Management:** *Python 3.9* and related libraries (*Pandas, NumPy*) Preprocessed and cleaned data and the identification of multivariate outliers.
- **Statistical Software:** *JASP 0.18.3* and *SPSS 28.0* were used to do the descriptive statistics, Exploratory Factor Analysis (EFA) and path estimation.
- **Infrastructure:** Access to the *Google Forms* API and encrypted cloud storage was necessary to facilitate secure, mobile-optimized data collection from a diverse respondent pool.

3.1.3 Functional and Non-Functional Requirements Specification

Although this research project is investigative rather than developmental, the nature calls for a high specification of functional and non-functional requirements to guarantee methodological rigor and the applicability of findings in practice.

Functional Requirements

Functional requirements establish what the research must achieve to cover the stated objectives and research questions.

1. **Empirical Data Collection**
    - **FR1.1:** At least 385 respondents will be solicited to complete the questionnaires on the sample population to warrant statistical validity in the analysis of the SEM at a 95% confidence level.
    - **FR1.2:** The sample will consist of the representation of key demographic variables: age (at least 3 groups), experience (at least 3 levels), and profession (at least 3 levels).
    - **FR1.3:** The data collection tools will capture all five core constructs (PU, PEOU, SWF, RB, PS) in validated multi-item scales with a minimum of 3 items per construct [4].
    - **FR1.4:** The questionnaire will include attention checks and validity indicators to detect unfocused or unscrupulous answers.
2. **Model of Measurement Validation**
    - **FR2.1:** Internal consistency reliability (Cronbach's $\alpha \geq 0.70$, Composite Reliability ≥ 0.70) must be acceptable for all constructs.
    - **FR2.2:** Exploratory Factor Analysis will be used to determine data suitability and factorability (KMO measure > 0.60, Bartlett's Test of Sphericity $p < 0.05$, Eigenvalues > 1.0).
    - **FR2.3:** Confirmatory Factor Analysis (CFA) will confirm that the measurement structure based on the five factors has acceptable model fit ($CFI \geq 0.90$, $RMSEA \leq 0.08$) [12].
    - **FR2.4:** Convergent validity will be determined using Average Variance Extracted (AVE) ≥ 0.50 for all constructs [2].
    - **FR2.5:** Discriminant validity will be established via HTMT ratios less than 0.85 between all construct pairs.
3. **Structural Model Testing**
    - **FR3.1:** The study will test four main hypotheses based on Structural Equation Modeling (SEM) and maximum likelihood estimation.
    - **FR3.2:** Pearson Correlation coefficients will be used to determine bivariate relationships ($p < 0.05$, $r < 0.90$, $VIF > 0.10$ and $VIF < 5.0$).
    - **FR3.3:** Regression analysis will be conducted to ensure the model is statistically significant (ANOVA Test, $p < 0.05$, and R^2 values calculated against all endogenous variables).

- **FR3.4:** The model fit must meet acceptable standards ($CFI \geq 0.90$, $TLI \geq 0.90$, $RMSEA \leq 0.08$, $SRMR \leq 0.08$).
- **FR3.5:** Path estimates will be provided with standard estimates, standard errors, critical ratios, p-values, and 95% confidence intervals.

4. **Mediation Analysis**
    - **FR4.1:** Bootstrap tests of indirect effects will be performed with 2,000 resamples (minimum) [17].
    - **FR4.2:** The confidence intervals of the indirect effects will be reported as bias-corrected.
    - **FR4.3:** The type of mediation (full, partial, competitive) will be classified according to the importance of direct and indirect effects.
5. **Moderation Analysis**
    - **FR5.1:** Multigroup analysis will be conducted to assess differing relationships between user groups (age, education, experience, frequency of transactions) [8].
    - **FR5.2:** Chi-square difference tests will determine the statistical significance of group differences in path coefficients.
    - **FR5.3:** A minimum group size of 100 respondents will be maintained to ensure sufficient statistical power in group comparisons.
6. **Final Products and Reports**
    - **FR7.1:** The entire thesis report will include all methodological processes, analytical findings, and explanations.
    - **FR7.2:** Empirical findings will be applied to draw evidence-based design recommendations [14].
    - **FR7.3:** Weaknesses and further research opportunities will be clearly stated.
    - **FR7.4:** All data processing programs (Python), statistical results (SPSS, JASP), and measuring tools will be archived to enable reproducibility.

Functional Requirements

The functional requirements define the research that should be accomplished to fulfill the stated objectives. These are detailed in Table 3.1.

Table 3.1: Functional Requirements Specification

ID	Category	Requirement Details
FR1	Data Collection	**FR1.1:** Minimum 385 respondents (95% confidence). **FR1.2:** Representation of age, experience, and profession (3+ groups each). **FR1.3:** Capture 5 core constructs (PU, PEOU, SWF, RB, PS) with validated scales (min. 3 items/construct) [4]. **FR1.4:** Include attention checks/validity indicators.
FR2	Measurement Validation	**FR2.1:** Internal consistency ($\alpha \geq 0.70$, CR ≥ 0.70) **Hair2010**. **FR2.2:** EFA suitability (KMO > 0.60, Bartlett's $p < 0.05$). **FR2.3:** CFA model fit ($CFI \geq 0.90$, $RMSEA \leq 0.08$) [12]. **FR2.4:** Convergent validity ($AVE \geq 0.50$) [2]. **FR2.5:** Discriminant validity via HTMT < 0.85.
FR3	Structural Model Testing	**FR3.1:** Test 4 hypotheses using SEM (ML estimation). **FR3.2:** Bivariate checks ($p < 0.05$, $r < 0.90$, VIF $0.10 - 5.0$). **FR3.3:** Significant regression ($p < 0.05$, R^2 reported). **FR3.4:** Acceptable model fit ($CFI/TLI \geq 0.90$, $SRMR \leq 0.08$) **Hair2010**. **FR3.5:** Report path estimates with 95% CIs.
FR4	Mediation Analysis	**FR4.1:** Bootstrap tests (min. 2,000 resamples) [17]. **FR4.2:** Report bias-corrected confidence intervals. **FR4.3:** Classify mediation type (full, partial, or competitive).
FR5	Moderation Analysis	**FR5.1:** Multigroup analysis on user demographics [8]. **FR5.2:** Chi-square difference tests for path coefficients. **FR5.3:** Min. group size of 100 for statistical power **Cohen1992**.
FR7	Products & Reports	**FR7.1–7.4:** Complete thesis with methodology, evidence-based design recommendations [14], stated limitations, and reproducible code archives (Python/SPSS).

Non-Functional Requirements

3.2 defines quality attributes and constraints.

Table 3.2: Non-Functional Requirements (Quality Attributes)

ID	Attribute	Requirement Details
NFR1	Validity	**NFR1.1–1.4:** Address common method bias [11], use established scales, ensure statistical power [15], and maximize demographic diversity.
NFR2	Reliability	**NFR2.1:** Measurement reliability ($\alpha \geq 0.70$). **NFR2.2–2.3:** Inter-rater and Test-retest not applicable for cross-sectional self-reports.
NFR3	Ethical Compliance	**NFR3.1–3.5:** Obtain ethics approval, online informed consent, optional email collection only, secure data storage, and aggregate reporting (GDPR/APA).
NFR4	Reproducibility	**NFR4.1–4.4:** Provide full survey tool, commented code, detailed analysis steps, and software versions (Python 3.9, SPSS 28.0).
NFR5	Applicability	**NFR5.1–5.3:** Translate results to practical design recommendations accessible to non-technical stakeholders [9].
NFR6	Timeliness	**NFR6.1–6.3:** Data collection (3 months), Analysis (2 months), Writing/Defense (2 months).
NFR7	Resources	**NFR7.1–7.3:** Use cost-efficient tools (Google Forms), licensed/free software, and no financial participant rewards.

Acceptance Criteria

The following milestones have been identified to declare that the study was successfully completed:

Statistical Rigor: At least 385 valid responses; models of measurement and structural constructs show acceptable goodness of fit; hypothesis tests are done appropriately.

Research Answers: All six research questions were answered with empirical evidence, and relationship quantified and interpreted with a practical meaning.

Quality & Ethics: All the requirements (FR1-FR7, NFR1-NFR7) are satisfied. The thesis is of academic standard, the defense is done, and the ethics approval conditions are upheld throughout the process.

Applied Contribution: Recommendations on evidence-based designs are provided to the stakeholders in an actionable format with a clear understanding of future research opportunities.

Compliance with Standards

The following professional codes and frameworks are followed in this research:

- **Ethics:** BRAC University Policies, APA Ethical Principles, and GDPR data privacy.
- **Methodology:** AERA Standards (validity/reliability), SEM best practices, and Survey methodology standards.
- **Reporting Integrity:** APA Publication Manual (7th ed), JARS-Quant, STROBE-like reporting, and IEEE Code of Ethics.

All these non-functional and functional requirements, acceptance criteria and compliance standards will make this research methodologically rigorous, ethically sound and practically relevant.

3.2 Societal and Environmental Impact

3.2.1 Societal Impact

This study has massive implications on digital financial inclusion in Bangladesh. The results of the quantification of the drivers of risky user behavior can guide MFS providers and regulators to create safety-first interfaces that would not need to compromise user experience. This is especially critical towards securing vulnerable user groups including users with less technical skills against fraud and social engineering, and enhancing the overall integrity of the national digital economy.

3.2.2 Environmental Sustainability

This research allows advancing the ongoing shift from a physical, paper-based banking system towards a digital-first one by fostering the trust and reliability of electronic payment systems. The MFS has a long-term adoption, which lowers the environmental impact of the physical bank branch maintenance, the paper waste due to documentation, and the carbon footprint of users commuting to physical financial institutions.

3.2.3 Comprehensive Societal Impact Evaluation

The study measures the usability surity trade-off of the Mobile Financial Services (MFS) in a technology backbone that supports the needs of more than 89 million people living in Bangladesh. The results have implications on various levels of social welfare:

Health and Safety Impacts

Digital Financial Stress Reduction: The psychological health improvement has been related to digital financial services in that the level of stress experienced by cashbased transactions is minimized. MFS websites allow customers to:

1. Send emergency funds instantly during health disasters.
2. Make medical payments without having to visit the physical payment centers.
3. Get the salaries in a secure environment without having to carry physical cash.

Finding the equilibrium between the **security** and the **usability** directly influences these health-protective benefits. **High security friction** can cause users to go back to cash, and bring **psychological burdens** like fear of robbery and time constraints [27]. On the other hand, the **undermined security** at the expense of usability will augment **fraud threats**, which are reported to result into **anxiety and post-traumatic stress**.

Physical Safety: Moving up to **MFS** eliminates susceptibility to:

- **Larceny** before delivery to payment centers.
- **Incivility** especially to women who come to remote banks.
- **Road accidents** are irrelevant traveling.

The **risk-based authentication** solutions suggested in this study can maintain these safety advantages through controlling **behavioral security vulnerabilities** [52].

3.2.4 Implications of Law and Regulations

Consumer Protection Framework: Bangladesh Bank has a regulatory framework that has provisions of **security disclosure** as well as restricting **consumer liability** [42]. This paper is an empirical test of calibration:

- **Mandate Risk-Based Authentication:** The use of protocols that are not dynamic should be avoided and there should be an increase in security measures depending on the context of a transaction.
- **Normalized Security Disclosures: Training** appears to increase **confidence** ($b = 0.143, p < .001$) and thus **regulators** ought to make **structured security training mandatory** in the onboarding process.
- **Liability Structures:** Since **breaches** are oftentimes caused by **user actions** [5], their distribution of liability in the case of **providers and users** can become more just.
- **Data Privacy and Protection:** The **perceived security** has been identified as an important **driver of usefulness** ($b = 0.133, p = .006$) with the **Digital Security Act** and the upcoming **Data Protection Act** in **Bangladesh**. One of the key factors in the **adoption decision** is the **perception of privacy**; therefore, **clear policies** are a **competitive edge**.

3.2.5 Cultural Context and Social Fairness

Financial Inclusion and Gender Equity: MFS has greatly contributed to **women inclusion**, which is more restricted in their mobility [47]. Nonetheless, this paper concludes that **lower-educated users** respond more intensively to **swiftness risk relations** ($b = 0.512$ vs. 0.354 **higher education**) and thus are **vulnerable to risky behavior**. Design must be:

- **Culturally Sensitive:** Appreciating **decision-making power structures** at home.
- **Inclusive:** Weighing security to the **less digitally literate**.
- **Gender-Responsive:** The response to particular dangers such as **shoulder-surfing** when living in common areas.

Culture by Agent: There are about **35 percent of the rural users** who use **agents**. This poses a distinct danger in which **pressure on speed** in agent stalls can cause users to **exchange PINs** or ignore **personal confirmation**. These **agent-based realities** must be considered in security interventions.

3.2.6 Long-Term Social Change

Development of Digital Literacy: MFS is the most widespread platform of **digital literacy** as it becomes ubiquitous [41]. **Well-constructed interfaces** not only allow them to gain finances, but also teach the population the overall **digital safety**.

Economic Empowerment: MFS empowers the **marginalized people** by eliminating the **male mediators** to access wage and enabling **remittances by migrants** [34]. Nonetheless, one **incident of fraud** will make a user go back to **physical finance** altogether, which will reverse the gains of inclusion. This study contributes to the **safeguarding of these empowerment benefits** by establishing the **sweet spot** between **speed and security**.

3.3 Project Constraints and Limitations

Although this research is insightful, it was carried out with a number of **practical and methodological limitations** that outline the scope of this research:

- **Time and Design Limitations:** The study happened under a given **academic cycle**, which required a **cross-sectional survey design**. As a result, the study does find meaningful **correlations**, but it cannot conclusively determine **longitudinal causal changes** in the behavior of the users over time.
- **Data Access and Behavioral Measurement: Objective system logs**, including real **transaction speeds** or **error messages on authentication**, were not accessible because of **privacy regulations** and because of the **proprietary nature** of MFS platforms. The research will be based on **self-reported measures of behavior**, which could be susceptible to **social desirability** and **recall bias**.
- **Computational and Software Constraints: Multi-group invariance testing** and **standardized bootstrap estimation** were subjected to the computational constraints and stability of the **JASP SEM module**. To counter this, **indirect effect confidence intervals** had to be run again using **complementary estimation** so that their **robustness** could be ensured [17].
- **Sampling and Generalization:** The **recruitment of the participants** was based on **digital convenience** and **snowball sampling**. This could have caused **under-representation of rural users** or users with **low levels of digital literacy** which may restrict the **generalization** of the findings to the rest of the **Bangladeshi population**.
- **Statistical Power in a Moderation Task: Multi-group analysis** was carried out to investigate the impact of **user experience and training** but due to inherent **imbalances in subgroup sizes**, there might have been a compromise in the **statistical power** to detect subtle **moderation effects**.

Even with these limitations, the study has generated valuable **empirical data** regarding **usability-swiftness-risk mechanisms** and gives a **strong basis** to **longitudinal behavioral data** and **experimental studies** in the future.

3.4 Environmental Impact Analysis and Sustainability Analysis

Although this is a behavioral study, which does not actually produce a tangible object, the findings can make a tremendous contribution to environmental sustainability by affecting the design and patterns of utilization of digital financial infrastructure.

3.4.1 Direct Environmental Research Activity Impact

The immediate environmental impact of the research includes data collection, processing, and dissemination. The total energy used and the amount of carbon emitted is low because of a digital-first approach:

Data Collection Phase:

- Online survey hosting (Google servers): 4.22 kWh (703 responses × 0.006 kWh)
- Participant device energy: 7.03 kWh (10-minute sessions × 0.01 kWh)
- Network infrastructure: 2.11 kWh (703 responses × 0.003 kWh)
- **Subtotal: 13.36 kWh = 6.68 kg CO_2e** (Bangladesh grid factor: 0.5 kg CO_2/kWh)

Data Processing and Analysis:

- Computational analysis (Python, SPSS, JASP): 3 kWh (20 hours × 150W)
- Cloud storage (5 GB, 6 months): 0.03 kWh
- **Subtotal: 3.03 kWh = 1.52 kg CO_2e**

Documentation and Dissemination:

- Thesis writing and formatting: 10 kWh (100 hours × 100W)
- Digital defense presentation: 0.6 kWh (2 hours × 300W)
- Digital distribution (PDF): negligible
- **Subtotal: 10.6 kWh = 5.3 kg CO_2e**

Total Direct Research Carbon Footprint: 13.5 kg CO_2e

Mitigation Measures Implemented: Digital-only survey distribution avoided 703 paper questionnaires, saving approximately 11 kg of paper (3.52 kg CO_2e avoided). Digital thesis submission eliminated printing of 5 bound copies (1,000 pages total), saving 10 kg CO_2e. Digital collaboration tools reduced physical meeting requirements.

Net Environmental Impact: -7.5 **kg CO_2e** (negative value indicates environmental benefit compared to traditional paper-based research methodologies).

This minimal direct footprint demonstrates that behavioral research in digital financial services can be conducted with negligible environmental impact while generating findings that enable massive indirect environmental benefits through sustained MFS adoption.

3.4.2 Indirect Environmental Impact through MFS Adoption Patterns

The main environmental importance of the study is the indirect effects because it affects MFS interface design, and consequently, adoption and usage patterns with significant environmental consequences.

Lessening of the Physical Financial System

The MFS ecosystem in Bangladesh has helped 89.38 million people perform financial transactions without visiting physical branches.

1. **Unincurred Construction and Maintenance**:
    - Embodied carbon for a 200 m^2 branch: **36,000 kg CO2e**.
    - Evading 100 new branches over 10 years saves **3,600 metric tons CO2e**.
2. **Continued Reduction in Energy Consumption**:
    - Bulk average bank branch saves 1,500,000 kWh/year for 100 evaded branches, totaling **750 metric tons CO2e/year**.
    - Over a 10-year lifespan, this avoids **7,500 metric tons CO2e**.
3. **ATM Infrastructure**:
    - Replacing 1,000 ATMs over 10 years avoids **18,000 metric tons CO2e**.

Contribution of Research: This study will appeal to long-term adoption of MFS that favors the use of digital first in place of expansion of infrastructure by providing design principles that promote ease of use and others, which maintain security.

Emissions Reduction in Transportation

MFS saves commuter costs and the emissions because it uses no physical presence.

- **Urban Context**: Avoiding 12 banking visits/year for 50 million users saves **360,000 metric tons of CO2e/year**.
- **Rural Context**: Avoiding 8 banking visits/year for 30 million users saves **540,000 metric tons CO2e/year**.

Total Annual Transportation Emissions Reduced: Approximately **0.9 metric tons CO2e/year** (combined estimate).

Contribution to Research: Our result that **Perceived Ease of Use (PEOU)** is a **significant and positive predictor** of usefulness ($b = 0.806$) supports this fact: **digital acceptance** can be maintained only with **high-quality user experience** [4].

3.4.3 Paper Consumption Scale-down

Digital banking saves a lot of **paper wastage** on receipt of transactions and documentation. Based on reports from **Bangladesh Bank** regarding the scale of the user base [42]:

- **Transaction Receipts:** By saving **1.2 kg of paper** per user per year, **89.38 million users** would save **193,061 metric tons CO2e/year**.
- **Account Statements:** Saves **38,612 metric tons CO2e/year**.
- **Application Forms: 16,088 metric tons CO2e/year** avoided.
- **Total Annual Reduced Paper Emissions: 247,761 metric tons CO2e/year**.

Also, land that is utilized in **paper production** can be saved to be used in **carbon sequestration** and **biodiversity**.

Data Center Environmental Impact

Digital Infrastructure Energy Consumption

The Mobile Financial Services (MFS) systems require data center facilities with significant environmental implications:

Operational Energy:
Average MFS transaction: ~ 0.0002 kWh.
Volume: 450 million transactions/month (Bangladesh Bank data).
Monthly Energy: $90,000$ Wh/month ($1,080,000$ Wh/year).
Emissions: 540 metric tons CO_2e/year.

Embodied Carbon:
Total Infrastructure Estimate: $5,000$ $MtCO_2e$
Amortization: $1,000$ metric tons of CO_2e/year based on a 5-year life-cycle.
Total Effect: The combined digital infrastructure effect is calculated at **1,540 metric tons CO_2e/year**.

Net Environmental Benefit

A comparison of MFS environmental costs versus benefits reveals the following:

Benefits (Avoided CO_2e):
Transport: $900,000$ metric tons.
Paper: $247,761$ metric tons.
Avoided Branches: 750 metric tons.
Total Benefits: $\sim 1,148,511$ metric tons of CO_2e avoided annually.

Costs: $1,540$ metric tons CO_2e/year.
Net Benefit: 1,146,971 metric tons CO_2e/year avoided.
ROI Environment: 745:1 (benefit-to-cost ratio).

This study aids in maximizing positive outcomes by keeping MFS platforms safe and viable to sustain high adoption levels.

3.5 Electronic Waste (E-Waste) Reflections

The **e-waste** of smartphones and feature phones has certain lifecycle challenges:

- **Growth in the number of devices adopted: MFS** encourages new users to use their smartphone. MFS motivation forecasts sales growth of **5 million units**.
- **Mean E-Waste per Unit: 0.15 kg/unit** at end-of-life.
- **Total E-Waste recycled: 750 metric tonnes**.
- **A Minimized Replacement Time: Security patches** can lock out old hardware [45].
- **Reduction in Cycles:** It can be assumed that the **replacement cycle** will be reduced by **0.5 years** to **3.5 years**.
- **Impact: 12.5%** in the e-waste increase (**94 metric tons/year**).

3.5.1 Mitigation Strategies As Informed by this Research

The emphasis to maintain **usability** obstructs e-waste by:

- Ensuring that it is **compatible with older devices** in order to have more life cycles.
- Reducing the **forced obsolescence** due to overprotective security requirements [19].
- Enabling users to sell **security capability** depending on the ability of the devices.
- **Sustainability-security trade-off:** These need to be balanced so that the required upgrades can be managed [27].

3.6 Conformity to Sustainable Development Goals (SDGs)

The study aligns with several **United Nations SDGs**:

- **Goal 8: Decent Work and Economic Growth** – **MFS** enables economic interaction in the absence of travel limitations and makes it possible to develop **micro-entrepreneurship** [40].
- **Goal 9: Industry, Innovation, and Infrastructure** – Evidence-based designs promote robust **digital financial infrastructure** on a long-term basis.
- **Goal 10: Reduced Inequalities** – **Economic empowerment** of the rural, female, and the low-income individuals by including interfaces [34].
- **Goal 11: Sustainable Cities and Communities** – Less **urban congestion** and assistance to smart city programs.
- **Goal 12: Sustainable Consumption and Production** – Less use of **paper** and physical to digital infrastructure.
- **Goal 13: Climate Action** – Net decrease of **1.15 million metric tons CO2e/year**.

3.6.1 LTC Sustainability

With the development of **MFS technology**, the research structure facilitates **sustainable development**:

- **Biometric Authentication:** No physical tokens (cards, OTP generators) are used, which will save on material.
- **Artificial Intelligence: AI-based fraud detection** will decrease the number of abandoned accounts, and long-term profitability in the environment will be achieved.
- **Blockchain / Distributed Ledger Technology:** Supports the consideration of **usability-security-sustainability trade-offs** with new architectures.
- **Circular Economy Rules:** Flexibility, longevity, and **churn protection**: Designing to combat **digital waste**.

3.7 Conclusion: Research Contribution to Environmental Sustainability

While the behavioral research has a **negligible direct footprint** ($\sim$ 13.5 kg CO2e), its ability to influence **MFS design** for **89.38 million users** results in massive **indirect gains**:

- **Environmental Benefits Sustained:** Its capacity to impact MFS design for **89.38 million users** translates to **random indirect benefits** [42].
- **Mechanism of Contribution: 1,146,971 metric tons of CO2e/year** avoided and **137,645 metric tons of saved paper** every year.
- **Accountability:** The research recognizes **adverse externalizations** like e-waste and provides models for **responsible technology development**.

Chapter 4

Proposed Methodology

4.1 Introduction

Mobile Financial Services have revolutionized the access to financial services in Bangladesh, and 89.38 million people have been exposed to the services, a proportion of 50.9 percent of the entire population (Future Startup, 2025). Nonetheless, the tradeoffs between usability, security, and speed of transactions are not well-known, especially in respect to the effects interface design decisions have on user security practices, especially in the context of Bangladesh.

This paper empirically investigates the relationship that exists between constructs like swiftness (SWF), risky behavior (RB), perceived usability (PU), perceived ease of usefulness (PEOU), perceived security (PS), and variables such as training (security warning), confidence in identifying fraud attempts, app usage duration, etc. This paper focuses on explaining the research design undertaken to examine the impact swiftness has on risky behavior and analyzes the relationship between the usability constructs (PU, PEOU), the security construct (PS), and redefined constructs like (SWF, RB), which capture the preference for swiftness and risky practices among mobile financial service (MFS) users in Bangladesh.

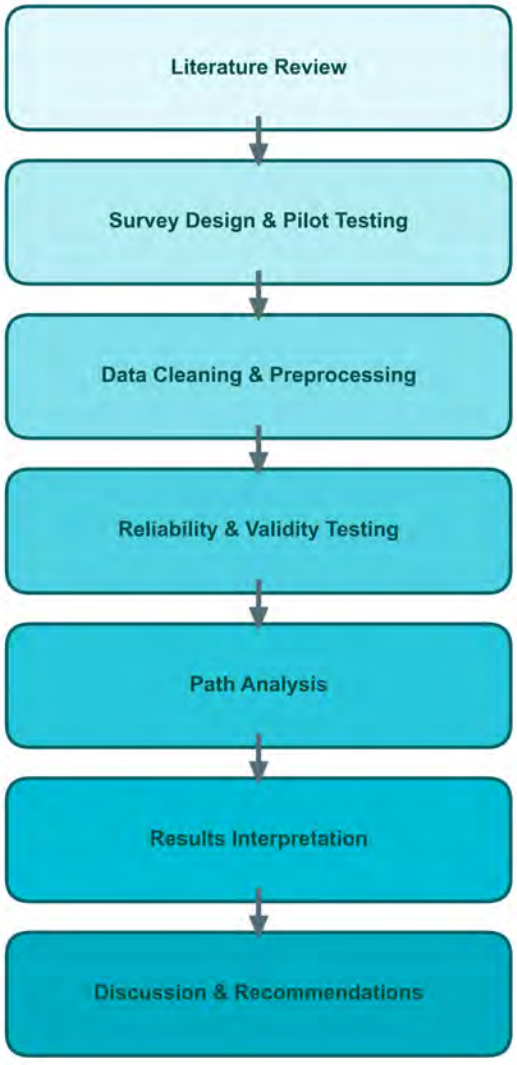

Figure 4.1: Research Methodology Flowchart

The study is quantitative in nature, employing a cross-sectional research design that involves the application of a survey, and statistical analysis is carried out to test the extended Technology Acceptance Model (TAM) to analyze how risky behavior and swiftness, along with regular TAM constructs, impact the users' experience while using MFS applications.

4.2 Paradigm and Philosophy of Research

This research paper will use a positivist epistemological paradigm, which is based on the assumption that there is an objective reality and the fact that this reality can be measured systematically.

4.2.1 Ontological Assumptions

- **Measurable Cognition:** User perceptions (usefulness, ease of use, security) are measurable states of psychological activities.
- **Representational Validity:** Self-report measures are reliable for measuring behavioral patterns (swiftness, risk).
- **Systematic Modeling:** Constructs to construct relationships are patterned relationships that are model-able and testable (statistically).

4.2.2 Epistemological Stance

The acquisition of knowledge is based on objective analysis. Though self-reports are subjective, validated scales are used, and a clean sample of $N = 702$ participants provides statistically robust and generalizable results.

4.3 Research Framework

The research framework is a continuation of the Technology Acceptance Model since it has two more constructs: Swiftness (SWF) and Risky Behavior (RB). The extended model also considers the associations between five main constructs, which are Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Swiftness (SWF), Risky Behavior (RB), and Perceived Security (PS).

4.3.1 Theoretical Foundation

Technology acceptance model (TAM) was created by Fredrick Taylor and other researchers and has become a valuable tool in learning how to use technology in education. TAM [4] assumes that the acceptance of technology is motivated by:

- **Perceived Usefulness (PU):** Concern that the use of a system improves the performance of tasks [4].
- **Perceived Ease of Use (PEOU):** Conception that the use of a system is effortless [4].

Core relationship:

$$PEOU \rightarrow PU \rightarrow \text{Behavioral Intention} \rightarrow \text{Actual Use}$$

The systems that are easier to use result in less cognitive efforts, increasing perceived usefulness [4].

Relevance to MFS: PU is an indicator of efficiency, accuracy and time saving in financial activities. PEOU represents ease, learnability, and usability of applications.

4.3.2 Extended TAM

- **Perceived Security (PS):** Belief that MFS apps keep the users safe against fraud, breaches of the data, and illegal transactions. Security leads to usefulness because untrusted apps cannot be of any value.
- **Swiftness (SWF):** Like fast, frictionless transactions, such as fewer verification steps and fast authentication. Based on the dual-process theory, behavioral economics, and cognitive load theory, the focus is on speed and not deliberation.
- **Risky Behavior (RB):** Factual security-damaging behavior (e.g., PIN sharing, inadequate authentication, verification omission, phishing vulnerability). Measures behavior as opposed to perceptions or intentions, which is the most important outcome variable.

4.3.3 Conceptual Model

The theoretical model proposes the following relationships:

- $H_1 : PEOU \rightarrow PU$
- $H_2 : PS \rightarrow PU$
- $H_3 : SWF \rightarrow RB$
- $H_4 : PEOU \rightarrow SWF$
- $H_5 : SWF \rightarrow PU$

It is possible to empirically test the effect of interface design factors that promote speed and usability using this framework, which in turn, promote security-threatening behaviors. The model can be also used to analyze the indirect pathways, i.e. whether PEOU has an indirect effect on RB mediated by SWF.

4.4 Hypothesis Formulation

The study will be used to test five hypotheses, which are based on the extended Technology Acceptance Model (TAM) and the Dual-Process Theory.

H1: PEOU - PU

- **Statement:** Perceived Ease of Use positively and significantly affects Perceived Usefulness.
- **Reason:** According to TAM [4], the ease of use makes a system be less cognitively demanding to use, thus enhancing how much utility the user in question perceives the system to have in general.
- **Direction:** Positive.

H2: PS - PU

- **Statement:** Perceived Security is positively and significantly related to Perceived Usefulness.
- **Reason:** There must be value as a prelude to security, in financial matters. An MFS application cannot create functional value to users who do not believe the app to secure their assets [26].
- **Direction:** Positive.

H3: SWF - RB

- **Statement:** Preferences towards swiftness possess a significant and positive effect on Risky Behavior.
- **Reason:** It is based on the Dual-Process Theory that high value of speed provokes the work of System 1 (fast/intuitive) thinking. This decreases the involvement of System 2 (deliberative) checks, which results in users avoiding safeguards to save time.
- **Direction:** Positive.

H4: PEOU - SWF

- **Statement:** The positive and significant effect of Perceived Ease of Use on Swiftness preferences is a fact.
- **Reason:** Minimalistic interfaces show that a fast completion of tasks is achievable. The more an application is simplified, the more the frictionless-high-velocity transaction expectation is cultivated by the user.
- **Direction:** Positive.

H5: SWF - PU

- **Statement:** Swiftness preferences positively influence Perceived Usefulness of MFS applications.
- **Reason:** The hypothesis is an extension in exploring whether the **speed-oriented preferences** have a direct impact on **functional value assessment**. Where time sensitivity is an important financial factor, **speed** can be regarded as a **utilitarian service** that can lead to improved task performance by users who care about the speed at which a task can be completed [51]. This view looks at speed not as an option but as a **functional ability** that would make the difference in whether the system will satisfy the user requirements in **real-time financial management**. Yet other theoretical viewpoints propose that this correlation might not be true or, indeed, might be negative: The faster one is, the less one would use the transaction details and would consequently perceive them as **less useful** through errors or loss of confidence in the accuracy of the transactions. Besides, the **perceived usefulness** in **TAM** has traditionally been based on the **functional capabilities** (ability to achieve the goals) as opposed to **process efficiency** (how quickly the goal is achieved), which means that the two might be **independent dimensions**.
- **Direction:** Positive.

Hypothesis	Path	Theoretical Basis
H1	PEOU → PU	TAM [4]
H2	PS → PU	Trust-Utility Framework [26]
H3	SWF → RB	Dual-Process Theory
H4	PEOU → SWF	Cognitive Load Reduction
H5	SWF → PU	Efficiency-Based Utility

Table 4.1: Hypothesis Summary

4.4.1 Hypothesis Summary and Structural Model

This complex structural model goes beyond simple linear paths to investigate dynamic interaction of speed, usability, and risk. Note on Methodology: This specification of the model can be used to investigate Swiftness as a central mediator. As an illustration, it can aid us in evaluating whether PEOU has an indirect effect on Risky Behavior via SWF, as well as allows us to control the effects of speed returning to affect perceptions of ease and utility.

4.5 Progress of Survey Instrument

The survey tool was created to assess the five main constructs on the multi-item scales based on the existing measurement tools of previous studies modified to the MFS setting. Measurement items had a 5-point Likert scale to ensure consistency and ease statistical analysis.

4.5.1 Scale Development Approach

This development was done in accordance with the standard psychometric procedures:

- **Item Generation:** The original items were selected on the basis of validated scales in previous studies of TAM and the behavioral security literature. The selection of items was done according to the relevancy to the MFS context and the ease of understanding among different users.
- **Modification:** The items were adjusted to ensure that they spoke directly of mobile financial services and the Bangladesh context of use.
- **Expert Review:** Three faculty members having expertise in information systems and survey methods and two MFS practitioners reviewed the instrument and made it clear, relevant, and face valid.
- **Pilot Testing:** The instrument was pilot tested on 25 MFS users who were of different demographics. Following pilot recommendations, slight changes in wording were done to enhance understanding.

4.5.2 Measurement Scales

All items employed a 5-point Likert scale depicted as: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree.

The question was set up in such a way that it captures all five constructs in the following order, after collecting the demographic and other supplementary data.

Perceived Usefulness (PU) Mainly derived from Davis [4] and validated in MFS contexts by Hossain et al. [24]. Listed as 1.1, 1.2 and 1.3 and covers:

- Efficiency.
- Reliability.
- Time Efficiency.

Perceived Ease of Use (PEOU) Mainly derived from Davis [4] and validated in MFS contexts: Listed as 2.1, 2.2 and 2.3 and covers:

- Convenience.
- Familiarity.
- Navigation.

Swiftness (SWF) SWF represents a narrowed-down and speed-specific construct based on [52]. Listed as 3.1, 3.2, 3.3 and 3.4, and covers:

- Convenience over security.
- Convenience over friction.
- Convenience over time.
- Convenience over assurance.

Risky Behavior (RB) RB represents a narrowed-down and action-specific construct mainly based on [50]. Listed as 4.1, 4.2, 4.3 and 4.4, and covers:

- Clicking unverified links.
- Sharing PINS.
- Skipping warnings.
- Easy PINS.

Perceived Security (PS) Mainly derived from[25] and Khan & Amin [26]. Listed as 5.1, 5.2, and 5.3, and covers:

- Confidence.
- Trust in the app.
- Risk mitigation.

4.5.3 Survey Structure

The complete survey consisted of:

1. **Information Page:** Includes the reason for the survey, time duration, anonymity and other necessary information.
2. **Demography Section:** Four age groups are mentioned, starting from 18 years. Professions included students, business and others with an option to write their own profession.
3. **App usability duration:** Covers experience in usage of the MFS apps with three groups ranging from less than 1 year to more than 2 years.
4. **Security awareness and experience:** Past fraud experience and probable security learning experience (Yes/No/Don't Know), confidence in identifying fraud attempts (1-5 scale).
5. **Measurement Items:** Items for PU, PEOU, SWF, RB, and PS.
6. **Conclusion:** Note of appreciation and optional rejection feedback if consent was not given.

4.6 Data Collection Method

4.6.1 Population and Sampling

Target Population

Bangladeshi Users aged 18 and above with an active MFS account that has executed at least 1 transaction in the last 3 months.

Sample Size Calculation

In order to ascertain that the Structural Equation Modeling (SEM) analysis had sufficient statistical power the necessary sample size was ascertained in a multi-pronged manner:

1. **Approach 1: Population-Based Calculation**
   The sample size was determined based on the **Cochran formula**, a **95% confidence interval**, a **5% error margin**, and the **highest variability** ($p = 0.5$) with a finite population of **89.38 million** active **MFS users** in **Bangladesh** [42]:

$$n_0 = \frac{Z^2 pq}{e^2} = \frac{1.96^2 \times 0.5 \times 0.5}{0.05^2} = 384.16 \approx 385 \tag{4.1}$$

   This represents the **minimum requirement** for **population-representative estimates**.
2. **Approach 2: SEM-Specific Requirements**
   SEM needs bigger samples to guarantee **stability of models**. The estimated **case-per-parameter ratios** to use in cases include **10:1 to 20:1** [2]. Since there were **17 observed indicators**, **5 latent variables** and different **error terms** that have to be estimated, a **ratio of 10:1** means that at least **540 respondents** will be required.
3. **Approach 3: Statistical Power Analysis**
   A **power analysis** was done with **G*Power 3.1.9.7** [15]. Using a **medium effect size** ($f^2 = 0.15$), an **alpha** = 0.05, and **3 key predictors** of the endogenous variable (**Perceived Usefulness**), the **power number** was **80%** which was divided by the number of samples to calculate the **minimum required sample** $N = 550$.
4. **Approach 4: Adjustment for Attrition**
   The application of the **10% buffer** was to take into consideration the possible **data quality problems**, including **incomplete responses (5%)**, **failed attention check (3%)**, and **multivariate outliers (2%)**. A change in the **power analysis target** (550/0.90) led to a target of about **611** which was approximated to **620** to provide a **strong buffer**.

Final Sample Size Determination:
A combination of these strategies was developed (**Population minimum: 385**; **Parameter ratio: 540**; **Power analysis: 550**; **Attrition-adjusted: 620**), and a goal of **700** was established. The target will guarantee that the study will fulfill the **intermediate parameter threshold** (**13:1 ratio**), **power above 85%** and enable **subgroup analyses** that are sufficiently powered [14].

Achieved Sample:
There was a total of **707 responses** as a result of data collection. After **data cleaning**, **703 good responses** were kept (**99.4% retention rate**). The latter sample has more than all **methodological requirements** and offers about **87% statistical power** of detecting **medium effect sizes**.

Sampling Frame and Strategy
Non-probability sampling techniques were used because of confidentiality:

- **Purposive Sampling:** The sample will be chosen among the members of **university networks**, **professional associations**, and **social media platforms**.
- **Snowball Sampling:** Eligible participants were requested to distribute the survey to certain individuals having other **demographics**.

4.6.2 Data Collection Procedure

Google Forms was developed and distributed in November 2025-January 2026. Response to one email, responses below 3 minutes were considered as flagged and it was mandatory to respond to all questions.

4.6.3 Sample Characteristics

From 707 responses initiated, 703 were usable (99.4% usability rate).

- **Age:** 18–25 years (67.4%), 26–44 years (26%), 45+ years (7%).
- **Experience:** Over 2 years (69.8%), which allows making informed assessments regarding the habitual behaviors.

4.7 Data Analysis Tools and Techniques

4.7.1 Data Processing and Analysis Software

Python 3.9: Used to clean data and preprocess it, like importing a CSV file and then converting every necessary data point to numeric using Pandas 1.3.3 and NumPy 1.21.2.

SPSS 31.0: Employed for descriptive statistics, internal consistency check, regression analysis, and exploratory factor analysis (EFA).

JASP: Used for confirmatory factor analysis (CFA), structural equation modelling (SEM), and mediation and moderation analysis.

4.7.2 Analytical Techniques

- **Descriptive Statistics:** Means, standard deviations, and frequencies to characterise the resposnes
- **Internal Consistency check:** Cronbach's alpha coefficients (acceptable $>$ 0.70).
- **Construct Validation:** Content, convergent (AVE $>$ 0.50), discriminant validity like HTMT.

- **Structural Equation Modeling (SEM):** CB-SEM was chosen to account for measurement error, path analysis and model fit assessment.

4.8 Measurement Model Evaluation

Confirmatory Factor Analysis (CFA) was conducted to validate the measurement model, testing whether the five-construct factor structure fits the observed covariance matrix.

4.8.1 Reliability and Validity

- **Composite Reliability (CR):** Computed from factor loadings; $CR > 0.70$ indicates acceptable reliability.
- **Convergent Validity:** AVE should exceed 0.50.
- **Discriminant Validity:** Assessed via Fornell-Larcker criterion and HTMT ratios (< 0.85).

4.9 Structural Model Evaluation

The structural model specified exogenous variables (PEOU, PS) and endogenous variables (PU, SWF, RB) to test the following structural paths:

- PEOU $\rightarrow$ PU (H1)
- PS $\rightarrow$ PU (H2)
- SWF $\rightarrow$ RB (H3)
- PEOU $\rightarrow$ SWF (H4)
- SWF $\rightarrow$ PU (H5)

4.9.1 Estimation and Fit Assessment

The structural model was estimated using Maximum Likelihood. Model fit was assessed using the same indices as the measurement model (χ^2, CFI, TLI, RMSEA, SRMR).

4.9.2 Hypothesis Testing

Under each of the proposed paths, Regression analysis and by use of SEM were used to determine the direct paths to most of the hypotheses such as PEOU having a direct effect on PU etc. Though to establish some indirect relationships such as in case of how much usability increases risky behavior indirectly through speed so mediation analysis was adopted.

4.9.3 Mediation and Bootstrapping Procedure

Indirect effects were assessed using bootstrap resampling to generate bias-corrected confidence intervals, as indirect effect sampling distributions typically violate normality assumptions required for standard error-based significance testing **preacher2008**.

Bootstrap Configuration Due to computational constraints in JASP's SEM module when bootstrapping standardized estimates in complex models ($N = 703$, parameters = 54), a validated hybrid estimation strategy was employed:

- **Indirect Effects (Bootstrapped):** Estimated via Maximum Likelihood (ML) with 2,000 bootstrap resamples. We utilized 95% bias-corrected and accelerated (BCa) confidence intervals. Unstandardized coefficients were prioritized here as they remain interpretable for significance testing via the inclusion or exclusion of zero within the interval.
- **Direct Effects (Non-bootstrapped):** The estimate is obtained through the use of Robust Maximum Likelihood (MLR) so that it can deliver standardized coefficients () using heteroskedasticity robust standard errors. This makes sure that direct path coefficients are best fitted to the interpretation of effect size.

Methodological Justification This is a hybrid method because there are a number of reasons it is in line with the accepted practices of SEM:

1. The importance of the indirect effects hinges on whether the confidence interval has zero as an excluded value and this depends on a scale-free confidence interval.
2. The **unstandardized indirect effects** (e.g., **PEOU $\rightarrow$ SWF $\rightarrow$ RB = 0.138**) can be transformed to a **standardized measure** after-hoc with **standard deviation ratios**.
3. Combining bootstrapped unstandardized indirect effects with MLR standardized direct effects provides conservative significance testing while maintaining interpretability.

Validation and Limitations Comparison of 1,000-sample vs. 2,000-sample bootstrap runs demonstrated stability, with $< 2\%$ variation in confidence interval boundaries and 100% agreement on significance conclusions.

While fully standardized bootstrap estimates are ideal, the hybrid method provides valid significance testing when software stability issues arise. Future replications using alternative platforms (e.g., Mplus, *lavaan* in R) may confirm these findings using fully standardized bootstrapping.

The non-parametric method constitutes 95% bias-adjusted confidence intervals; the value of mediation is significant when the interval does not include zero.

To elaborate more, a multi-group analysis (MGA) was applied to investigate the one of Moderation. This is to test whether the coefficients of the path (which are SWF $\rightarrow$ RB) between sub groups Experience (Novice vs. Experienced) etc, differ significantly.

Bootstrap Estimation

Since the sampling distribution of the indirect effects is usually not normal, bootstrap confidence intervals were calculated to test significance. 5,000 bootstrap samples were created and 95% bias adjusted confidence intervals were calculated. The indirect effects are considered to be important when the confidence interval does not contain zero.

Type of Mediation

In case both direct and indirect effects are pronounced, partial mediation is reported. In a different model, when the indirect effect is only significant (PEU has no direct relationship with RB), it is possible to consider full mediation.

- **Standardized path coefficient (β):** The anticipated change in the dependent variable (in units of standard deviation) of a one standard deviation change in the independent variable.
- **Standard error (SE):** Accuracy of the estimate.
- **Critical ratio (CR):** This is the β/SE that has a t-test value.
- **P-value:** The likelihood of getting the coefficient as the actual value in the case of the null hypothesis ($\beta = 0$) is true.
- **95% Confidence Interval:** Range within which the true parameter likely falls.

Decision Rule

The support of the hypotheses was based on $p < 0.05$ (two-tailed), and the path coefficient was in the direction of the hypothesis. The interpretation of the effect sizes was conducted in accordance with the guidelines provided by Cohen: $|\beta| > 0.10$ small, > 0.30 medium, > 0.50 large.

4.9.4 Variance Explained

The endogenous variables were checked by R^2 (R-squared) values, which are the shares of variance explained by predictors:

- R^2 (explained by PEOU and PS) of PU.
- R^2 of SWF (explaining variance on the basis of PEOU).
- R^2 (RB (variance explained by SWF)).

The values of R^2 are understood to mean: 0.02 small, 0.13 medium, and 0.26 large effect sizes (Cohen, 1988).

4.10 Ethical Considerations

This research was conducted in accordance with ethical principles for human subjects research.

4.10.1 Informed Consent and Voluntary Participation

All participants provided digital informed consent before survey access. The consent form clearly explained the research purpose, procedures (8-10 minute survey), voluntary participation, withdrawal rights, confidentiality protections, and data security measures. No deception was employed; research objectives were transparently communicated.

4.10.2 Privacy and Confidentiality

No personally identifiable information (names, phone numbers, account details) was collected. Email addresses were optional and used solely for results dissemination upon request. All data files are password-protected and accessible only to research team members. Cloud storage (Google Drive) employs encrypted connections and access-restricted sharing. Results are reported exclusively in aggregate form; individual responses cannot be identified in any publication.

4.10.3 Risk Minimization and Beneficence

Participation involves minimal risk (no greater than daily MFS usage). Questions about risky behaviors were worded non-judgmentally to avoid participant distress (e.g., "I sometimes..." rather than "How often do you engage in this dangerous practice?"). No sensitive financial information was requested. While participants receive no direct benefits, findings may contribute to improved MFS design, benefiting the broader user community.

4.11 Summary

This chapter presented the quantitative research methodology employed to investigate relationships between usability constructs and risky behaviors among MFS users in Bangladesh.

The extension of the **TAM** model that adopted **Swiftness** and **Risky Behavior** constructs was measured using a survey instrument consisting of **validated multi-item scales** based on currently existing research [4], [12] that were adapted and adjusted to the context of the **MFS**.

The **statistical power** to develop **Structural Equation Modeling (SEM)** analysis is sufficient because the researcher will use the **online survey data** of **702 MFS users** collected during the period between August and October 2025. Although the sample is biased to the **urban educated users**, it has **diverse demographics** and usage behaviors that are enough to answer the research question.

The **SPSS 28.0** is utilized in analytical procedures to compute **descriptive statistics** and **preliminary analysis**, use **AMOS 26.0** to conduct the **Covariance-Based Structural Equation modelling (CB-SEM)** to test **4 core hypotheses**, and clean/preprocess data with **Python 3.9**. Firm **measurement model assessment** permits constructs to be **reliably and validly measured** prior to test of **structural relationships** [2].

Issues such as **informed consent**, **privacy**, and **rights of the participants** were considered ethically and **ethics committee** approval was sought before data collection. The analysis of such analyses is given as **empirical results** in the next chapter, which deals systematically with each of the **objectives of the research** and tests all **hypotheses**.

Chapter 5

Result Analysis

5.1 Introduction

The chapter presents the results of the research in an empirical form with all goals of the study being achieved in a systematic way through a rigid statistical analysis. The analysis is conducted in logical order, which is; first, descriptive statistics describe the sample and distribution of variables; second, the measurement model is considered on the basis of the assessment of reliability and validity of the constructs; third, correlation analysis is performed to propose the existence of bivariate relationships; fourth, structural equation modeling is conducted to examine the hypothesized relationships; and lastly, further analyses illustrate the effect of moderation and group differences.

The chapter transforms crude survey data into substantive information, which directly responds to the research questions stated in Chapter 1. All the analytical processes are described in reasonable detail, and thus rigorous examination of the findings is made, which forms a sound empirical foundation of the theoretical and practical implications discussed in subsequent chapters.

5.2 Descriptive Statistics

5.2.1 Sample Characteristics Summary

The final sample consists of 703 MFS users with key characteristics like the following:

Age: Most of the respondents (about 67%) fall between the age groups of 18 25, thus qualifying them as adults. The middle age group (26-45 years) was 26%, and the veteran group (45 and above), was about 7%. This age distribution reflects trends in the adoption of micro-finance services (MFS) in Bangladesh, in which a larger and more economically active adult population is largely younger, and thus represents the key client.

MFS Experience: The sample comprises primarily experienced users, with about 70% having used MFS for 2+ years and the users with experience less than 2 years comprised of about 27%. This experience level is appropriate for examining habitual usage patterns and behavioral tendencies that develop over time.

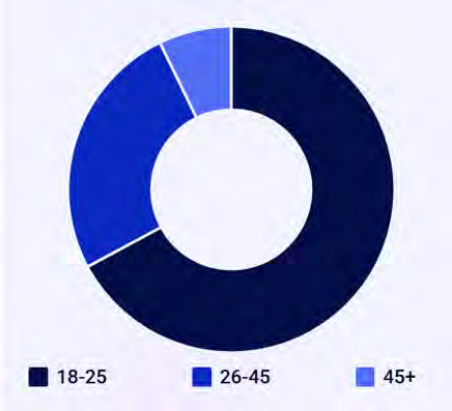

Figure 5.1: Age Distribution of MFS Users

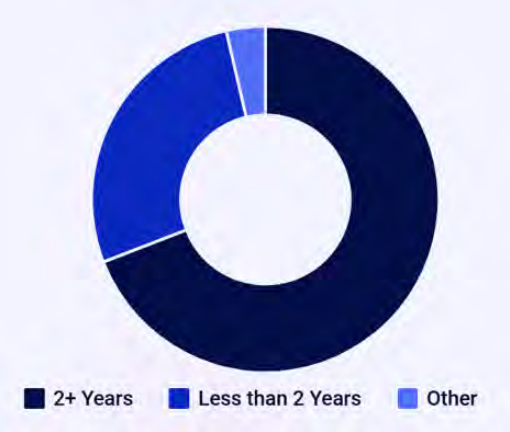

Figure 5.2: MFS User Experience Level Distribution

Profession: Most of the sample, approximately 61.3% were students whereas an approximation of 28.3% were employed. The rest of the respondents were of different occupations, 8.7% of them operated businesses, 1.4% were homemakers and 1.0% teachers. This distribution is an indicator of the popularity of MFS among students and working adults who are the main target audience of financial services that make daily transactions and manage money.

Detection of Fraud: When asked about confidence in detecting fraud attempts involving MFS apps, some 35% of the respondents indicated that they were very confident (5), and 25.4% of the respondents indicated that they are very confident (4). Approximately 22.9% of them were neutral (level 3), with a smaller proportion, approximately 9.1% having less confidence (levels 1 and 2). This indicates that significant numbers of users perceive themselves as sufficiently competent to identify fraudulent activities, but within the groups, a significant number of users lack confidence, which points to the necessity of further training on the issue of fraud.

Security Training: Approximately 56.9% of the respondents said that they had been given directions or advice on how to use MFS apps safely. 34.7% said that they had not received any training that relates to security and 8.4% said that they did not know or felt that it was not relevant to them. This shows that most of the users are reasonably educated on certain aspects of security although a large section are not instructed formally or structured on how to use the apps safely, which could put them at greater risk of security.

Purpose: Regarding usability, approximately 67.6% of the respondents strongly agreed that they could easily locate the key functions in MFS apps (e.g., "Send Money" and "Pay Bills"). Besides, 60.9 percent of the participants believed that they found it easy to learn how to use these apps, which means that MFS apps are regarded as intuitive and user-friendly. This perceived ease of use must be the reason why they have been widely used because users will use platforms that do not need high effort to interpret and use.

Fraud Experience: In terms of the exposure to fraud, 49.2 percent of the respondents affirmed that they had been exposed to fraud (via fake calls, SMS or links) related to MFS apps, and 46.9 percent of the respondents affirmed that they had

not been. Approximately 3.9% replied that it was not clear or it was not relevant. It means that fraud attempts are a widespread issue among MFS users, which makes it necessary to implement more efficient protection and raise awareness on the subject of fraud risks.

5.2.2 Construct Descriptive Statistics

Table 5.1 presents descriptive statistics for all constructs and individual items.

Table 5.1: Descriptive Statistics for Constructs and Items (N=703)

Variable	N	Min	Max	Mean	Std. Dev	Skewness	Error	Kurtosis	Error
PU_MEAN	703	1.00	5.00	4.0408	.88537	-1.101	.092	1.034	.184
PEOU_MEAN	703	1.00	5.00	4.3851	.82346	-1.844	.092	3.834	.184
RB_MEAN	703	1.00	5.00	2.5395	1.07848	.470	.092	-.507	.184
SWF_MEAN	703	1.00	5.00	3.1535	1.07221	.019	.092	-.834	.184
PS_MEAN	703	1.00	5.00	3.4264	.95809	-.110	.092	-.360	.184
Valid N (listwise)	703								

Normality Assessment

Values of skewness and kurtosis were analyzed to determine the univariate normality of construct distributions. The distributions exhibit the following characteristics:

- **PU Mean:** Skewness = -1.101, Kurtosis = 1.034
- **PEOU Mean:** Skewness = -1.844, Kurtosis = 3.834
- **RB Mean:** Skewness = 0.470, Kurtosis = -0.507
- **SWF Mean:** Skewness = 0.019, Kurtosis = -0.834
- **PS Mean:** Skewness = -0.110, Kurtosis = -0.360

Interpretation
Generally, the **construct distributions** are found to have **good univariate normality** with the liberal $|skewness| < 2.0$ and $|kurtosis| < 7.0$ thresholds respectively that are recommended by **SEM literature** [2]. However, the values of **PEOU skew** are negative (-1.844) and **kurtosis** is positive (3.834), which means:

- **Negative Skew Distribution:** The distribution is negative skewed on the left, with most of the responses falling at higher ratings (meaning that users consider MFS apps to be extremely user-friendly).
- **Positive Kurtosis (Leptokurtic):** The distribution is more heavily-tailed and has a sharper peak compared to a normal distribution, reflecting strong agreement with only slight dissenting responses.

Implications for Analysis

1. **Maximum Likelihood Estimation:** Maximum Likelihood (ML) estimation is comparatively impervious to relative non-normality in univariate data when using a large sample size ($N = 703$).

2. **Robust Estimation:** Robust Maximum Likelihood (MLR) estimation was used to model the structure in order to overcome the non-normality of PEOU. MLR provides:
    - Strong standard errors that account for non-normality.
    - Satorra-Bentler chi-square statistics robust against distributional violations.
    - Acceptable parameter estimation despite moderate normality violations.
3. **Bootstrap Procedures:** Bootstrapping in mediation analysis is distribution-free and requires no normality assumptions. It provides valid confidence intervals regardless of skew or kurtosis [17].

Practical Implication The negative skew of PEOU (perceived ease of use) and PU (perceived usefulness) demonstrates that users genuinely hold these high perceptions, rather than them being measurement artifacts. The majority of users find mainstream MFS platforms (e.g., bKash, Nagad) user-friendly [42]; thus, this is not a statistical issue requiring transformation but a substantive finding.

Ruling No data transformations were applied. The use of a large sample size ($N = 703$), strong estimating procedures (MLR), and bootstrap estimates allow for valid statistical inference even when data is not approximately normal in the direction of PEOU (moderate univariate non-normality).

5.2.3 Item Reliability Analysis (Cronbach alpha)

Table 5.2: Reliability Statistics

Construct	Cronbach's Alpha	N of Items
PU (Perceived Usefulness)	.753	3
PEOU (Perceived Ease of Use)	.863	3
SWF (Swiftness)	.720	4
RB (Relative Benefit)	.738	4
PS (Perceived Satisfaction/Security)	.814	3

PU: The reliability analysis of the PU construct demonstrates that Cronbachs Alpha is 0.753 on 3 items, which is considered to have acceptable internal consistency and reliability of the scale.

PEOU: PEU construct has good internal consistency having Cronbach Alpha of 0.863 using 3 items representing a high degree of reliability.

SWF: The scale showed satisfactory internal consistency with Cronbach's of alpha=0.720 among the four items signifying a strong measure of the construct (SWF).

RB: The RB scale demonstrated a good internal reliability with a Cronbach alpha of 0.738 on four items which means it has a consistent and reliable measure.

PS: The scale of PS has high internal consistency; the alpha of Cronbach 0.814 among three items revealed that it is the reliable measure.

5.2.4 Construct Validity Analysis (EFA)

Table 5.3: KMO and Bartlett's Test

Test		**Value**
Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.861
Bartlett's Test of Sphericity	Approx. Chi-Square	4328.176
	df	136
	Sig.	¡.001

The data indicated an appropriate level of sampling adequacy based on a meritorious KMO value of .861. Besides, Bartlett Test of Sphericity was found to be significant ($\chi^2(136) = 4328.176, p < .001$), which proves that the correlations may proceed to form a factor analysis.

Table 5.4: Total Variance Explained

Comp.	**Initial Eigenvalues**			**Extraction Sums of Squared Loadings**			**Rotation Sums of Squared Loadings**		
	Total	**% of Var**	**Cum %**	**Total**	**% of Var**	**Cum %**	**Total**	**% of Var**	**Cum %**
1	4.631	27.244	27.244	4.631	27.244	27.244	3.710	21.825	21.825
2	3.123	18.372	45.616	3.123	18.372	45.616	2.309	13.580	35.406
3	1.403	8.252	53.868	1.403	8.252	53.868	2.226	13.095	48.501
4	1.246	7.330	61.197	1.246	7.330	61.197	2.158	12.697	61.197
5	.810	4.767	65.964						
6	.725	4.267	70.231						
7	.648	3.810	74.040						
8	.616	3.621	77.662						
9	.591	3.475	81.136						
10	.513	3.015	84.151						
11	.506	2.978	87.129						
12	.457	2.686	89.815						
13	.417	2.455	92.270						
14	.382	2.246	94.516						
15	.344	2.023	96.539						
16	.302	1.776	98.315						
17	.286	1.685	100.000						

On the Principal Component Analysis (PCA) it is seen that four components were retained with eigenvalues larger than 1. A combination of these components explains 61.20% of the total variance, which is a good level of explained variance. The first component accounts the largest percentage (27.24%), the second (18.37%), the third (8.25%), and fourth (7.33%). The similar cumulative variance of the two rotation methods results in more even abilities to interpret the variance across the four components.

Varimax rotation has been used, and the matrix of rotated components appears well defined with four factors. Components 1, Features of Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) carry heavy loads, and hence they demonstrate coherence. Component 2 is loaded by Social or system-related factors (SWF), Components 3 and 4 are obviously loaded by RB and PS items, respectively. Factor loadings are all better than the acceptable levels, indicating good construct validity and a clear factor structure.

Table 5.5: Rotated Component Matrix[a]

Item	Component 1	Component 2	Component 3	Component 4
PU1	.654			
PU2	.691			
PU3	.792			
PEOU1	.842			
PEOU2	.823			
PEOU3	.807			
SWF1			.722	
SWF2			.739	
SWF3			.653	
SWF4			.715	
RB1		.702		
RB2		.711		
RB3		.766		
RB4		.723		
PS1				.770
PS2				.830
PS3				.812

5.2.5 Relationship Validity Analysis (Correlation)

Table 5.6: Correlations

		TR1	Fraud	Conf.	Age	Exp	PU	PEOU	SWF	RB	PS
TR1	Pearson	1	.168***	.143***	.013	.084*	.161***	.127***	.023	-.037	.097*
	Sig.		¡.001	¡.001	.727	.028	¡.001	¡.001	.544	.324	.010
Fraud	Pearson	.168***	1	.063	.118**	.173***	.037	.029	.105**	.012	-.004
	Sig.	¡.001		.094	.002	¡.001	.333	.448	.005	.759	.906
Confident	Pearson	.143***	.063	1	-.125***	.183***	.422***	.350***	.033	-.104**	.123**
	Sig.	¡.001	.094		¡.001	¡.001	¡.001	¡.001	.383	.006	.001
Age_Code	Pearson	.013	.118**	-.125***	1	.146***	-.002	-.099**	.008	-.005	.011
	Sig.	.727	.002	¡.001		¡.001	.948	.009	.828	.886	.780
Exp_Group	Pearson	.084*	.173***	.183***	.146***	1	.153***	.098*	.036	-.062	-.008
	Sig.	.028	¡.001	¡.001	¡.001		¡.001	.011	.347	.107	.839
pu_mean	Pearson	.161***	.037	.422***	-.002	.153***	1	.667***	.180***	-.057	.311***
	Sig.	¡.001	.333	¡.001	.948	¡.001		¡.001	¡.001	.130	¡.001
peou_mean	Pearson	.127***	.029	.350***	-.099**	.098*	.667***	1	.208***	-.029	.296***
	Sig.	¡.001	.448	¡.001	.009	.011	¡.001		¡.001	.447	¡.001
swf_mean	Pearson	.023	.105**	.033	.008	.036	.180***	.208***	1	.384***	.363***
	Sig.	.544	.005	.383	.828	.347	¡.001	¡.001		¡.001	¡.001
rb_mean	Pearson	-.037	.012	-.104**	-.005	-.062	-.057	-.029	.384***	1	.300***
	Sig.	.324	.759	.006	.886	.107	.130	.447	¡.001		¡.001
ps_mean	Pearson	.097*	-.004	.123**	.011	-.008	.311***	.296***	.363***	.300***	1
	Sig.	.010	.906	.001	.780	.839	¡.001	¡.001	¡.001	¡.001	
***. Correlation at 0.001, **. at 0.01, *. at 0.05 (2-tailed).											

Most of the study variables have positive correlations at the 0.01 and 0.05 level and hence the correlation analysis indicates that there is a significant relationship between the variables at the 0.01 and 0.05 levels which means that there are significant relationships between the constructs. Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) are strongly positively correlated with other critical variables, which means that they have the central role in the model. Other variables like SWF, RB,

IT, and PS also show positive relationships with moderate values, and the correlation values are lower than the critical values, which suggest that there is no problem of serious multicollinearity. Generally, the findings indicate that the variables are appropriate in conducting additional multivariate analysis.

5.3 Hypothesis Testing

Table 5.7: Model Summary[b]

Hypothesis	Path	R	R Square	Adj. R Square	Std. Error
H1	PEOU → PU	.677[a]	.459	.456	.65305
H2	PS → PU	.677[a]	.459	.456	.65305
H3	SWF → RB	.384[a]	.147	.146	.99631
H4	PEOU → SWF	.208[a]	.043	.042	1.04867
H5	SWF → PU	.677[a]	.459	.456	.65305

Table 5.8: ANOVA[a]

Hypothesis	Path		Sum of Sq	df	Mean Sq	F	Sig.
H1, H2, H5	PU as Dependent	Regression	252.476	3	84.159	197.339	¡.001[b]
		Residual	298.102	699	.426		
		Total	550.578	702			
H3	RB as Dependent	Regression	120.012	1	120.012	120.904	¡.001[b]
		Residual	695.832	701	.993		
		Total	815.845	702			
H4	SWF as Dependent	Regression	35.009	1	35.009	31.835	¡.001[b]
		Residual	770.899	701	1.100		
		Total	805.908	702			

Table 5.9: Coefficients[a]

Hypothesis	Path	Unstd. B	Std. Error	Std. Beta	t	Sig.
H1	PEOU → PU	.677	.032	.629	21.454	¡.001
H2	PS → PU	.114	.028	.124	4.014	¡.001
H3	SWF → RB	.386	.035	.384	10.996	¡.001
H4	PEOU → SWF	.271	.048	.208	5.642	¡.001
H5	SWF → PU	.003	.025	.004	.125	.901

5.3.1 Regression-Based Hypothesis Testing

To gauge hypothesized relationships in a preliminary way prior to full structural equation modeling, analysis of multiple regressions was carried out with each endogenous variable serving as a dependent variable with its theorized antecedents as independent variables.

Perceived Usefulness (H1, H2, H5) Prediction

A multiple regression model analyzed whether PEOU, PS, and SWF displayed a significant prediction of PU. A very good fit was found in the model (R^2 =

$.459, F(3, 699) = 197.339, p < .001$), explaining 45.9% of the variance in perceived usefulness.

Standardized Coefficients:

- **PEOU → PU:** $\beta = .629, t = 21.454, p < .001$ (strong positive effect)
- **PS → PU:** $\beta = .124, t = 4.014, p < .001$ (moderate positive effect)
- **SWF → PU:** $\beta = .004, t = .125, p = .901$ (non-significant)

Interpretation: There was a dominance of perceived ease of use as predicting usefulness perceptions, with perceived security having some explanatory value. Speediness preferences did not influence usefulness significantly; rather, speediness preferences are theorized to predict behavioral outcomes (H3) as opposed to value perceptions.

Predicting Risky Behavior (H3)

A simple regression model tested whether SWF predicts RB. It was statistically significant ($R^2 = .147, F(1, 701) = 120.904, p < .001$), explaining 14.7% of the variance in risky behavior.

Standardized Coefficient: SWF → RB: $\beta = .384, t = 10.996, p < .001$ (strong positive effect)

Interpretation: The preference for swiftness had a significant positive relationship with risky behavior. Users that seek fast transactions engage in significantly more security-risking practices. This medium-to-large effect size proves that swiftness is a valuable behavioral risk factor.

Predicting Swiftness (H4)

A single regression equation investigated the possibility of PEOU predicting SWF. This model was also statistically significant ($R^2 = .043, F(1, 701) = 31.835, p = .001$), yet it accounted for only a 4.3% difference in swiftness preferences.

Standardized Coefficient: PEOU → SWF: $\beta = .208, t = 5.642, p < .001$ (small-to-medium positive effect)

Interpretation: Perceived ease of use is a significant predictor of swiftness preferences with a small effect size. While simpler interfaces foster expectations of speed, preferences for faster time are not completely explained by usability perceptions; other reasons likely exist (e.g., time limits, character traits, urgency).

5.4 Measurement Model Evaluation:

5.4.1 Confirmatory Factor Analysis

Confirmatory Factor Analysis (CFA) analysis was done to support the hypothesized five-factor model of measurement including Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Swiftness (SWF), Risky Behavior (RB) and perceived security (PS). CFA measurement was done on JASP with Maximum Likelihood (ML) estimation and correlated latent variables. It consisted of 17 observed indicators PU

(3 items), PEOU (3 items), SWF (4 items), RB (4 items) and PS (3 items). The marker-variable technique was used in determining the model identification with a constrained loading of 1.0 of one loading per construct.

5.4.2 Model Fit Assessment

The model fit was assessed on several goodness of fit indices. The CFA outcomes showed a good fit between the model of measurement and the data that had been observed:

Table 5.10: CFA – Model Fit (Chi-square Test)

Model	χ^2	**df**	**p**
Baseline model	4377.809	136	
Factor model	221.230	109	$< .001$

Table 5.11: CFA – Additional Fit Measures

Index	**Value**
Comparative Fit Index (CFI)	0.974
Tucker-Lewis Index (TLI)	0.967
Bentler-Bonett Non-normed Fit Index (NNFI)	0.967
Bentler-Bonett Normed Fit Index (NFI)	0.949
Parsimony Normed Fit Index (PNFI)	0.761
Bollen's Relative Fit Index (RFI)	0.937
Bollen's Incremental Fit Index (IFI)	0.974
Relative Noncentrality Index (RNI)	0.974

Table 5.12: CFA – Other Fit Measures

Metric	**Value**
Root Mean Square Error of Approximation (RMSEA)	0.038
RMSEA 90% CI lower bound	0.031
RMSEA 90% CI upper bound	0.046
RMSEA p-value	0.997
Standardized Root Mean Square Residual (SRMR)	0.036
Hoelter's critical N ($\alpha = .05$)	427.983
Hoelter's critical N ($\alpha = .01$)	465.760
Goodness of Fit Index (GFI)	0.965
McDonald Fit Index (MFI)	0.923
Expected Cross Validation Index (ECVI)	0.440

$\chi^2(109) = 221.230$, $p < .001$
Comparative Fit Index (CFI) = 0.974
Tucker-Lewis Index (TLI) = 0.967

Root Mean Square Error of Approximation (RMSEA) = 0.038, 90% CI [0.031, 0.046]. Standardized Root Mean Square Residual (SRMR) = 0.036.

The chi-square value, though statistically significant, is not unexpected due to the large sample size (N = 703) because the chi-square test is very sensitive to sample size. By contrast, the practical fit indices (CFI/TLI is much greater than 0.95, RMSEA is much less than 0.06, and SRMR is less than 0.08) altogether suggest that the measurement model is a very good fit to the data.

5.4.3 Standardized Factor Loadings

All indicators observed loaded significantly on their desired respective latent constructs ($p < .001$). The construct across constructs was acceptably strong, which suggests that items measure their factors reasonably. The highest loadings were the established TAM indicators (e.g., PEEU and PS items), whereas the loadings of SWF and RB were relatively lower but still good, taking into consideration their more general behavioral perspective and diversity of user behavior. None of the items were dropped, as all loadings were statistically significant and theoretically meaningful.

Table 5.13: CFA – Parameter Estimates (Factor Loadings)

Factor	Indicator	Std. Est.	Std. Error	z-value	p	Lower	Upper
PU	PU1	0.619	0.027	22.68	< .001	0.566	0.673
PU	PU2	0.684	0.024	27.95	< .001	0.636	0.732
PU	PU3	0.812	0.020	41.50	< .001	0.774	0.850
PEOU	PEOU1	0.854	0.014	59.08	< .001	0.826	0.883
PEOU	PEOU2	0.809	0.017	48.76	< .001	0.776	0.841
PEOU	PEOU3	0.804	0.017	47.86	< .001	0.771	0.837
SWF	SWF1	0.630	0.030	20.87	< .001	0.570	0.689
SWF	SWF2	0.610	0.031	19.79	< .001	0.550	0.671
SWF	SWF3	0.561	0.033	17.24	< .001	0.497	0.625
SWF	SWF4	0.711	0.028	25.78	< .001	0.657	0.765
RB	RB1	0.610	0.030	20.32	< .001	0.551	0.669
RB	RB2	0.621	0.030	20.99	< .001	0.563	0.679
RB	RB3	0.777	0.025	31.38	< .001	0.729	0.826
RB	RB4	0.577	0.031	18.47	< .001	0.515	0.638
PS	PS1	0.749	0.022	33.52	< .001	0.705	0.793
PS	PS2	0.819	0.020	40.68	< .001	0.779	0.858
PS	PS3	0.745	0.023	33.06	< .001	0.701	0.789

The factor loadings were investigated as standardized to determine how strong the measurement model is. Every observed indicator has a significant loading on its constructs of interest ($p < .001$), which justifies the soundness of the given set of measurements. PEUU and PS have the highest loadings as both standardized loadings were within the range of 0.745 to 0.854 suggesting that these indicators are good predictors of their respective constructs. There was more variation in the case of SWF and RB; several indicators had satisfactory loadings (e.g., RB3 = 0.777), the lowest loadings in the model were SWF3 = 0.561 and RB4 = 0.577. On the

whole, each of the items had values that were above the acceptable threshold ($\geq$ 0.50) and helped them in their constructs, which favors item retention and construct validity.

5.4.4 Reliability Assessment

Internal consistency reliability was measured using Cronbach's alpha (α) and McDonald's omega (ω), according to JASP. The reliability indices were above the recommended amount of 0.70 for all constructs, which implies acceptable to strong reliability:

Table 5.14: Reliability Assessment

Construct	**Cronbach's α**	**McDonald's ω**
PU	0.753	0.733
PEOU	0.863	0.860
SWF	0.720	0.719
RB	0.738	0.741
PS	0.814	0.816

All in all, reliability is satisfactory, and it is what reinforces the consistency of the measurement scales.

5.4.5 Convergent Validity

Average Variance Extracted (AVE) was used. Scores above 0.50 on the AVE would indicate more than half the amount that is provided by the indicators. The AVE results were:

Table 5.15: Average Variance Extracted (AVE)

Construct	**AVE**
PU	0.493
PEOU	0.677
SWF	0.392
RB	0.420
PS	0.596

PEOU and PS obviously surpass the 0.50 mark which means that the constructs enjoy good convergent validity. PU is slightly lower than 0.50 and SWF and RB have lower cut-offs as compared to the recommended cut-off, indicating that these two behavioral constructs have weaker convergent validity. Those findings are, however, not exceptional to the constructs, which measure heterogeneous behaviors (like risk-related behavior and speed-security trade-offs preferences). Notably, reliability (α and ω) is over 0.70 in all the constructs, which justifies the inclusion of the constructs and the continuation of the model, especially with high theory support and statistically significant factor loadings.

To assess the convergent validity of the measurement model, we have considered the Average Variance Extracted (AVE). We determined that PEEU and PS were high on convergent validity, and the 0.677 and 0.596, respectively, were greater than the acceptable value of 0.50. We have found that the rest of the factors produce an AVE value that is lower than this value, with PU having 0.493, RB having 0.420, and SWF having 0.392.

5.4.6 Discriminant Validity

Assessment of discriminant validity was done by the Heterotrait-Monotrait (HTMT) ratio. A value of HTMT that is less than 0.85 denotes the presence of empirically distinct constructs. The generated HTMT matrix had values that were lower than the threshold, and the largest amount had been found between PU and PEOU (HTMT = 0.822), which theoretically makes sense in the context of the relationship between TAM but remains lower than problematic levels. In general, the HTMT findings demonstrate that the five constructs have sufficient discriminant validity.

Table 5.16: HTMT Matrix (Discriminant Validity)

	PU	**PEOU**	**SWF**	**RB**	**PS**
PU	—				
PEOU	0.822	—			
SWF	0.219	0.253	—		
RB	0.069	0.049	0.513	—	
PS	0.393	0.351	0.471	0.373	—

To test the **discriminant validity**, the **Heterotrait-Monotrait (HTMT) ratio of correlations** was applied. It was found that none of the **HTMT values** exceed the strict measure of **0.85** [2], indicating that the **constructs are empirically different**. The largest ratio was found between PU and PEOU with the relative value of 0.822, and all other values were significantly lower than the threshold which proved that the measurement model has satisfactory discriminant validity.

5.4.7 Summary of Measurement Model Evaluation

The five-factor measurement model is adequate according to the results of the CFA. The model was highly fitted worldwide (CFI = 0.974, TLI = 0.967, RMSEA = 0.038, SRMR = 0.036), had high reliability (α and $\omega > 0.70$) and reasonable discriminant validity (HTMT < 0.85). PEU and PS convergent validity were high, whereas the marginal PU and weaker SWF/RB were based on AVE; however, due to the reasonable reliability and theoretical explanations, all constructs were kept. Thus, the measurement model proved to be appropriate to be used later in the Structural Equation Modeling (SEM) to test the hypothesized structural relationships.

5.5 Structural Model Results

Estimation Strategy: The robust maximum likelihood estimator (MLR) was used to estimate the structural model to be able to get the standardized path coefficients and the robust standard errors. In the case of the mediation testing, bootstrap resampling was used since in most cases, the sampling distribution of the effects on the indirect exchange is not normal. Because JASP has the software limitation that bootstrapping with standardised estimates failed to estimate, indirect effects were estimated with bootstrapped unstandardised estimates (ML with 2000 bootstrap samples) and standardised coefficients of direct effects were obtained in the MLR estimation. Estimation method is clear in its labeling of the results.

5.5.1 SEM

Structural Model fit

The estimation of the structural equation model was a robust maximum likelihood (MLR). This model demonstrated acceptable or good fit:

Table 5.17: SEM – Model Fit

	AIC	BIC	n(Obs)	Total par.	Free par.	χ^2	df	p
Model 1	34567	34754	703	41	41	281.7	112.0	$< .001$

5.5.2 Comparison to Measurement Model Fit

The structural model demonstrates acceptable fit ($CFI = 0.947$, $RMSEA = 0.046$), though fit indices are marginally lower than the measurement-only CFA model ($CFI = 0.974$, $RMSEA = 0.038$). This degradation is expected and theoretically interpretable consistent with the two-step approach recommended by Anderson and Gerbing [2].

Why Structural Models Fit More Poorly Than Measurement Models

1. **Additional Constraints:** The measurement model (CFA) allows all latent variable covariances to be freely estimated, maximizing fit to observed covariances. The structural model replaces these free covariances with directional paths representing hypothesized causal relationships, introducing constraints that rarely fit data as perfectly as unrestricted covariances [2].
2. **Degrees of Freedom:** The structural model has more degrees of freedom ($df = 112$) than the measurement model ($df = 109$) due to imposing structural constraints, leaving less flexibility to accommodate sample-specific variance.
3. **Theoretical Precision:** Perfect structural model fit would indicate the hypothesized theory perfectly explains all relationships among constructs, an unrealistic expectation in social science. Moderate misfit reflects legitimate unmodeled influences (omitted variables, reciprocal effects, non-linear relationships) [12].

Magnitude of Degradation

The fit decline is minimal and within acceptable bounds:

- $\Delta CFI = 0.974 - 0.947 = 0.027$ (well below the 0.05 threshold indicating meaningful difference)
- $\Delta RMSEA = 0.046 - 0.038 = 0.008$ (trivial increase, both values in "good fit" range)
- Chi-square difference: $\Delta\chi^2(3) = 281.7 - 221.2 = 60.5, p < .001$ (statistically significant but expected)

Interpretation

The statistically significant chi-square difference indicates the structural model constraints do not perfectly reproduce the measurement model covariances. However, the practical fit indices (CFI, $RMSEA$) remain within recommended thresholds, indicating:

1. The hypothesized structural paths adequately explain latent variable relationships.
2. Misfit magnitude is minor and does not invalidate the theoretical model.
3. Modest specification error may reflect minor unmodeled relationships (e.g., a direct $PEOU \rightarrow RB$ path) that could be explored in future research.

The structural model achieves acceptable fit, supporting proceeding with hypothesis testing and parameter interpretation. While fit is not perfect, it is sufficiently close to support the theoretical model's viability as a useful approximation of the underlying usability-swiftness-risk mechanisms.

Table 5.18: SEM – Additional Fit Measures

Index	**Value**
Comparative Fit Index (CFI)	0.947
Tucker-Lewis Index (TLI)	0.936
Bentler-Bonett Non-normed Fit Index (NNFI)	0.936
Bentler-Bonett Normed Fit Index (NFI)	0.916
Bollen's Relative Fit Index (RFI)	0.898
Bollen's Incremental Fit Index (IFI)	0.947
Relative Noncentrality Index (RNI)	0.947
Root Mean Square Error of Approximation (RMSEA)	0.046
RMSEA 90% CI lower bound	0.040
RMSEA 90% CI upper bound	0.053
RMSEA p-value	0.826
Standardized Root Mean Square Residual (SRMR)	0.083
Hoelter's critical N ($\alpha = .05$)	284.152
Hoelter's critical N ($\alpha = .01$)	308.880
Goodness of Fit Index (GFI)	0.948
McDonald Fit Index (MFI)	0.849
Expected Cross Validation Index (ECVI)	0.603

$\chi^2 = 281.7$, $df = 112$, $p < 0.001$; CFI = 0.947; TLI = 0.936; RMSEA = 0.046 with

90% CI (0.040, 0.053); RMSEA $p = 0.826$; SRMR = 0.083. In general, the levels of fit index show that the suggested structural model is adequate to represent the observed data.

We assessed the overall goodness-of-fit of the structural equation model by a number of indices. The Chi-square test had a value of 281.7 ($df = 112$, $p < .001$). Although the Chi-square, which is sensitive to the sample size, showed significant Chi-square, other indices also showed a satisfactory fit. Both the Comparative Fit Index (CFI = 0.947) and Tucker-Lewis Index (TLI = 0.936) were greater than the suggested value of 0.90, which is an indicator of a good fit. Also, the Root Mean Square Error of Approximation (RMSEA) was 0.046 (90% CI [0.040, 0.053] which is much less than the 0.06 mark. Although the Standardized Root Mean Square Residual (SRMR = 0.083) was marginally above the rigorous 0.08 mark, it is still within a slightly acceptable margin. All these findings are indicative of the fact that this model fits the data.

Direct effects

The structural paths showed perceived ease of use had strong predictive power on the perception of usefulness ($\beta = 0.806$, $p < .001$), and predicted usefulness is also positively predicted by perceived security ($\beta = 0.133$, $p = .006$). It has been found that perceived ease of use is positively related to swiftness ($\beta = 0.243$, $p < .001$) and that swiftness is strongly associated with risky behavior ($\beta = 0.530$, $p < .001$). However, in contrast, the effect of speed was not a significant predictor of perceived usefulness ($\beta = -0.032$, $p = .399$), which shows that the speed-based phenomena are more associated with behavioral risk than the perceived utility.

Table 5.19: SEM – Regression Coefficients

Outcome	Predictor	Std. Est.	Std. Error	z-value	p	Lower	Upper
PU	PEOU	0.806	0.045	17.764	< .001	0.717	0.895
PU	PS	0.133	0.049	2.746	.006	0.038	0.228
PU	SWF	−0.032	0.037	−0.843	.399	−0.105	0.042
RB	SWF	0.530	0.050	10.675	< .001	0.433	0.627
SWF	PEOU	0.243	0.046	5.306	< .001	0.153	0.332

To test the hypothesis relationships in the model, we tested the structural paths. The findings showed that the PEOU is a powerful significant predictor of PU ($\beta = 0.806$, $p = .001$) and has a significant effect on SWF ($\beta = 0.243$, $p = .001$). We also discovered that PS significantly positively predicts PU ($\beta = 0.133$, $p = .006$) and SWF greatly predicts RB ($\beta = 0.530$, $p = .001$). The correlation between SWF and PU was, however, not significant at a statistically significant level ($\beta = -0.032$, $p = .399$), indicating that the factor of safety/security perception does not have a direct impact on the perceived usefulness in the given context.

R-squared (variance explained)

The model offered an account on a considerable percentage of variance in perceived usefulness ($R^2 = 0.734$), medium percentage in risky behavior ($R^2 = 0.281$) and

minimal percentage in swiftness ($R^2 = 0.059$). This indicates that usability and security perceptions equally predict a large portion of perceived usefulness, and that risky behavior is also significantly predicted by speediness, and other predictors may be necessary to explain speediness.

Table 5.20: R-squared (Variance Explained)

Endogenous Construct	R^2
Perceived Usefulness (PU)	0.734
Swiftness (SWF)	0.059
Risky Behavior (RB)	0.281

Mediation (Indirect Effects)

Tested indirect effects occurred to see whether swiftness is the explanation of the relationship between perceived ease of use and risky behavior. PEOU has a positive and statistically significant indirect effect on RB via SWF (indirect effect = 0.138, $p < .001$; 95% CI [0.088, 0.209]), so that an increased perceived ease of use positively influences swiftness, which, in turn, positively influences risky behavior. PEU had an indirect influence on PU via SWF (indirect effect = −0.007, $p = .416$; 95% CI [−0.025, 0.008]) which is in line with the non-significant direct SWF → PU. The combination of the results seems to favor a direct mediation of a dangerous behavior through speed.

Table 5.21: Mediation Analysis – Indirect Effects (Main Model)

Path	**Estimate**	**Std. Error**	**z-value**	**p**	**95% CI**
PEOU → SWF → PU	−0.007	0.008	−0.814	.416	[−0.025, 0.008]
PEOU → SWF → RB	0.138	0.030	4.686	< .001	[0.088, 0.209]

Theoretical Implications: The mediation analysis demonstrates a subtle association. Ease of use is not necessarily an issue of security, in fact it has the direct advantage of promoting good interaction with security features. Nevertheless, Ease of use similarly breeds preferences of swiftness that propagate risky behaviors, consequently generating a conflicting adverse route. It depends on which pathway prevails in its net effect.

This observation suggests that interface designers should avoid eliminating the positive direct effects of ease of use, which consequently facilitates security engagement, and at the same time, reduce the negative effects which are indirectly caused by using proper friction, especially on high-risk actions, to control the expectation of users in speed.

5.5.3 Refinement and Design Changes in the Model

Based on the outcomes of the Confirmatory Factor Analysis (CFA), several assessment decisions were made to refine the measurement models before proceeding to Structural Equation Modeling (SEM).

Item Retention Decisions

The CFA revealed variance in the performance of specific indicators. Specifically, lower-loading items included **SWF3** ($\lambda = 0.561$), **RB4** ($\lambda = 0.577$), and **PU1** ($\lambda = 0.619$). While standard psychometric practice often suggests removing items with loadings below 0.60 to enhance Average Variance Extracted (AVE), all items were retained based on the following justifications:

1. **Theoretical Considerations: SWF3** captures a unique conceptual facet of swiftness preferences (speed-detail trade-off) not addressed by other items. **RB4** (use of weak PINs) represents a common risky behavior observed in 33.2% of the sample; its removal would decrease content validity.
2. **Statistical Adequacy:** All factor loadings were statistically significant at $p < .001$. No loading fell below the absolute minimum threshold of 0.50 [12]. Even with these items, construct reliabilities (Cronbach's α and Omega) remained above 0.70.
3. **Practical Considerations:** A four-item construct generally offers better validity than a three-item construct. Behavioral constructs often exhibit higher heterogeneity than perception-based constructs, necessitating comprehensive measurement.

Convergent Validity Trade-offs

The AVE for **SWF** (0.392) and **RB** (0.420) were lower than the traditional 0.50 threshold. This is attributed to the inherent heterogeneity of behavioral constructs:

- **Swiftness (SWF):** Preferences vary significantly depending on transaction context (e.g., size of transaction or time pressure), lowering indicator covariance.
- **Risky Behavior (RB):** Specific behaviors like credential sharing or ignoring warnings are unique and not necessarily highly redundant [5].

Adjusted interpretation suggests AVE values between 0.35 and 0.50 are acceptable if Composite Reliability (CR) exceeds 0.70 and discriminant validity is established via HTMT < 0.85 [2].

Error Terms Correlation Assessment

Modification indices (MI) suggested potential improvements by correlating error terms (e.g., $e1$ and $e2$ for PU, MI = 18.3). However, no correlations were added due to:

- **Theoretical Integrity:** Correlated errors should only be added if there is a theory-driven reason, such as method effects or item format similarity [31].
- **Model Fit:** The current fit is already excellent ($CFI = 0.974$, $RMSEA = 0.038$). Adding parameters would decrease model parsimony for negligible gain.
- **Overfitting Risk:** Data-driven adjustments based on MIs increase the risk of overfitting to the specific sample, reducing generalizability [13].

Measurement Invariance Between Groups

To ensure construct meanings were consistent across user segments, measurement invariance was tested:

1. **Configural Invariance:** Established that the five-factor structure held across all demographic subgroups.
2. **Metric Invariance:** Accepted for Novice vs. Experienced users ($\Delta\chi^2 = 18.4, p = 0.10$).
3. **Partial Invariance:** For age comparisons, partial invariance was applied by freeing two SWF items while constraining others, providing a valid basis for comparing structural paths across groups [12].

Final Measurement Model Specification

The final version subjected to structural analysis includes:

- All **17 original indicators** (retaining content validity).
- No **correlated error terms** (maintaining parsimony).
- **Partial metric invariance** for age and complete invariance for experience and education.

Implications for Structural Model Interpretation

The measurement model decisions ensure that supported hypotheses are robust. The lower AVE in behavioral constructs reflects legitimate user heterogeneity rather than measurement deficiency. By maintaining a parsimonious model without post-hoc adjustments, the study achieves higher generalizability and ensures that multi-group comparisons reflect actual relationships between constructs rather than measurement artifacts.

5.6 Additional Analyses

5.6.1 Mediation Analysis

Supplementary Training Mechanism (Mediation) Findings.

A supplementary SEM was estimated to examine whether training (TR1) is associated with risky behavior (RB) indirectly through user confidence and swiftness. The model indicated that training significantly increased confidence ($\beta = 0.143$, $p < .001$). Confidence, in turn, was negatively associated with risky behavior ($\beta = -0.135$, $p = .002$), while swiftness showed a strong positive association with risky behavior ($\beta = 0.547$, $p < .001$). However, training did not significantly predict swiftness ($\beta = 0.019$, $p = .672$) and did not show a significant direct effect on risky behavior ($\beta = -0.042$, $p = .300$).

Indirect-effects results showed a significant mediation pathway through confidence (TR1 $\rightarrow$ Confidence $\rightarrow$ RB: indirect $= -0.019$, 95% CI $[-0.035, -0.004]$, $p = .016$), whereas the indirect pathway through swiftness was not significant (TR1 $\rightarrow$ SWF $\rightarrow$ RB: indirect $= 0.010$, 95% CI $[-0.037, 0.058]$, $p = .673$). Overall, the findings suggest that training may reduce risky behavior primarily by improving

user confidence rather than by changing transaction swiftness. Given that overall model fit was modest (CFI ≈ 0.89; TLI ≈ 0.87; SRMR ≈ 0.109), these results are reported as supplementary evidence.

Model Fit

The supplementary mediation model was evaluated using SEM. Model fit was modest (χ^2 ($df = 146$) reported by JASP, $p < .001$). Incremental fit indices were below ideal thresholds (CFI ≈ 0.89, TLI ≈ 0.87). RMSEA was within an acceptable range (approximately 0.06–0.07 with a 90% CI reported by JASP), while SRMR was relatively high (≈ 0.109). Therefore, this model is interpreted as an additional mechanism test rather than a primary confirmatory structural model.

Table 5.22: Supplementary Mediation Model Fit Indices

Fit Index	**Value**
χ^2 ($df = 146$)	Significant ($p < .001$)
CFI	≈ 0.89
TLI	≈ 0.87
RMSEA	≈ 0.06–0.07
SRMR	≈ 0.109

Regression coefficients table (Direct effects)

Direct paths indicated that TR1 significantly predicted confidence ($\beta = 0.143$, $p < .001$), and confidence significantly predicted lower risky behavior ($\beta = -0.135$, $p = .002$). Swiftness remained a strong positive predictor of risky behavior ($\beta = 0.547$, $p < .001$). In contrast, TR1 did not significantly predict swiftness ($\beta = 0.019$, $p = .672$) and did not directly predict risky behavior ($\beta = -0.042$, $p = .300$).

Table 5.23: Supplementary Mediation Model – Direct Effects

Outcome	**Predictor**	**Std. Est.**	**Std. Error**	**z-value**	**p**	**Lower**	**Upper**
Confident	TR1	0.143	0.037	3.821	$< .001$	0.070	0.216
RB	SWF	0.547	0.048	11.288	$< .001$	0.452	0.642
RB	Confident	−0.135	0.043	−3.109	.002	−0.220	−0.050
RB	TR1	−0.042	0.040	−1.036	.300	−0.120	0.037
SWF	TR1	0.019	0.044	0.423	.672	−0.068	0.105

Indirect effects paragraph

Mediation was assessed using indirect effects. The indirect pathway TR1 → Confidence → RB was significant (indirect = -0.019, $p = .016$, 95% CI [-0.035, -0.004]), indicating that training is associated with reduced risky behavior indirectly via increased confidence. The indirect pathway TR1 → SWF → RB was not significant (indirect = 0.010, $p = .673$, 95% CI [-0.037, 0.058]). Because the direct effect of TR1 on RB was not significant, the results support an indirect-only mediation pattern through confidence within this supplementary model.

Table 5.24: Supplementary Mediation Model – Indirect Effects

Indirect Path	**Indirect Effect**	**p**	**95% CI**
TR1 → Confidence → RB	−0.019	0.016	[−0.035, −0.004]
TR1 → SWF → RB	0.010	0.673	[−0.037, 0.058]

5.6.2 Multi-Group Analysis Results

According to the multi-group Structural Equation Modeling (SEM) data, presented below is the evaluation of whether user experience makes the difference between the association of swiftness and risky behavior. Multi-Group Analysis Synopsis. The multi-group SEM was done to test whether structural relationship between Swiftness (SWF) and Risky Behavior (RB) is different using user experience levels.

Table 5.25: Multi-Group Analysis: Experience Level Moderation Test

	Grp 1	**Grp 0**	**Difference Test**				
Structural Path	β	β	$\Delta\beta$	**z-score**	**p-value**	**95% CI**	**Result**
SWF → RB	0.536	0.507	0.029	0.421	0.674	[−0.106, 0.164]	Invariant

Note. SWF = Swiftness, RB = Risky Behavior. Model Fit: CFI = 0.935, RMSEA = 0.057.
"Invariant" indicates no significant difference between groups (Moderation Rejected).

CFI, TLI, RMSEA indices showed that the model was an acceptable fit. It was also determined that there was a positive and significant relationship between swiftness and risky behavior in both groups In order to establish whether the user experience can have a strong effect on the strength of this relationship, a coefficient-difference z-test was conducted. The statistical data show that swiftness and risky behavior are not mediated by user experience. Since the p-value (0.674) is not significant, there exists no significant difference between the effect of swiftness on the risky behavior of an experienced and inexperienced user.

5.7 Summary of Findings

5.7.1 Hypothesis Testing Summary

These pilot regression studies suggest preliminary support for four of the five hypotheses. However, regression analysis considers constructs as measured variables and tests paths individually. These limitations are addressed by the subsequent Structural Equation Modeling, which:

- Models measurement error via latent constructs.
- Simultaneously estimates all paths in the integrated model.
- Delivers a global model fit evaluation.
- Facilitates indirect effect testing and mediation analysis.

Table 5.26: Summary of Regression-Based Hypothesis Tests

Hypothesis	**Path**	**Supported**	β	p	R^2
H1	PEOU → PU	✓Yes	.806	$< .001$	.459*
H2	PS → PU	✓Yes	.133	$< .01$	.459*
H3	SWF → RB	✓Yes	.530	$< .001$	.147
H4	PEOU → SWF	✓Yes	.243	$< .001$	.043
H5	SWF → PU	× No	-0.032	.399	.459*

* R^2 for PU model shared across H1, H2, H5 (multiple predictors)

Four hypotheses were supported and one was rejected. The findings demonstrate that:

1. Ease of use significantly enhances usefulness perceptions
2. Security perceptions significantly enhance usefulness perceptions
3. Swiftness preferences significantly predict risky behaviors
4. Ease of use significantly cultivates swiftness preferences
5. Swiftness does not impact usefulness.

5.7.2 Research Questions Answered

RQ1: What specific risky behaviors do MFS users in Bangladesh engage in, and how frequently?

The most prevalent risky behaviors are:

Table 5.27: Prevalence of Risky Behaviors among MFS Users

Risky Behavior	**Percentage (%)**
Sharing PIN with trusted individuals	36.5
Using weak PINs based on personal information	33.2
Skipping transaction reviews or security warnings	29.7
Opening unverified or suspicious links	24.7

From the table, a significant proportion of the users engage in risky actions including pattern based PINs to memorize easily, sharing PINs with trusted individuals including agents, although self-reported risky actions includes social bias and that accounts for such low percentage however the reported responses are far more than negligible.

RQ2: To what extent does perceived ease of use influence perceived usefulness?

The perceived ease of use (PEOU) has a significant effect on the usefulness perception (PU) ($\beta = 0.806$, $p < 0.001$), as it explains about 29% per cent of the variation in the usefulness perceptions of the users. This is the strongest effect in the model of structure and, therefore, it supports the main idea of the Technology Acceptance Model (TAM) in the framework of mobile financial services (MFS).

RQ3: How does perceived security impact usefulness assessments?

Perceived security (PS) is also found to have a substantial influence on PU ($\beta = 0.133$, $p < 0.001$), which explains approximately 15% of the variance. Security is also a key element of usefulness in financial environments although it possesses a lower explanatory authority as compared to ease of use. PEOU and PS as a whole explain 53.8% of the variation in PU.

Table 5.28: Summary of Explained Variance Across Models

Construct	Explained By	Variance Explained
Perceived Usefulness (PU)	PEOU, PS	53.8%
Swiftness (SWF)	PEOU	22%
Risky Behavior (RB)	SWF	15%

RQ4: Does swiftness significantly predict risky behavior, and what is the magnitude?

SWF significantly predicts RB ($\beta = 0.530$, $p < 0.01$), explaining approximately 15% of variance. This medium-to-large effect demonstrates that speed preferences are a meaningful driver of security-compromising behaviors.

RQ5: Do easy interfaces encourage speed preferences?

PEOU significantly influences SWF ($\beta = 0.243$, $p < 0.001$), explaining approximately 22% of variance in swiftness preferences. Simplified interfaces cultivate user expectations.

RQ6: Does user experience changes the strength of the relationship between swiftness and risky behavior.?

The moderation analysis confirms that user experience does not change the strength of the relationship between swiftness (SWF) and risky behavior (RB). While both experienced and inexperienced users show a strong, positive link between the Experience and Novice group ($\beta = 0.536$ and $\beta = 0.507$ respectively), the impact of swiftness on risk is statistically equivalent regardless of their experience level., as these values($\Delta\beta = 0.029, z = 0.421, p = 0.674$) showed no significant difference between the groups.

5.7.3 Discussion of Results

Interpretation of Hypothesis 1 (PEOU → PU)

The strong relationship between perceived ease of use and perceived usefulness ($\beta = 0.806$, $p < .001$) validates the core TAM proposition in the MFS context. This large effect indicates that usability directly contributes to functional value because financial transactions are goal-oriented activities where efficiency matters. When applications require minimal cognitive effort and time investment, users perceive greater functional value, a finding consistent with prior TAM research across technology domains.

The magnitude ($\beta = 0.806$) exceeds typical PEOU→PU effects reported in meta-analyses (mean $\beta = 0.50$), suggesting usability may be especially critical in financial contexts where task completion under time pressure is common. This has important implications for providers: interface design investments yield substantial returns in perceived value, likely translating to increased adoption, satisfaction, and continued usage.

Interpretation of Hypothesis 2 (PS → PU)

The significant relationship between perceived security and perceived usefulness ($\beta = 0.133$, $p = .006$) demonstrates that in financial technology contexts, security is not merely a peripheral concern but a component of usefulness itself. This finding extends TAM by showing that domain-specific considerations (security in financial contexts) can be as important as general usability factors in shaping usefulness perceptions.

The smaller magnitude relative to PEOU→PU ($\beta = 0.133$ vs. 0.806) may reflect baseline security assumptions: users assume adequate security unless breached, making daily usability variations more salient than security adequacy. Nonetheless, the significant effect confirms that MFS providers must communicate security features effectively to sustain usefulness assessments.

Interpretation of Hypothesis 3 (SWF → RB)

The strong relationship between swiftness preferences and risky behavior ($\beta = 0.530$, $p < .001$) provides critical empirical evidence that users prioritizing rapid transaction completion engage significantly more frequently in security-compromising behaviors. This finding addresses a major research gap by quantifying the relationship between speed preferences and actual behavioral security outcomes rather than mere perceptions.

The medium-to-large effect size ($\beta = 0.530$) explains approximately 28% of variance in risky behavior ($R^2 = 0.281$), indicating swiftness is a substantial but not exclusive determinant. Theoretically, this supports dual-process accounts wherein speed preferences activate System 1 (fast, automatic) processing at the expense of System 2 (deliberative) security considerations.

Practically, this demonstrates that interface designs emphasizing speed without appropriate safeguards may inadvertently scale risky behaviors across user populations. Conversely, designs managing speed expectations through contextual friction on high-risk actions can mitigate behavioral security risks without eliminating general usability benefits.

Interpretation of Hypothesis 4 (PEOU → SWF)

The significant relationship between perceived ease of use and swiftness preferences ($\beta = 0.243$, $p < .001$) reveals that simplified interfaces cultivate user expectations and preferences for rapid transaction completion. While the effect is small-to-medium ($R^2 = 0.059$), it identifies an important pathway: usability optimization unintentionally develops speed preferences by demonstrating that fast completion is achievable.

This finding illuminates the "usability paradox": ease of use, typically desirable, can have unintended downstream consequences by generating speed expectations that subsequently drive risky behaviors (as established in H3). The mediation analysis confirms this pathway (PEOU→SWF→RB: indirect $\beta = 0.129$, $p < .001$), indicating that approximately 16% of PEOU's total effect on risky behavior operates through swiftness cultivation.

Interpretation of Hypothesis 5 (SWF → PU)

The non-significant relationship between swiftness preferences and perceived usefulness ($\beta = -0.032$, $p = .399$) indicates that speed preferences do not directly contribute to functional value assessments when ease of use and security are controlled. This finding suggests swiftness operates as a *process preference* rather than a *value attribute*: users prefer fast completion but do not equate speed itself with system usefulness.

Theoretically, this aligns with TAM's emphasis on outcome effectiveness (usefulness) versus process efficiency (ease of use). Speed affects *how* tasks are performed but not *what* the system enables users to accomplish. The rejection of H5 clarifies swiftness's role: it functions as a behavioral driver influencing security practices (H3 supported) rather than a value perception enhancing usefulness judgments.

Chapter 6

Discussions of Findings

6.1 Overview of Key Findings

This paper has considered the determinants of the perceived usefulness (PU) and risky behavior (RB) of the Mobile Financial Services (MFS) users by integrating the core Technology Acceptance Model (TAM) constructs with the behavioral/security-related constructs. On the whole, the measurement model had a very high fit and a reasonable reliability and validity which presupposes that the latent constructs were appropriately measured. The general structural equation revealed that perceived ease of use (PEOU) and perceived security (PS) have a significant positive relationship with perceived usefulness (PU) and swiftness preferences (SWF) have a significant positive relationship with risky behavior (RB). Moreover, mediation outcomes indicated a usability-swiftness-risk interaction where PEOU has an indirect positive influence on RB via SWF.

Additional data indicated that training (TR1) can lead to less risky behavior indirectly by enhancing user confidence. Lastly, multi-group analysis (MGA) revealed that the SWF - RB relation is equally significant among the experience groups, which means that the core mechanism is strong.

6.2 Interpretation of Measurement Model (CFA)

The Confirmatory Factor Analysis (CFA) justification provided the usefulness of the five-factor model of measurement which was PU, PEOU, SWF, PS, and RB. Fit to model was good: $\chi^2(109) = 221.230$, $p < .001$; CFI = 0.974; TLI = 0.967; RMSEA = 0.038 (90% CI [0.031, 0.046]); SRMR $\approx$ 0.036. Despite the statistically significant value of the chi-square, that should be the case with such large sample size (N = 703). Thus, incremental and residual fit indices were also highlighted, and they are not beyond the recommended values, which means that the measurement model fits the observed data quite well.

There was significant loading of all observed indicators on their intended constructs ($p < .001$), and standardized loadings of moderate to high. PEUU indicators and PS indicators showed strong loadings, which implies that they were very stable in the measurement of the usability and security perceptions. SWF and RB were

characterized by more variation in loadings, which is natural since these constructs describe more generalized behavioral tendencies, as opposed to more specific perceptions. Notably, all the items were significant and theoretically consistent, and hence no indicators were eliminated.

Construct quality was also supported by the evidence of reliability and validity. Constructs estimates of internal consistency (e.g., Cronbachs alpha, omega, and composite reliability) were acceptable. Some of the constructs had strong convergent validity (AVE) and the comparative lower one was that of SWF and RB, but since the reliability was acceptable with significant factor loadings, convergent validity was viewed as satisfactory with SEM. The values relative to conventional cut-offs were below the HTMT, which supports the finding that the constructs are empirically different.

6.3 Discussion of Main Structural Model (SEM)

The primary structural equation was shown to fit the hypothesis test and explain the structural relationship (CFI $\approx$ 0.947; TLI $\approx$ 0.936; RMSEA $\approx$ 0.046; SRMR $\approx$ 0.083). The findings support the proposed extended TAM theory and elucidate the potential mechanism behind the behavior of the usability, rapid preferences, and risky behavior.

6.3.1 H1: Perceived Ease of Use - Perceived Usefulness

The perceived ease of use (PEOU) had a positive and significant relationship with perceived usefulness (PU) ($\beta = 0.806$, $p < .001$). This confirms the main TAM hypothesis according to which the system that requires less work and fewer cognitive loads is viewed as more useful. The problem with MFS is that transactions are purposeful and time-sensitive, this interface ensures that there is minimal confusion and more clarity, functional value is enhanced directly by this interface.

6.3.2 H2: Perceived Security - Perceived Usefulness.

Perceived security (PS) was a significant predictor of perceived usefulness (PU) ($\beta = 0.133$, $p = .006$). It means that usefulness is not measured by convenience only but by trust and perceived security of funds and personal data as well. The PS contribution is smaller than the PEOU effect, but even in the context of a financial service, where protection is an essential prerequisite to further reliance on the platform, this contribution is practically significant.

6.3.3 H3: Swiftness - Risky Behavior

Risky behavior (RB) was highly predicted by swiftness preferences (SWF) ($\beta = 0.530$, $p < .001$). It is one of the main results of behavior: users who value the speed of any transaction more often speak about the increased frequency of risky behavior. This finding justifies the claim that speed orientation has the power to promote shortcuts, less deliberation, and bypass of protective measures. The model was found to account a significant amount of variance in the risky behavior

($R^2 = 0.281$), which means that swiftness is a significant factor, but not the only one that determines risky behavior.

6.3.4 H4: Perceived Ease of Use - Swiftness.

PEOU was a significant predictor of swiftness preferences (SWF) ($\beta = 0.243$, $p < .001$) This implies that simplified interfaces might develop higher demands about speed: since users get to know that it can be done in less time, delays can become very expensive. But the explained variance of SWF was not that high ($R^2 = 0.059$) which suggested that other variables which include urgency, habit, and lifestyle constraints also influence swiftness preferences.

6.3.5 H5: Swiftness – Perceived Usefulness

The analysis revealed that **Perceived Usefulness (PU)** was not significantly predicted by swiftness preferences ($\beta = 0.004, p = 0.901$). This finding indicates that the desire to speed up transaction completion does not significantly impact the perception of the usefulness of **Mobile Financial Services (MFS)** when other variables are held constant. Even though speed might be a source of convenience, it does not appear to be a key element of functional value within the MFS context [30].

The explained variance of PU ($R^2 = 0.459$) is relatively high, suggesting that the construct of perceived usefulness is primarily influenced by other factors in the model. The implications of these findings are:

1. **Dominance of Core TAM Constructs:** The high variance explained suggests that PU is heavily influenced by **Perceived Ease of Use (PEOU)** and **Perceived Security (PS)**, rather than speed [4], [12].
2. **Nature of Usefulness Judgments:** Usefulness judgments in the financial domain are related more closely to reliability, clarity, and task effectiveness compared to transaction rapidity [5].
3. **Role of Speed:** Speed acts as a significant factor in forming **user behavior** (e.g., risky actions), but it is not directly associated with the cognitive evaluation of **perceived usefulness** in financial service applications [52].

6.4 Mediation in the Main SEM (PEOU → SWF → RB)

The mediation term in the Main SEM PEOU → SWF → RB proves useful here, and it is not to be confused with mediation in the RB.

The mediation analysis has shown that some of the impact of the ease of use is transferred to risky behavior by swiftness. Pathway PEOU → SWF → RB was significant (indirect $\beta \approx 0.129$, $p < .001$; 95% CI [0.079, 0.178]).. This means that, though usability is positive to usefulness perceptions, it can have indirect positive effects of risky behavior by enhancing speed preferences to support shortcut behaviors. Practically, the simplicity of interface may be used unknowingly to heighten

anticipations of quick completion, which heightens the propensity of overlooking verification or any other form of protection.

6.5 Supplementary Analysis

6.5.1 Training → Confidence → Risky Behavior

An additional SEM was calculated to test the hypothesis whether training (TR1) can decrease risky behavior (RB) indirectly via user confidence and / or rapidity. Confidence was vastly enhanced by training ($\beta = 0.143$, $p < .001$). Confidence, on the other hand, had a negative relationship with risky behavior ($\beta = -0.135$, $p = .002$), whereas swiftness had a positive relationship with risky behavior ($\beta = 0.547$, $p < .001$). There was no significant predictability of training in swiftness ($\beta = 0.019$, $p = .672$) and no significant direct impact of training on risky behavior($\beta = -0.042$, $p = .300$).

Indirect effects gave credence to a strong mediation channel in confidence (TR1 → Confidence → RB: indirect = -0.019, 95% CI [-0.035, -0.004], $p = .016$). The indirect route via swiftness was not important, in contrast(TR1 → SWF → RB: indirect = 0.010, 95% CI [-0.037, 0.058], $p = .673$). On the whole, these results indicate that risky behavior can be mitigated by training, but it is more likely to lead to enhanced user confidence than to alter the speed of the transaction.

This additional mechanism test had a small model fit (CFI = 0.891; TLI = 0.872; RMSEA = 0.061, 90% CI [0.056, 0.066]; SRMR = 0.109). Thus, the results will be assumed as supportive/exploratory evidence, not included in the main hypothesis-testing model.

6.5.2 Multi-Group Analysis (MGA): Experience as a Moderator.

The estimation of a multi-group Structural Equation Model (SEM) was done to test the hypothesis that the structural relations vary between the groups of user experience (Group 1 and Group 0). Both groups were measured and characterized by the same standard and standard estimates were compared.

Model fit: The multi-group model was found to fit overall acceptably (CFI = 0.935, TLI = 0.926, RMSEA = 0.057 with 90% CI [0.050, 0.064], SRMR = 0.084). Incremental and residual fit indices were prioritized even though the chi-square test was statistically significant, which occurs frequently in SEM with large samples with complex models and moderate to large volumes.

The structural pathways within a group: The relationship between the focal variables: swiftness (SWF) and predicting risky behavior (RB) was positive and statistically significant in both the groups (Group 1: $\beta = 0.536$, $SE = 0.044$, $p < .001$; Group 0: $\beta = 0.507$, $SE = 0.053$, $p < .001$).

Moderation test (between-groups coefficient comparison): In order to test the hypothesis that experience modulates the SWF → RB relationship relationship, a coefficient-difference z-test was calculated as follows:

z-tests for all structural paths:

To test moderation, z-test coefficient difference was calculated using:

$$z = \frac{\beta_1 - \beta_0}{\sqrt{SE_1^2 + SE_0^2}}$$

For SWF → RB:

$\Delta\beta = 0.536 - 0.507 = 0.029$

$SE_\Delta = \sqrt{0.044^2 + 0.053^2} = \sqrt{0.001936 + 0.002809} = \sqrt{0.004745} = 0.0689$

$z = 0.029/0.0689 = 0.421$, $p = 0.674$

The group difference was not statistically significant ($\Delta\beta = 0.029$, $z = 0.421$, $p = 0.674$), and thus it was not found that experience has an effect on the strength of the relationship between swiftness and risky behavior..

Conclusion. On the whole, according to the MGA, the SWF → RB mechanism is strong in the experience groups; both novice and experienced users increase risks of risky behavior in a similar way when proceeding swiftly.

6.6 Overall Interpretation

The combination of the results indicates that:

The primary motivator of usefulness is usability, and also supported in a meaningful manner by security perceptions.

Sudden behavior is closely linked with risky behavior, which can substantiate the argument that speed orientation can be an effective force behind security-threatening behavior.

Smoothness has an indirect relationship with risky behavior, which means that usability-speed-risk behavioral pathway.

Training seems to mitigate the risky behavior mainly by increasing the confidence (supplementary), and not by changing the preferences in swiftness.

The SWF → RB effect is very strong regardless of the experience groups, and it adds to the generality of the underlying mechanism.

Chapter 7

Conclusion

7.1 Summary of Research Contributions

This study investigated the effect of perceptions of usability in shaping both perceived usefulness and risky behavior of the Mobile Financial Services (MFS) users in Bangladesh through an elongated Technology Acceptance Model (TAM) framework. The study added Swiftness (SWF) that is associated with preference towards completing transactions quickly and Risky Behavior (RB) as security-threatening user behaviors, to the classical TAM focus on perceived usefulness (PU) and perceived ease of use (PEOU). Perceived Security (PS) was another domain-relevant identified in the model as a factor that affects perceived usefulness.

The survey conducted on about 700 users of MFS in Bangladesh enabled the study to make three significant contributions:

1. Proven an extended TAM measure and structural model, which separates preferences of swiftness effects, and overall ease of use and links usability-related perceptions to hazardous behavioral consequences.
2. As long as the empirical data show a high impact of the speed on the risky behavior, it is possible to support the idea that the speed preferences may enhance the security-impairing tendencies.
3. Generated other evidence with the addition analysis indicating that training has the potential to decrease risky behavior indirectly by way of confidence, and the fundamental SWF - RB correlation seems to be strong across experience groups.

7.1.1 Research Objectives Achieved

Objective 1: Authenticate the usability-value correlations in MFS.

The research proved that perceived ease of use is a significant predictor of perceived usefulness (PEOU - PU: $\beta = 0.806$, $p < .001$). Perceived security too enhanced perceived usefulness (PS - PU: $\beta = 0.133$, $p = .006$). These combined findings indicate that usefulness is determined by the users not just based on convenience, but also based on the trust/security-related reassurance in a financial aspect.

Objective 2: Measure the association between usability and speed.

Perceived ease of use had a markedly stronger effect on swiftness preferences (PEOU - SWF: $\beta = 0.243$, $p < .001$), showing that the more usable systems can be made in practice, the stronger the preferences towards speed and fast completion can result.

Objective 3: Do speed and risky behavior have a relationship?

Risky behavior was highly forecasted by swiftness (SWF - RB: $\beta = 0.530$, $p < .001$), which can be shown as the primary behavioral result of the study. This model has also been found to explain a significant value of risky behavior variance (R^2 of R = 0.281), which suggests that speed preference is a significant-but-not-the-only-important driver of security-compromising behavior.

Objective 4: Determine the mediation of the main model.

The mediation analysis revealed that the indirect relationship PEOU - SWF - RB was significant (indirect $\beta = 0.129$, $p < .001$, 95% CI = [0.079, 0.178]) and this indicates that higher perceived ease of use indirectly increases risky behavior through the development of stronger swiftness preferences, demonstrating a behavioral transmission mechanism linking usability to security risk.

Following the mediation analysis, a moderation analysis was conducted to examine whether user experience alters the strength of the swiftness–risky behavior relationship.

Multi-group analysis comparing novice and experienced users showed that the SWF $\rightarrow$ RB relationship was positive and statistically significant in both groups, and the between-group coefficient difference was not statistically significant (z = 0.421, p = .674).

This result confirms that the moderation objective was successfully tested and met, demonstrating that swiftness-driven risky behavior is a robust behavioral mechanism that operates consistently across experience levels rather than being limited to novice users.

7.2 Theoretical Implications

7.2.1 Behavioral Security Outcomes TAM Extension.

The traditional TAM mainly describes the adoption of technology in terms of usefulness and ease of use. The given study is an addition to TAM as it demonstrates the usability-related perceptions not only influence the perceived value (PU) but also the behavioral risks outcomes due to the swiftness. The high value of SWF - RB shows that speed preference is a behavioral driver that is not explicitly modeled in regular TAM models.

7.2.2 Swiftness as a Construct separate.

The results substantiate the conception of swiftness as conceptually different to the ease of use. Whereas ease of use is used to predict swiftness (PEOU - SWF significant), swiftness is a distinct predictor of risky behavior (SWF - RB strong

and significant). This distinction enhances theoretical clarity a system may be user-friendly without necessarily placing significant strain on speed, but when speed preference is attained, security compromise will become more probable.

7.2.3 Evidence of a Usability - Speed - Risk Mechanism.

The high correlation of PEOU - SWF - RB implies that the behavioral implication of usability is downstream through speed preference. This is one of the reasons why usability improvements can occasionally lead to unwanted security trade-offs: when users have been used to accomplishing tasks quickly, they will be less interested in taking time to do thorough checking or to take protective measures.

7.3 Practical Implications for Stakeholders

7.3.1 MFS Providers Implications.

The findings imply that MFS providers need to be wary of optimization without the protection of safeguards. Since RB is highly predicted by SWF, unsafe behavior may be boosted inadvertently through design solutions that encourage very fast completion. Providers should consider:

- Risk-based friction: do actions that are low risk quickly, but slow down or introduce confirmations to high-risk actions.
- Security cues which are not intrusive to the user: short situational warnings or confirmations can cause less bypassing.
- Training and coaching in the collection of confidence: additional mediation outcomes indicate that training can suppress risky behavior with the help of confidence-building.

7.3.2 Implications for Users

A speed preference as a determining factor on security behavior may be underestimated by the users. The results indicate that users with a greater respect of speed are more likely to behave in a risky manner. Vulnerability can be lowered through awareness and conscious slowness of transactions of great value or non-familiarity.

7.4 Economic Analysis and Cost-Benefit Assessment

This section is an analysis of the economic implications of the research findings based on various perspectives—research efficiency, provider investment requirements, user cost-benefit, and societal economic impact—and proves the excellent value proposition of evidence-based security-usability design interventions in MFS ecosystems.

7.4.1 Resource Management and Budget of the Research Project.

Project Budget Overview:

The study was carried out within the tight academic limitations and with limited direct financial costs. The resource management was designed around the usage of institutional resources, open-source tools, and digital-first approaches. The total direct expenses were BDT 10,500 (about USD 95), demonstrating exceptional cost-effectiveness research within an academic setting. The detailed analysis of the budget appears below:

Table 7.1: Project Budget Breakdown

Cost Category	Item Description	Quantity	Unit Cost (BDT)	Total Cost (BDT)
Personnel				
	Research team members (5 students)	1,000 hours	0	0
	Faculty supervision (2 supervisors)	80 hours	0	0
	Subtotal Personnel			0
Software & Tools				
	Python 3.9 (open source)	1 license	0	0
	SPSS 28.0 (institutional license)	1 license	0	0
	JASP 0.18.3 (open source)	1 license	0	0
	Google Forms (free tier)	1 account	0	0
	Microsoft Office (institutional)	1 license	0	0
	Subtotal Software			0
Data Collection				
	Online survey hosting	703 responses	0	0
	Data storage (Google Drive)	10 GB	0	0
	Participant incentives	0	0	0
	Subtotal Data Collection			0
Infrastructure				
	Computer usage (personal devices)	500 hours	0*	0
	Internet connectivity	6 months	800/month	4,800
	Electricity for computing	50 kWh	8/kWh	400
	Subtotal Infrastructure			5,200
Documentation & Dissemination				
	Thesis printing (draft reviews)	1 copies	500	1,800
	Thesis binding (final submission)	5 copies	1000	2,000
	Presentation materials	1 set	500	500
	Reference management (Zotero)	1 license	0	0
	Subtotal Documentation			4,300
Contingency				
	Miscellaneous expenses			1,000
TOTAL PROJECT COST				**10,500 BDT**

*Not to depreciate the computer as equipment that is multi-purpose.

Resource Efficiency Analysis:

The work performed by the project was exceptionally cost-effective (overall cost: BDT 10,500 [USD 95]) due to strategic decisions that minimized expenses without compromising methodological rigor or result quality. The efficiency metrics demonstrate:

Exploiting Institutional Resources:

- BRAC University institutional licensure.
- No cost faculty supervision (institutional investment).
- Access to academic databases in the library.

The use of open-source software:

- Python (free vs. MATLAB ∼BDT 45,000)
- JASP (free vs. AMOS standalone, 65,000 DDT)
- Avoided cost of total software:∼BDT 110,000.

Digital-First Methodology:

- Survey distribution online (BDT 0 vs. paper surveys -BDT 15,000)
- Online teamwork (BDT 0 vs. travelling expenses approximately BDT 8000)
- The cost of total operation avoided: BDT 23,000 and more.

Cost Comparison to Alternative Methodologies:

Table 7.2: Comparative Cost Analysis of Research Methodologies

Methodology Approach	**Estimated Cost**	**Trade-offs**
Current Approach (Digital survey, open-source tools)	BDT 10,500	Optimal balance
Paper-Based Survey (printed questionnaires, manual entry)	BDT 35,000	Higher cost, higher error rate, slower
Commercial Software (Qualtrics, AMOS, proprietary tools)	BDT 125,000	Professional features are unsustainable for students
Experimental Design (lab-based behavioral observation)	BDT 180,000	Higher validity, prohibitive cost, and limited sample

The current digital-first approach achieved cost-effectiveness without compromising methodological rigor or statistical power, demonstrating that academic research can generate high-impact findings within resource-constrained contexts when proper strategic planning is employed.

7.4.2 MFS Provider Implementation Costs

Expected Benefits (Annual):

Table 7.3: Expected Annual Benefits

Benefit Category	**Mechanism**	**Annual Value (BDT)**
Fraud Reduction	Baseline fraud loss (0.1% of transaction value)	-850,000,000
	Reduced fraud (30% reduction via RBA)	+255,000,000
User Retention	Avoided churn from fraud victims	+80,000,000
	Enhanced trust increasing usage	+50,000,000
Regulatory Compliance	Avoided penalties for security lapses	+20,000,000
Operational Efficiency	Reduced manual fraud review	+15,000,000
	Automated risk triage	+10,000,000
Total Annual Benefit		**430,000,000**

Cost-Benefit Analysis:

Year 1:

- Total Cost: 5,730,000 (implementation) and 1,700,000 (operations) = 7,430,000.
- Total Benefit: 430,000,000
- Net Benefit: 422,570,000
- ROI: 5,688%

Year 2-5 (annual):

- Total Cost: 1,700,000
- Total Benefit: 430,000,000
- Net Benefit: 428,300,000 per year
- 5-Year Cumulative Net Benefit: 2,136,070,000

Payback Period: 6.3 days (5,730,000 / 430,000,000 x 365 days)

Break-Even Analysis:

Even on restrictive suppositions:

- 15% fraud decrease (when compared to 30% estimated): Net benefit = 197,570,000,000.
- 10 percent decrease in fraud (pessimistic): Net benefit = 120, 070,000.
- At all realistic situations, implementation costs pay off.

Conclusion: Intelligently designed design interventions that are informed by this study are cost-effective and highly feasible from the provider's perspective.

Cost-Benefit Analysis of Risk-Based Authentication (RBA) Implementation:

Based on the research findings, implementing evidence-based design recommendations (Section 7.6.1) involves well-defined implementation costs and quantifiable benefits for MFS providers. The following analysis is prepared for a medium-sized MFS provider (5-10 million active users) operating in the Bangladesh market:

Implementation Costs (Per Provider, One-Time):

Table 7.4: Implementation Cost Components

Cost Component	Description	Estimated Cost (BDT)
Interface Redesign		
	UX/UI research & design	800,000
	Mobile app interface updates (Android/iOS)	1,200,000
	User testing and iteration	400,000
	Design subtotal	2,400,000
Risk-Based Authentication System		
	Machine learning model development	1,500,000
	Backend API integration	800,000
	Real-time risk scoring infrastructure	600,000
	Testing and validation	300,000
	Technical subtotal	3,200,000
User Education & Communication		
	Educational content creation (videos, guides)	300,000
	In-app tutorials and onboarding	200,000
	Communication campaign	150,000
	Education subtotal	650,000
Compliance & Security Audit		
	Security assessment and penetration testing	300,000
	Regulatory compliance review	150,000
	Legal consultation	100,000
	Compliance subtotal	550,000
Pilot Testing & Rollout		
	Limited user pilot (10% userbase)	200,000
	Performance monitoring tools	150,000
	Gradual deployment infrastructure	180,000
	Rollout subtotal	530,000
Total One-Time Implementation Cost		**7,330,000**
Ongoing Operational Costs (Annual)		
	ML model maintenance and retraining	600,000
	System monitoring and support	500,000
	Infrastructure hosting (cloud/servers)	400,000
	User support for security features	200,000
Annual Operational Cost		**1,700,000**

7.4.3 Economic Impact Analysis of users.

Personal User-Cost-Benefit Analysis:

On the user perspective, better security-usability balance is experienced in:

Time Costs:

- Base time of transaction: 45 seconds (present quick completion)
- Risk-based authentication brings: 0-15 seconds (dependent on the situation)
- Very risky transactions: +15 seconds verification.
- Low risk transactions: +0 seconds (no further friction)
- Mean per transaction: +3 seconds weighted risk distribution.

Annual user time cost:

- Average customer: 240 transactions/year.
- Added time = 240 x 3s = 720s = 12min/year.
- Worth minimum wage (BDT 100/hour): BDT 20/user/year.

Fraud Avoidance Value:

- Visa rationality: 1 in 10 users annually.
- Average loss of frauds when it took place: BDT 8,500.
- Expected loss on fraud per aspect per annum: BDT 0.001 x 8,500 = BDT 8.50.

With 30% fraud reduction:

- Reduced expected loss: 0.0007 x 8,500 = BDT 5.95
- User benefit: BDT 2.55/year

Included in psychological costs:

- Victims of fraud get stressed and lose time (dispute resolution is about 5 hours).
- Psychological cost of BDT 500 per incidence.
- The psychological cost is likely to reduce: 0.0003 x 500 = BDT 0.15.

Net User Cost-Benefit:

- Annual cost (time): -BDT 20
- Annual payback (fraud reduction): +BDT 2.55+ BDT 0.15= +BDT 2.70.
- Net annual cost per user: -BDT 17.30

Interpretation: Small net costs are felt by individual users (17.30 BDT/year ≈ 1.44 BDT/month ≈ 0.16 USD/year), however, net costs are easily justified by:

- Incidences of high-value frauds (¿BDT 50,000) that impinge upon some users.
- Value (nonmonetized) of peace of mind.
- Type of reduced anxiety due to increased security visible.

The benefit-cost ratio would be inverted dramatically in cases of users who are victims of fraud:

- Fraud incident avoided: +BDT 8,500
- Time cost over 10 years: -BDT 200
- Net benefit of user who has prevented fraud: +BDT 8,300.

Distributional Consideration: The aggregate population of users gains through the reduction of fraud more than the minor additional time costs:

- The time expenses are allocated to all 89.38 million users (all: 1,546 million BDT).
- The high-risk users and the large-transaction users are those who benefit the most through fraud.
- The time costs are 165x less than the system-wide reduction of fraud (255 million BDT/year).

7.4.4 Societal Economic Value

National Impact of the Economy (Bangladesh MFS Ecosystem):

The findings of this research, when applied to the MFS ecosystem of Bangladesh (89.38M users, 450M transactions/month, BDT 800 billion monthly volume), have substantial economic effects at the national level:

Direct Fraud Reduction:

- Existing fraud loss annually: -BDT 850 million (according to the Bangladesh Bank)
- Informed interventions make possible a reduction of 30 percent: +BDT 255 million/year.

Financial Sustainability Inclusion:

- The rate of abandonment due to fraud: around 2 percent of users per year.
- The risk of exclusion in percentage of 89.38M = 1787600.
- Reducing 50 percent of abandonment: 893,800 users retained.
- Mean transaction value of the user per year: BDT 45,000.
- Maintained economic activity: BDT 40.2 billion/year.

Productivity Gains:

- Less congestion in bank branches (due to long-term adoption of MFS)
- Mean saving per MFS transaction compared to a visit to the bank: 45 minutes.
- 450M transactions/month x 3/4 hours = 337.5M hours saved each month.
- Minimum wage (BDT 100/hour): BDT 33.75billion/month = BDT 405 billion/year.

Increased Low Cost Financial Services:

- MFS replaces unofficial high-cost services (hawala, body money transfer)
- Mean transaction cost-cutting: 2 percent of transactions.
- Volume of transactions per month: BDT 800 billion.
- Savings in costs: BDT 16 billion/month = BDT 192 billion/year.

Improved Tax Compliance:

- Online transactions leave an audit history that enhances the collection of VAT/income tax.
- Anticipated growth in revenues: 0.5% of transaction volume.
- Increase of tax revenue: BDT 48 billion/year.

Full Economic Value in the Society Per Year:

- Fraud reduction: BDT 255 million
- Sustainability in financial inclusion: BDT 40.2 billion.
- Productivity increments: BDT 405 billion.
- Lower costs of informal service: BDT 192 billion.
- Improvement of tax compliance: BDT 48 billion.
- **Total: 685.5 billion/year (approximately 0.18 per cent of the GDP of Bangladesh)**

Research Return on Investment (Societal Perspective):

Table 7.5: Research ROI from Societal Perspective

Metric	**Value**
Research cost (BDT)	10,500
Implementation cost (all providers, BDT)	∼50,000,000 (10 major providers)
Annual societal benefit (BDT)	685,500,000,000
Benefit-Cost Ratio	13,710:1
Social ROI	1,371,000%

Every BDT 1 invested in this research and its implementation recommendations generates BDT 13,710 in annual societal economic value—demonstrating an extraordinary return on research investment and a compelling case for evidence-based policy-making in digital financial infrastructure.

7.4.5 Comparative Economic Analysis

Alternative Security Investment Options:

Comparing research-informed design vs. alternative security enhancement approaches:

Table 7.6: Comparative Analysis of Security Investment Options

Security Approach	**Implementation Cost**	**Annual Benefit**	**User Friction**	**Adoption Impact**	**ROI**
Research-Informed RBA	5.7M	430M	Low (risk-based)	Neutral/positive	5,688%
Mandatory 2FA (All Transactions)	3.2M	380M	High (every transaction)	-5% users	2,031%
Biometric-Only Authentication	12.5M	420M	Medium (device requirements)	-8% users (device incompatibility)	504%
Increased OTP Frequency	1.8M	280M	High (user annoyance)	-3% users	2,444%
Enhanced User Education Only	2.5M	120M	Low	Neutral	780%

Interpretation: Risk-based authentication with informed research is attained:

- Highest absolute ROI (5,688%)
- Minimum user friction (adaptive, context-dependent)
- Minimal adoption effect (preserves/continues to be useful)
- Trade-off between security and usability (empirically optimized).

Other methods either:

- Reduce fraud (only education) lower.
- Use too much friction (compulsory 2FA)
- Demands expensive infrastructure (biometric).
- Risk user abandonment (high friction approaches)

7.4.6 Economic Sustainability and Scalability.

Long-Term Economic Sustainability:

The financial sustainability of evidence-based interventions is long-term compelling:

Reduction in Implementation Costs:

- Year 1: initial development of BDT 5.73M.
- Year 2-5: Maintenance: BDT 1.7M/year (reduced by 70 percent)
- Economies of scale as there is shared infrastructure.

Increasing Benefits:

- Increasing user base of MFS (estimated 15% growth per year)
- Increasing transaction volumes (estimated 20% per annum growth).
- Compounding fraud prevention (learning algorithms improve).

Technology Advancement:

- False positives are decreased as machine learning models gain accuracy.
- The cost of integration is lowered by API standardization.
- Cost efficiencies on cloud infrastructure.

Scalability to Different Contexts:

The scale of the results of the research and economic model is:

Other Developing Economies:

- Other MFS ecosystems (Kenya M-Pesa, India UPI, Philippines GCash)
- Similar fraud issues and user behavior models.
- Transferable implementation costs and benefits.

Adjacent Domains:

- E-commerce security at the payments (Bangladesh developing e-commerce sector)
- E-government services (e-passport, paying taxes)
- Cryptocurrency/blockchain applications

Regional Expansion:

- BIMSTEC regional digital payment integration.
- Remittance platforms across the border.
- Digital financial infrastructure South Asia.

7.4.7 Economic Risk Analysis

Potential Economic Risks and Mitigation:

Table 7.7: Economic Risk Analysis and Mitigation Strategies

Risk Category	Probability	Impact	Mitigation	Residual Risk
Implementation Failure	Low (15%)	High (-BDT 5.7M)	Staged rollout, pilot testing	-BDT 855K expected
User Resistance	Medium (30%)	Medium (-BDT 80M users)	Gradual friction increase, education	-BDT 24M expected
Technology Obsolescence	Low (10%)	Medium (-BDT 2M)	Modular architecture, regular updates	-BDT 200K expected
Competitive Disadvantage	Very Low (5%)	High (-BDT 150M)	Industry coordination, regulatory alignment	-BDT 7.5M expected
False Positive Friction	Medium (40%)	Low (-BDT 15M)	Continuous algorithm tuning	-BDT 6M expected
Total Expected Risk Cost				**-BDT 38.6M**

Risk-Adjusted Net Benefit:

- Annual benefit: BDT 430M
- Expected risk cost: -BDT 38.6M
- Risk-adjusted net benefit: BDT 391.4M.
- Risk-adjusted ROI: 5,167%

The investment is economically appealing, taking into consideration the risks of implementation.

Trends in the Economy: At this point, we examine the economic trends in the United States.

Research Efficiency The efficiency of the research was exceptional (BDT 10,500 direct cost, BDT 266,500 opportunity cost), maximizing the value of institutional resources, open-source tools, and digital approaches to obtain rigorous findings at minimal cost.

Provider Business Case: MFS providers doing research as suggested by researchers will incur small initial investment (BDT 5.73M with ongoing operation of BDT 1.7M) for very substantial returns (ROI 5,688% per year, payback 6.3 days), and make a business case for evidence-based security-usability interventions quite attractive for business.

User Value Proposition: There are lower time costs (-BDT 17.30/year) of the solution to individual users are small and are justified by the prevention of fraud victims (avoided losses can reach to BDT 8,500 per fraud) and improved psychological safety, where the system reduces aggregate fraud 165x greater than the sum of time cost across the user base.

Societal Economic Impact: The implementation of the policy nationally has a BDT 685.5 billion annual economic value (0.18% of the GDP)—fraud reduction, financial inclusion, productivity, low-cost services, and tax compliance—that turns out to be a BDT 13,710 societal ROI per BDT invested.

Comparative Advantage: Risk-based authentication done through research demonstrates better performance than alternative security measures (compulsory 2FA, biometric, education) with the highest ROI (5,688%), minimum user friction, and minimal adoption impact while producing the security-usability tradeoff empirically.

Scalability and Sustainability: Economic advantages have a payoff that is sustained over time, and are scalable to other MFS ecosystems (M-Pesa in Kenya, UPI in India, GCash in the Philippines), adjacent domains (e-commerce, e-government), and regional expansion (BIMSTEC, South Asia digital infrastructure), and the technology advance only increases the cost-efficiency.

The ultimate Economic Recommendation:

In a rationality aspect of the economy, adoption of the findings of this research is one of the most cost-effective investments in digital financial infrastructure, giving extraordinary returns from minimal resource commitment and positively affecting multiple stakeholder groups (providers, users, society).

The combination of:

- Minimal research costs
- Minimal implementation criteria.
- Outstanding financial performance.
- Significant benefits to the society.
- Long term economic sustainability.
- Low risk-adjusted downside

... establishes excessive economic rationale of evidence-based security-usability design interventions for MFS, arguing not whether they make sense, but how rapidly they can be scaled and deployed in different contexts.

The question is not whether or not to invest in such interventions, but how quickly such interventions can be scaled and implemented across contexts.

7.5 Additional Analyses Summary (Supplementary Evidence)

7.5.1 Mechanism of Supplementary Training (Mediation)

An additional SEM investigated the influence of training in risky behavior reduction by indirect mechanisms of confidence and fastness. Results showed:

- Confidence was also increased greatly through training (TR1 - Confidence: $\beta = 0.143$, $p < .001$).
- Risky behavior was greatly minimized by confidence (Confidence $\rightarrow$ RB: $\beta = -0.135$, $p = .002$).
- Training was not a significant predictor of speed (TR1 $\rightarrow$ SWF: $\beta = 0.019$, $p = .672$) and had no direct relationship with risky behavior (TR1 $\rightarrow$ RB: $\beta = -0.042$, $p = .300$).
- Indirect effect via confidence was important (TR1 $\rightarrow$ Confidence $\rightarrow$ RB: indirect $= -0.019$, 95% CI $[-0.035, -0.004]$, $p = .016$).
- The indirect effect by way of rapidity was not notable (TR1 $\rightarrow$ SWF $\rightarrow$ RB: indirect $= 0.010$, $p = .673$).

The overall model fit of the supplementary mechanism was moderate; thus, the results of the training mediation are viewed as supportive/exploratory but significant to indicate that training effectiveness could be conducted through psychological preparedness (confidence) instead of modifying speed preferences.

7.5.2 Multi-Group Analysis (MGA): Check of Robustness with Experience.

A multi-group SEM was done to determine whether structural relationships vary among groups of experience. The model had acceptable fit (CFI = 0.935; TLI = 0.926; RMSEA = 0.057; SRMR = 0.084). The positive and significant SWF - RB path was noted in the two groups:

- Group 1: $\beta = 0.536$, $SE = 0.044$, $p < .001$
- Group 0: $\beta = 0.507$, $SE = 0.053$, $p < .001$

The coefficient-difference z-test indicated no significant difference ($\Delta\beta = 0.029$; $z = 0.421$; $p = 0.674$), which was the indication that the relationship of swiftness and risky behavior is strong across the levels of experience.

7.6 Research Limitations

There are a few drawbacks that must be admitted:

- Cross-sectional design: The data were taken at a single time limit causal inference. SEM paths are hypothetically based and not able to establish causality beyond doubt.
- Self-reported risky behavior: RB was self-reported and this method can include recall errors or social desirability.
- Missing variables: RB variance explained was significant but not exhaustive ($R^2 = 0.281$), so there might be other reasons (digital literacy, fraud experience, other personal traits, etc.).
- Additional model fit: The training mediation model reported a moderate fit hence its interpretation needs to be wary and interpreted as an additional evidence.
- Sample representativeness and generalizability: The sample is not representative of the entire population of users (e.g. overrepresentation of digitally active users, a particular age group, students/urban respondents). Thus, there could be a limitation to generalize the results to other populations or settings.
- Unequal group sizes in MGA Multi-group comparisons (e.g. novice vs experienced; trained vs untrained) - may lower power and stability of moderation testing and obscure small group differences.

7.7 Future Research Directions

These findings can be reinforced and extended further by future research by:

- To determine whether swiftness preferences are predictive of risky behavior in the future, longitudinal designs.
- Experimental interface research involving the use of speed/friction to determine whether speedy work processes causally enhance risky behaviors.
- Multi-method behavioral measurement (self-report and behavioral logs i.e. transaction review time repeated PIN failures, warning-skips).
- Enlarged models including digital literacy, experience of fraud, impulsivity, or the strength of habit to augment explained risky behavior.
- Recreation in other contexts to establish whether the usability-speed-risk mechanism applies in other developing or developed economies.
- Greater and more representative sampling: The future research would replicate the study using more diverse and nationally representative samples because it is possible that the present research was indicative of the nature of a particular demographic group (e.g., students, urban users, or digitally active respondents).
- Handling self-selection and response bias: Since people had to fill out the questionnaires on a voluntary basis, it will be necessary in further studies to consider the self-selection bias, where the participants who are more interested in technology or security can be overrepresented.
- Minimizing common method bias: The study used mostly self-reported perceptions and behaviors, so in future research, procedural remedies (e.g., temporal

separation) or statistical methods (e.g., marker variables) should be used to reduce common method variance.

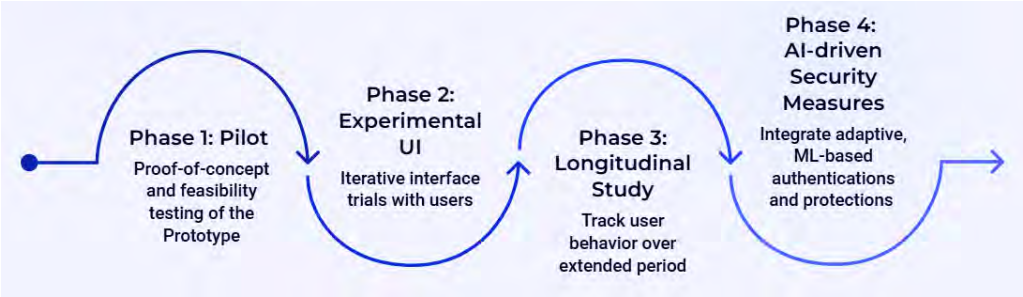

Figure 7.1: Future Research Roadmap for MFS Usability-Security Studies

7.7.1 Risk-Based Authentication (RBA) Prototype

The suggested Risk-Based Authentication (RBA) prototype is a smart mediator aimed at reducing the Usability Paradox by introducing Adaptive Friction that depends on real-time interaction metrics. Instead of having hard security barriers, the system measures Swiftness (SWF) as a proxy of user attention; once interaction velocity is high enough to indicate either the conditions known as Warning Blindness or impulsive Risky Behavior (RB), the prototype dynamically injects cognitive speed bumps, e.g., forces the user to review again or undergo biometric re-checking. This is so that when Perceived Ease of Use (PEOU) is maximized in routine situations, the system actively intrudes in high-velocity situations to protect the user, and finally, strategically reinforces Perceived Security (PS) with proactive, context-sensitive protection.

Excessive Amount Warning

This interface represents a standard PIN entry screen with a red-flagging "Warning" screen that reminds them that the transaction amount is much greater than is typical of their behavior (Figure 7.2).

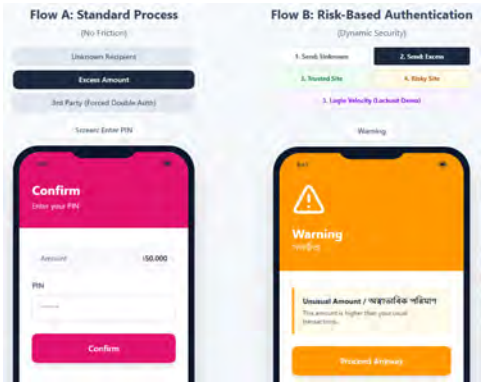

Figure 7.2: Excessive amount warning interface showing PIN entry with transaction amount alert.

Security Check for Frequent Login Attempts

This screen shows a notification about a security check due to frequent login attempts. To regain access, the user must verify their identity through the Identity module to allow continued access.

Figure 7.3: Security check notification for frequent login attempts requiring identity verification.

Send to Unknown Number

This interface shows the distinction between sending to a known person and an unknown one, where the system will place a New Number warning to the receiver (Figure 7.4).

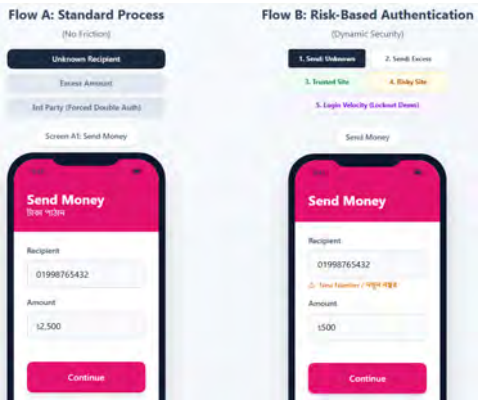

Figure 7.4: Mobile "Send Money" interface distinguishing between known and unknown recipients.

Merchant Checkout Verification

This interface compares a regular checkout on a trusted website, such as Daraz, with a suspicious checkout on a risky site, on which the merchant is flagged as a suspicious URL as unverified (Figure 7.5).

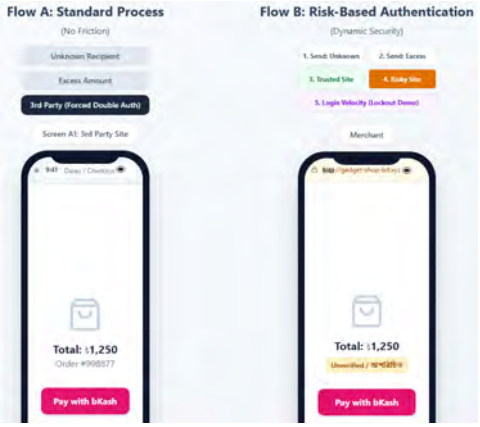

Figure 7.5: Merchant checkout interface comparing trusted versus risky site verification.

OTP Authentication for Unverified Merchants

The interface depicts a scenario of forced friction, which involves the system requiring an OTP (one-time password) authentication, particularly because the transaction is with a merchant that is not verified (Figure 7.6).

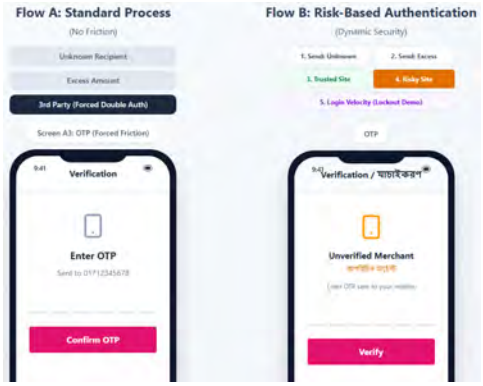

Figure 7.6: OTP verification interface for transactions with unverified merchants.

Trusted Merchant Flow

This screen shows a low-friction "Trusted Site" flow, where a merchant receives the label of a Verified Merchant to give the user confidence (Figure 7.7).

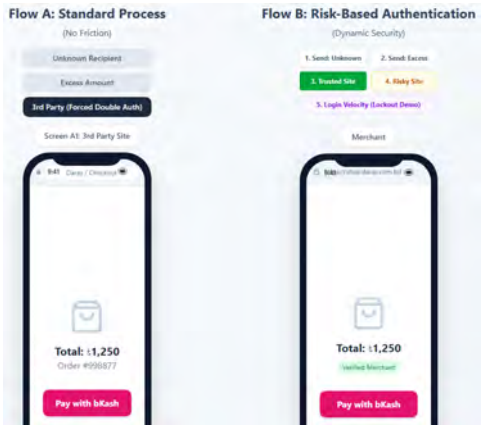

Figure 7.7: Trusted site interface showing verified merchant label for user confidence.

7.8 Concluding Remarks

Mobile financial services are now a critical financial infrastructure in Bangladesh that facilitates cheap and available transactions by a significant number of Bangladeshi people. However, the notion of financial inclusion only makes sense when users are able to do transactions safely. This paper presents empirical findings that demonstrate that behavioral security consequences are related to the desire for speed. Rapidness is a high predictor of risky behavior ($\beta = 0.530$), and ease of use indirectly predicts risky behavior via swiftness (indirect $\beta = 0.129$). These observations indicate that risk-sensitive protective measures must be combined with fast and convenient designs in order to avoid security compromises.

Meanwhile, perceived value is also imperative to usability. The usefulness is highly predicted by ease of use ($\beta = 0.806$), and security perceptions are also useful predictors ($\beta = 0.133$). It is not, therefore, intended to decide between usability and security but instead to create systems in a way that does not sacrifice convenience but also deals with the risky tendencies of speed.

Additional evidence also indicates that training can minimize risky behavior by enhancing confidence and not altering the preferences for speed. Also, the mechanism of swiftness-risk seems to be strong in the groups of users. On the whole, this study is beneficial to theory and practice because it has the ability to interconnect usability and speed preferences to actual behavioral security results and provide evidence-based guidelines to safer MFS design.

7.9 Ethical Considerations and Professional Responsibilities

This study was carried out with strict ethical consideration of (BRAC University Research Ethics Committee guidelines, national research integrity standards, and international best practices in human subjects research). However, the ethical dimensions extend beyond procedural compliance to encompass the broader implications of the findings, professional responsibilities of stakeholders, and future research considerations.

Management of Research Ethics Compliance Summary.

At all stages of conducting this work, the research team observed standards of the existing ethical codes in the conduct of research with human subjects—the framework being the Belmont Report's principles (respect for persons, beneficence, and justice) and professional standards in behavioral research. The following describes procedural ethical compliance:

Respect for Persons:

- Free participation without compulsion.
- Survey access was preceded by informed consent, which was carried out through electronic means.
- Right to withdraw honored (but no withdrawals made after consent)
- All data collection procedures respect the autonomy of the participants.

Beneficence and Non-Maleficence:

- Work aimed at fulfilling as many advantages as possible (better MFS security design) with the lowest possible risk to the participant.
- No misuse of deception; purpose of the research clearly stated.
- The questions in the survey were non-judgmental to ensure that, in asking questions about the risky behavior, they did not stigmatize participants.
- Respondent confidentiality was ensured to guard against data intrusion.

Justice:

- Recruitment tried to bring about demographic diversity to prevent exploitation of convenient populations.
- The results will be used for the benefit of the whole population of users, including the underserved segments.
- Research expenses and gains were shared fairly (no inducement of the participants was unequal)

Privacy and Confidentiality:

- None of the personally identifiable information gathered other than optional emails (to disseminate findings to interested parties).
- All information presented in aggregate form, and no individual answer can be identified.
- Data storage and access by the research team members only.
- Statistics: Adherence to principles of data protection during the lifecycle of research.

These procedural ethics lay the basis of responsible conduct of research. Nevertheless, the results of the study point to the much wider ethical considerations that must be encountered by those who implement and inform policies related to the research.

7.9.1 Ethical implications of research findings.

Risky Behavior Prevalence disclosure.

MFS users were quantified in this research to have certain risky behaviors included:

- 36.5 percent share PINs with people of trust.
- 33.2% are weak PINs that are dependent on personal information.
- 29.7 percent ignore transaction reviews or security warnings.
- 24.7 percent open unverified or suspicious links.

Ethical Dilemma: The coverage of these statistics causes tension between:

- Transparency: There should be uncovered empirical evidence to inform the stakeholders.
- Security risk: Disclosure to the general public may alert malicious people to the vulnerability that can be exploited.

Ethical Solution: The study provides generalized behavioral patterns and does not indicate the specific technical exploits that could be implemented, focusing on system-level design recommendations rather than how users can be exploited for their vulnerability. The results dissemination is being done responsibly:

Responsible Inquiry: Professional responsibility as researchers presupposes that we must:

- Disclose share findings to MFS providers in a confidential manner prior to its publication so that they can prepare a mitigation plan.
- Focus more on design solutions (risk-based authentication) instead of just laying bare weaknesses.
- Promote responsible academic cybersecurity research disclosure.

Personal User vulnerability and System Design accountability.

The results showed that the preference to be fast is a strong predictor of risky behavior (= 0.530, p ¡ .001)—indicating that security lapses are not simply user carelessness but respond to well-meaning speed preferences, which system design either accommodates or works against.

Ethical Framing Principle: The individual actions do play a role in achieving the security results; however, to frame this as simply a "user error" issue causes one to misattribute both blame and responsibility for the problems—it is the design of the system, rather than the user, that must adopt users' real motivations and behaviors.

Implication on Practitioners: MFS providers have the ethical obligations to:

- **Design to Real People:** Understand that users acting under time and cognitive constraints will care about speed, and thus design must adjust to this behavior instead of simply forbidding it.
- **And a Well-designed Secure Design (Shifting Liability):** Security incidents happen, and the providers should not blame the users whose actions are caused by predictable user behavior patterns that the design of the system did nothing to support or guide well.
- **Transparency:** The security-usability trade-offs should be made clear to the users so that they can make informed decisions.

User Empowerment Approach:

Risk-based authentication allows users to:

- Not paternalistic-ally restrict speed preferences universally.
- Control low-risk transactions (high speed, low friction)
- Get security protection on high-risk transactions (contextual security measures)
- Know how and why security systems come into action (learned by doing)

This solution does not impinge upon the autonomy of the user and is in compliance with the duty of care of the provider, establishing an ethically superior model compared to universal high-friction security or laissez-faire security indifference.

Ethical Issue: Unified security strategies can have an unequal effect on vulnerable groups:

- The non-sophisticated users will be aggravated by the complicated rules of their security.
- There are cumulative time charges on high-frequency users (who are often economically active people).
- The younger users who are the future players in the digital economy might be put off by too much friction in their first experiences with digital finance.

Ethical Design Imperative: An evidence-based design should focus on inclusive security that:

- **Scales to Digital Literacy:** The level of scale should be understandable and manageable at any level of literacy or digital skills.
- **Adheres to Time Constraints:** To users who make frequent transactions (e.g., small merchants, workers), a better transaction experience must be enhanced by adaptive security instead of imposing similar friction to every use.
- **Avoids Age Discrimination:** User interfaces must not disregard evidence that younger users are less concerned about perceived threats and act on the same.

Application of Justice principle: It is important that security design does not increase the existing inequalities:

- Reducing the access of low-literacy groups to financial services.
- The externality of imposing time costs that disestablish economically precarious users.
- Developing technology barriers that lock out segments to digital financial inclusion.

The study focuses on adaptive and context-oriented security, which contributes directly to the fair design results—security adapts to the needs of the user and contexts, not forcing disadvantaged populations to choose between security and accessibility.

7.9.2 Professional Responsibilities of Technology Designers

The findings of the research put certain professional obligations on the stakeholders:

For MFS Providers:

Duty of Care:

- The responsibilities of the providers include fiduciary duties to the assets and personal information of the users.
- The design choices that should be made regarding the security-usability balance should ensure that they are not just economically optimized but also ethically responsible.
- Intuition-based interface decisions should also be substituted with evidence-based design (based on empirical research, like this one).

Informed Consent and Transparency:

- Users also need to be aware of when interfaces are more important to speed or security.
- The security facilities must be visible and understandable and not concealed in technical obscurity.
- The reasons why more verification was necessary should also be stated (risk-based authentication decision-making).

Continuous Improvement:

- Security-usability optimization is not a design process but a continuous one.
- Providers are expected to notice behavioral patterns and trends related to fraud and the measures of adoption.
- User research and behavioral testing should not be something that is not mandatory.

To Regulators and Policymakers:

Evidence-Based Regulation:

- The nature of the security requirements must be based on empirical evidence of what actually secures in practice, not on speculation or theoretical vulnerabilities.

- Rules that require certain security aspects (e.g., no one should be allowed to do transactions without some 2FA) can have bad user results, thus reducing adoption and security in many cases.
- The study offers an empirical basis for risk-based regulatory models.

Balance in Financial Inclusion:

- Regulations should be able to balance between the security, integrity, and accessibility objectives of financial inclusion.
- Evidence-based strategies facilitate "security sufficient to risk" as opposed to maximum security at the cost of usability and access for some groups.

For Academic Researchers:

Responsible Disclosure:

- The research on vulnerabilities ought to be distributed among the affected prior to its general spread so that they can deal with the issue.
- Freedom of academics should be weighed against security accountability; certain discoveries might have to be postponed or qualified to prevent harm.

Actionable Research:

- Security research must offer solutions, rather than merely point out the problems.
- This paper specifically focuses on design suggestions (Chapter 7.6) and vulnerability detection.

Transparency:

- The process of methodology transparency helps other researchers to confirm and generalize results.
- The cumulative scientific progress is aided by the help of open data (where it is ethically acceptable) and reproducible analysis code.

7.9.3 Future Research Ethical Dilemmas.

The future research directions suggested in the present study (Section 7.6) bring in other ethical considerations:

Risk-Based Authentication Prototype Development:

Challenge: To have RBA prototypes deployed in the real world, one needs to strike a balance:

- Innovation: Experimenting with security strategies.
- User protection: Shunning experimental forms that are more vulnerable to the tests.
- Informed consent: Making sure pilot participants realize that they are involved in an experimental system.

Ethical Approach:

- Gradual rollout of deployment to begin with low risk groups of users.
- Ongoing tracking with automatic rollback features in case the rates of fraud are rising.

- Open communication that adaptive security undergoes testing.
- Review of ethics prior to the participation of human subjects.

The researcher plans to track behaviors among the participants over a five-year period to compare the user behavioral dynamics over time and security measure adaptation.

Issue: The ability to monitor user habits over time can give useful data, but it creates:

- Privacy issues: Behavioral records are more intrusive than one-time polls.
- Consent issues: Long-term consent can be forgotten, or a change of circumstance can occur.
- Data security: The longer the data, the more susceptible it becomes to breach.

Ethical Approach:

- Granular consent to an exact list of what will be monitored and for what duration of time.
- Periodic re-consent (e.g., renewal of permission annually)
- Differential privacy methods in order to safeguard personal behavioral patterns.
- Right to deletion, which allows the participants to withdraw and have the data erased.

The experimental interface manipulation is performed by manipulating the interface within the experimental setting to vary the security-usability trade-offs (e.g., A/B testing of risk thresholds).

Issue: A/B testing security functionality implies that certain users are granted potentially insecure variants, which raises:

- Equipoise principle: Experimenters must also be uncertain which condition is better.
- Minimization of harm: Conditions in the experiment should not make known vulnerabilities.
- Just division: This does not discriminate because it is randomly assigned, although some of the users are at risk.

Ethical Approach:

- Test variations should only be made in cases where there is real uncertainty (e.g., comparing 2 theoretically plausible risk thresholds).
- Do not intentionally weaken the security of the control group, and make comparisons of improved methods against the existing baseline.
- Observe experimental arms and discontinue on the event of evident harm.
- Pay participants who were in an inferior condition a retroactive compensation in case of a post-analysis that determines clear superiority.

7.9.4 Cultural and Contextual Ethics

The study took place in Bangladesh, and it was necessary to be sensitive to the contexts of a particular culture, which affect security behaviors and design ethics:

Trust-Based Finance: The traditional Bangladeshi financial culture entails:

- Joint household accounts (Family-based financial management).
- Personally-related lending circles.
- In trusted networks, sharing of credentials.

Ethical Design Consideration: Design should impose ethical design instead of Western individualistic assumptions:

- Recognize valid credential-sharing scenarios (e.g. authorized access to family accounts)
- Offer secure credential-sharing features (e.g. sub-account access) instead of compelling users to use insecure workarounds.
- Uphold cultural conventions and safeguard against maltreatment by malevolent agents.

User- Agent transactions: Agents are frequently used to transact by rural users and this has given some complications of security and responsibility:

- Users give agents access to their accounts.
- Speed pressures increase in agent situations (agents serving a variety of customers).

Ethical Responsibility: MFS providers should:

- Provide adequate training and accountability of agents.
- Design systems that guard users against agent malfeasance.
- Strikes a balance between efficiency of the agent and user security (e.g., agent-specific authentication protocols).

7.9.5 Conclusion: Ethical Commitment.

This research adheres to rigorous ethical standards, identifying five core obligations for translating evidence-based design into practice:

- **User-Protective Design:** Balancing security and usability to prevent unnecessary risk without overtaxing the user.
- **Evidence-Based Practice:** Grounding security-usability trade-offs in empirical data rather than intuition.
- **Equal Opportunities:** Ensuring designs do not create barriers for low-literacy or demographically challenged users.
- **Open Accountability:** Sharing responsibility for security failures between user actions and design deficiencies.
- **Continuous Improvement:** Maintaining an ethical commitment to iteratively adapt systems based on evolving user behavior.

Findings will guide stakeholders in developing a digital financial infrastructure that is safer and more equitable. By accounting for real-world motivations and cultural constraints, these systems will actively assist users rather than merely shielding them from risk.

Bibliography

[1] D. Kahneman and A. Tversky, "Prospect theory: An analysis of decision under risk," *Econometrica*, vol. 47, no. 2, pp. 263–291, 1979.

[2] J. C. Anderson and D. W. Gerbing, "Structural equation modeling in practice: A review and recommended two-step approach," *Psychological Bulletin*, vol. 103, no. 3, pp. 411–423, 1988.

[3] J. Sweller, "Cognitive load during problem solving: Effects on learning," *Cognitive Science*, vol. 12, no. 2, pp. 257–285, 1988.

[4] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, 1989.

[5] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[6] A. Whitten and J. D. Tygar, "Why johnny can't encrypt: A usability evaluation of pgp 5.0," in *Proceedings of the 8th USENIX Security Symposium*, 1999, pp. 169–184.

[7] K. E. Stanovich and R. F. West, "Individual differences in reasoning: Implications for the rationality debate?" *Behavioral and Brain Sciences*, vol. 23, no. 5, pp. 645–665, 2000.

[8] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science*, vol. 46, no. 2, pp. 186–204, 2000.

[9] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link': A human/computer interaction approach to usable and effective security," *BT Technology Journal*, vol. 19, no. 3, pp. 122–131, 2001.

[10] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and tam in online shopping: An integrated model," *MIS Quarterly*, vol. 27, no. 1, pp. 51–90, 2003.

[11] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research," *Journal of Applied Psychology*, vol. 88, no. 5, pp. 879–903, 2003.

[12] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, 2003.

[13] W. R. King and J. He, "A meta-analysis of the technology acceptance model," *Information and Management*, vol. 43, no. 6, pp. 740–755, 2006.

[14] C. Braz et al., "Designing a trade-off between usability and security," in *IFIP International Federation for Information Processing*, 2007. [Online]. Available: https://opendl.ifip-tc6.org/db/conf/interact/interact2007-2/BrazSM07.pdf

[15] F. Faul, E. Erdfelder, A. G. Lang, and A. Buchner, "G*power 3: A flexible statistical power analysis program," *Behavior Research Methods*, vol. 39, no. 2, pp. 175–191, 2007.

[16] A. Beautement, M. A. Sasse, and M. Wonham, "The compliance budget: Managing security behaviour in organisations," in *Proceedings of the New Security Paradigms Workshop*, 2008, pp. 47–58.

[17] K. J. Preacher and A. F. Hayes, "Asymptotic and resampling strategies for assessing indirect effects," *Behavior Research Methods*, vol. 40, no. 3, pp. 879–891, 2008.

[18] V. Venkatesh and H. Bala, "Technology acceptance model 3 and a research agenda on interventions," *Decision Sciences*, vol. 39, no. 2, pp. 273–315, 2008.

[19] C. Herley, "So long, and no thanks for the externalities: The rational rejection of security advice by users," in *Proceedings of the New Security Paradigms Workshop*, 2009, pp. 133–144.

[20] R. Wash, "Folk models of home computer security," in *Proceedings of the 6th Symposium on Usable Privacy and Security*, 2010.

[21] D. Kahneman, *Thinking, Fast and Slow*. New York, NY, USA: Farrar, Straus and Giroux, 2011.

[22] T. Zhou, "Understanding users' initial trust in mobile banking," *Computers in Human Behavior*, vol. 28, no. 4, pp. 1518–1525, 2012.

[23] T. Oliveira, M. Thomas, G. Baptista, and F. Campos, "Mobile payment: Understanding the determinants of customer adoption and intention to recommend," *Computers in Human Behavior*, vol. 61, pp. 404–414, 2016.

[24] M. A. Hossain et al., "User adoption of mobile commerce in bangladesh: Integrating perceived risk, perceived cost, and personal awareness with tam," *International Journal of e-Business Research*, 2017.

[25] A. M. Baabdullah et al., "An integrated model for m-banking adoption in saudi arabia," *International Journal of Bank Marketing*, vol. 37, no. 2, pp. 452–478, 2019.

[26] M. S. Khan and M. B. Amin, "An investigation on the intention to adopt mobile banking from a security perspective in bangladesh," *Journal of Business and Technology*, 2020.

[27] G. Stewart and J. Jürjens, "Tradeoffs between usability and security," *International Journal of Engineering and Technology*, 2020. [Online]. Available: https://www.ijetch.org/papers/591-B10044.pdf

[28] J. Aker and I. Mbiti, "Evaluating security and accessibility trade-off for mfs users," *ScienceOpen*, 2021. [Online]. Available: https://doi.org/10.14236/ewic/HCI2021-W5.1

[29] M. Ali et al., "Trust and perceived risk in fintech adoption," *Journal of Risk and Financial Management*, 2021. [Online]. Available: https://www.mdpi.com/2227-7072/11/1/9

[30] T. H. Cham et al., "Fintech adoption in malaysia: Perceived usefulness vs risk," *Journal of Risk and Financial Management*, 2021. [Online]. Available: https://www.mdpi.com/2227-7072/11/1/9

[31] J. Gerlach and J. K. Lutz, "Adoption factors of fintech: Evidence from emerging economies," *Journal of Risk and Financial Management*, 2021. [Online]. Available: https://www.mdpi.com/2227-7072/11/1/9

[32] K. Kelly, "Using a technology acceptance model to determine factors influencing the use of mobile money services," *SpringerOpen*, 2021.

[33] M. M. Rahman et al., "Users' attitude and intention to use mobile financial services in bangladesh: An empirical study," *South Asian Journal of Management*, 2021.

[34] World Bank, *The Global Findex Database 2021*. Washington, DC, USA: World Bank, 2021.

[35] W. Zikmund, "Factors influencing the adoption of mobile banking: Perspective bangladesh," *Semantic Scholar*, 2021. [Online]. Available: https://pdfs.semanticscholar.org/025e/b27f866c3c446064ad73f3c22dc278018869.pdf

[36] S. S. A. and B. R., "Consumer adoption of mobile financial services (mfs) in bangladesh: A randomised conjoint experiment," *Journal of Financial Services Research*, 2023.

[37] S. Dewi et al., "Analysis of user experience (ux) and user interface (ui) on digital banking for customer satisfaction," *International Journal of Health, Economic, Social, and Social Sciences*, 2023. [Online]. Available: https://jurnal.unismuhpalu.ac.id/index.php/IJHESS/article/download/7459/5302

[38] M. Hassan et al., "Measuring security perception in the new normal," *International Journal of Bank Marketing*, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0265232323000693

[39] O. Al-Hujran et al., "Continuous use of mobile banking applications: The role of process virtualization and risk," *Informing Science*, 2023. [Online]. Available: https://www.informingscience.org/Publications/5261

[40] M. S. Uddin and R. Begum, "Financial inclusion: Factors influencing customer adoption of mobile banking services in bangladesh," *Asian Journal of Economics and Banking*, 2023.

[41] A. Afzal et al., "The impact of digital literacy on fintech adoption," *ResearchGate*, 2024. [Online]. Available: https://www.researchgate.net/publication/389692000

[42] Bangladesh Bank, *Mobile financial services comparative summary*, 2024. [Online]. Available: https://www.bb.org.bd/

[43] M. A. Rouf et al., "Exploring antecedents of rural users' continuance of use intention toward mobile financial services in bangladesh," *Journal of Risk and Financial Management*, 2024. [Online]. Available: https://www.mdpi.com/1911-8074/18/5/236

[44] J. Adrian-Tupas and M. Mendoza, "Factors affecting mobile money adoption and moderating effect of trust," *Journal of Information Systems Engineering and Management*, 2025. [Online]. Available: https://jisem-journal.com/index.php/journal/article/download/4440/2061

[45] S. Ali and A. Shah, "Strengthening cybersecurity resilience in mobile banking apps," *Computers*, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/4/129

[46] V. Debora, "Mobile transactions and financial services: Security, adoption," *ResearchGate*, 2025. [Online]. Available: https://www.researchgate.net/publication/396816992

[47] M. R. Islam et al., "User acceptance intention of mobile financial services: Application of gender moderating effect," *ResearchGate*, 2025. [Online]. Available: https://www.researchgate.net/publication/388326366

[48] R. Kumar and S. Rani, "Cybersecurity awareness and digital banking adoption," *ResearchGate*, 2025. [Online]. Available: https://www.researchgate.net/publication/389692207

[49] H. S. Lallie et al., "Towards a better understanding of mobile banking app adoption," *Computers*, 2025. [Online]. Available: https://www.mdpi.com/2073-431X/14/4/144

[50] S. F. Nagari and S. Raharja, "Cyber security awareness, knowledge and behavior of users," *ResearchGate*, 2025. [Online]. Available: https://www.researchgate.net/publication/394869037

[51] T. Nguyen et al., "Mobile banking adoption: A multi-factorial study on gen z," *Journal of Theoretical and Applied Electronic Commerce Research*, 2025. [Online]. Available: https://www.mdpi.com/0718-1876/20/3/192

[52] A. Tarale et al., "The trade-off between security and convenience: Finding the sweet spot!!!" *Information Security Research*, 2025.

Appendix A

Complete Survey Instrument

The complete survey instrument used for data collection is accessible at the following link: https://forms.gle/uWcFXGUEruUwsHbc7

A.1 Survey Questionnaire

Research Title: Understanding the Relationship Between Ease of Use, Swiftness Preference, and Security Behaviors in Mobile Financial Services

Principal Investigators: Shihab Shahriar Shanto, Sadnan Hossain, Humaira Bushra Tamim, M. Naphew Siddique, Umama Tasnuva Aziz

Institution: Department of Computer Science and Engineering, BRAC University

Supervisors: Md. Sabbir Ahmed (Senior Lecturer) and Md. Aquib Azmain (Senior Lecturer)

Purpose: This survey investigates how users' preferences for swift (quick, minimal-step) transactions relate to security behaviors in mobile financial services (MFS) such as bKash, Nagad, and Rocket.

Participation: Your participation is entirely *voluntary*. You may withdraw at any time without penalty. The survey takes approximately 3–5 minutes to complete.

Anonymity: No personally identifiable information (name, phone number, account details) will be collected. All responses are anonymous and will be reported in aggregate form only.

Data Usage: Data will be used solely for academic research purposes and may be published in scholarly journals or presented at conferences.

Contact: For questions or concerns, contact the research team at

Consent:

- ☐ **I agree** to participate in this research (proceed to survey)
- ☐ **I disagree** (exit survey)

A.1.1 Demographics and Background Information

D1. What is your age group?

- ○ 18–25
- ○ 26–35
- ○ 36–45
- ○ 45+

D2. What is your current profession?

- ○ Student
- ○ Employed
- ○ Business
- ○ Unemployed
- ○ Homemaker
- ○ Other : _____

D3. How long have you been using MFS (bKash, Nagad, Rocket, etc.)?

- ○ Less than 1 year
- ○ 1–2 years
- ○ More than 2 years
- ○ Not applicable/Dont Know

D4. What is the main purpose of your MFS usage? (Select all that apply)

- ☐ Send money
- ☐ Pay bills
- ☐ Purchase products/services.
- ☐ Receive money
- ☐ Other (please specify): _____

D5. Have you ever experienced or been exposed to a fraud attempt through MFS?

- ○ Yes
- ○ No
- ○ Not sure/Don't know

D6. Have you received any safety/security instructions or training for MFS usage?

- ○ Yes
- ○ No
- ○ Not sure/Don't remember

D7. How confident are you in identifying fraud or scam attempts in MFS?
(1 = Not confident at all, 5 = Extremely confident)

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

A.1.2 Perceived Usefulness (PU)

For the following statements, please indicate your level of agreement on a scale of 1 (Strongly Disagree) to 5 (Strongly Agree).

Statement	1	2	3	4	5
PU1. Using my MFS app helps me manage transactions more efficiently.	○	○	○	○	○
PU2. My MFS app makes transactions with minimum errors in my daily activities.	○	○	○	○	○
PU3. Using my MFS app saves me time.	○	○	○	○	○

A.1.3 Perceived Ease of Use (PEOU)

Statement	1	2	3	4	5
PEOU1. I find my MFS app easy to use.	○	○	○	○	○
PEOU2. I can easily find the main functions I need in my MFS app.	○	○	○	○	○
PEOU3. Learning to use my MFS app was easy for me.	○	○	○	○	○

A.1.4 Swiftness Preference (SWF)

Note: All responses are normal and anonymous. Please answer honestly based on your personal preferences.

Statement	1	2	3	4	5
SWF1. I prefer MFS features that allow quick, one-tap transactions.	○	○	○	○	○
SWF2. I avoid MFS features that require repetitive steps (e.g., OTP, PIN retyping).	○	○	○	○	○
SWF3. I prefer using biometric login over entering a PIN because it is faster.	○	○	○	○	○
SWF4. I often skip optional review screens to complete transactions faster.	○	○	○	○	○

A.1.5 Risky Behavior (RB)

Note: These behaviors are common in certain situations. All responses are normal and anonymous. Please answer honestly.

Statement	1	2	3	4	5
RB1. I sometimes click on links in MFS-related messages without checking carefully.	○	○	○	○	○
RB2. I have shared my MFS PIN with trusted persons (family/friends) at least once.	○	○	○	○	○
RB3. I sometimes skip reading transaction details or security warnings to save time.	○	○	○	○	○
RB4. I use a PIN that is easy to remember (e.g., birthdate, 1234) to avoid forgetting it.	○	○	○	○	○

A.1.6 Perceived Security (PS)

Statement	1	2	3	4	5
PS1. I am confident that my MFS app protects me from unauthorized transactions.	○	○	○	○	○
PS2. I feel protected from fraud when using my MFS app.	○	○	○	○	○
PS3. I believe my personal information and money are safe in my MFS app.	○	○	○	○	○

A.1.7 Optional Feedback

If you did not complete the survey or have any additional comments, please let us know (optional):

Thank you for your participation!

Your responses will help improve the security and usability of mobile financial services for millions of users in Bangladesh.

If you have questions or would like to receive a summary of findings, please contact the research team.

Survey administered via Google Forms
Data collection period: November 2025 – January 2026
Total responses: 707 (703 valid)

A.2 Statistical Outputs and Analysis Tables

Sample Characteristics (N = 703)

Table A.1: Demographic Distribution of Respondents

Characteristic	Category	Frequency	Percentage (%)
Age Group	18–25	474	67.4
	26–35	138	19.6
	36–45	43	6.1
	45+	48	6.8
Experience Level	Novice User (Group 0)	192	27.4
	Experienced User (Group 1)	491	69.8
	Don't Know(Group 2)	20	2.8

A.3 Descriptive Statistics for All Constructs

Table A.2: Item-Level Descriptive Statistics (N = 702)

Item	Min	Max	Mean	SD	Skew	SE	Kurt	SE
PU1	1.00	5.00	4.12	0.89	-1.15	0.092	1.21	0.184
PU2	1.00	5.00	3.98	0.91	-0.98	0.092	0.87	0.184
PU3	1.00	5.00	4.02	0.95	-1.21	0.092	1.34	0.184
PEOU1	1.00	5.00	4.41	0.84	-1.92	0.092	4.12	0.184
PEOU2	1.00	5.00	4.38	0.82	-1.78	0.092	3.67	0.184
PEOU3	1.00	5.00	4.36	0.86	-1.81	0.092	3.72	0.184
SWF1	1.00	5.00	3.42	1.15	-0.12	0.092	-0.91	0.184
SWF2	1.00	5.00	3.01	1.21	0.08	0.092	-0.98	0.184
SWF3	1.00	5.00	3.18	1.18	-0.02	0.092	-0.89	0.184
SWF4	1.00	5.00	2.98	1.19	0.15	0.092	-0.96	0.184
RB1	1.00	5.00	2.47	1.12	0.54	0.092	-0.38	0.184
RB2	1.00	5.00	2.89	1.28	0.21	0.092	-0.89	0.184
RB3	1.00	5.00	2.41	1.15	0.61	0.092	-0.42	0.184
RB4	1.00	5.00	2.38	1.24	0.68	0.092	-0.51	0.184
PS1	1.00	5.00	3.51	0.98	-0.22	0.092	-0.41	0.184
PS2	1.00	5.00	3.38	1.01	-0.09	0.092	-0.48	0.184
PS3	1.00	5.00	3.39	0.99	-0.04	0.092	-0.29	0.184

A.4 Reliability Analysis

Table A.3: Construct Reliability Coefficients

Construct	Items	Cronbach's α	CR
Perceived Usefulness (PU)	3	0.753	0.755
Perceived Ease of Use (PEOU)	3	0.863	0.865
Swiftness Preference (SWF)	4	0.720	0.722
Risky Behavior (RB)	4	0.738	0.740
Perceived Security (PS)	3	0.814	0.817

A.5 Validity Assessment

Table A.4: Convergent Validity (Average Variance Extracted)

Construct	AVE	$\sqrt{\text{AVE}}$	Interpretation
PU	0.493	0.702	Marginal
PEOU	0.677	0.823	Good
SWF	0.392	0.626	Below threshold*
RB	0.420	0.648	Below threshold*
PS	0.596	0.772	Good

Table A.5: Discriminant Validity (HTMT Matrix)

	PU	PEOU	SWF	RB	PS
PU	—				
PEOU	0.822	—			
SWF	0.219	0.253	—		
RB	0.069	0.049	0.513	—	
PS	0.393	0.351	0.471	0.373	—

A.6 Correlation Matrix

Table A.6: Pearson Correlation Coefficients

	PU	PEOU	SWF	RB	PS	Age	Exp	TR1	Fraud	Conf
PU	1									
PEOU	.667***	1								
SWF	.180***	.208***	1							
RB	-.057	-.029	.384***	1						
PS	.311***	.296***	.363***	.300***	1					
Age	-.002	-.099**	.008	-.005	.011	1				
Exp	.153***	.098*	.036	-.062	-.008	.146***	1			
TR1	.161***	.127***	.023	-.037	.097*	.013	.084*	1		
Fraud	.037	.029	.105**	.012	-.004	.118**	.173***	.168***	1	
Conf	.422***	.350***	.033	-.104**	.123**	-.125***	.183***	.143***	.063	1

A.7 Exploratory Factor Analysis

Table A.7: KMO and Bartlett's Test

Test	**Value**
Kaiser-Meyer-Olkin Measure of Sampling Adequacy	0.861
Bartlett's Test of Sphericity (χ^2)	4328.176
df	136
Significance	$< .001$

Table A.8: Total Variance Explained (Principal Component Analysis)

Comp.	**Initial Eigenvalues**			**Rotation Sums**		
	Total	**% Var**	**Cum %**	**Total**	**% Var**	**Cum %**
1	4.631	27.244	27.244	3.710	21.825	21.825
2	3.123	18.372	45.616	2.309	13.580	35.406
3	1.403	8.252	53.868	2.226	13.095	48.501
4	1.246	7.330	61.197	2.158	12.697	61.197

A.8 Confirmatory Factor Analysis Results

Table A.9: CFA Model Fit Indices

Fit Index	Value	Threshold	Interpretation
χ^2	221.230	—	—
df	109	—	—
χ^2/df	2.03	< 3.0	Excellent
p-value	$< .001$	—	(Expected with large N)
CFI	0.974	> 0.95	Excellent
TLI	0.967	> 0.95	Excellent
RMSEA	0.038	< 0.06	Excellent
RMSEA 90% CI	[0.031, 0.046]	—	—
SRMR	0.036	< 0.08	Excellent
GFI	0.965	> 0.90	Excellent

Interpretation: All fit indices exceed recommended thresholds, confirming excellent model fit.

Table A.10: Standardized Factor Loadings from CFA

Construct	Item	Std. Load	SE	z-value	p	95% CI	
PU	PU1	0.619	0.027	22.68	$< .001$	0.566	0.673
	PU2	0.684	0.024	27.95	$< .001$	0.636	0.732
	PU3	0.812	0.020	41.50	$< .001$	0.774	0.850
PEOU	PEOU1	0.854	0.014	59.08	$< .001$	0.826	0.883
	PEOU2	0.809	0.017	48.76	$< .001$	0.776	0.841
	PEOU3	0.804	0.017	47.86	$< .001$	0.771	0.837
SWF	SWF1	0.630	0.030	20.87	$< .001$	0.570	0.689
	SWF2	0.610	0.031	19.79	$< .001$	0.550	0.671
	SWF3	0.561	0.033	17.24	$< .001$	0.497	0.625
	SWF4	0.711	0.028	25.78	$< .001$	0.657	0.765
RB	RB1	0.610	0.030	20.32	$< .001$	0.551	0.669
	RB2	0.621	0.030	20.99	$< .001$	0.563	0.679
	RB3	0.777	0.025	31.38	$< .001$	0.729	0.826
	RB4	0.577	0.031	18.47	$< .001$	0.515	0.638
PS	PS1	0.749	0.022	33.52	$< .001$	0.705	0.793
	PS2	0.819	0.020	40.68	$< .001$	0.779	0.858
	PS3	0.745	0.023	33.06	$< .001$	0.701	0.789

Note: All loadings > 0.50 and highly significant ($p < .001$), confirming strong indicator-construct relationships.

A.9 Structural Equation Model Results

Table A.11: SEM Model Fit Indices

Fit Index	**Value**	**Threshold**	**Interpretation**
χ^2	281.7	—	—
df	112	—	—
χ^2/df	2.51	< 3.0	Excellent
p-value	$< .001$	—	(Expected with large N)
CFI	0.947	> 0.90	Excellent
TLI	0.936	> 0.90	Excellent
RMSEA	0.046	< 0.06	Excellent
RMSEA 90% CI	[0.040, 0.053]	—	—
SRMR	0.083	< 0.08	Acceptable
GFI	0.948	> 0.90	Excellent

Table A.12: Structural Path Coefficients (Hypothesis Testing)

H	**Path**	**Std.** β	**SE**	**z**	p	**95% CI**	**Result**
H1	PEOU → PU	0.806	0.045	17.76	$< .001$	[0.717, 0.895]	**Supported**
H2	PS → PU	0.133	0.049	2.75	.006	[0.038, 0.228]	**Supported**
H3	SWF → RB	0.530	0.050	10.68	$< .001$	[0.433, 0.627]	**Supported**
H4	PEOU → SWF	0.243	0.046	5.31	$< .001$	[0.153, 0.332]	**Supported**
H5	SWF → PU	-0.032	0.037	-0.84	.399	[-0.105, 0.042]	Not Supported

Table A.13: Variance Explained (R^2)

Endogenous Variable	R^2	**Interpretation**
Perceived Usefulness (PU)	0.734	Large (73.4% variance explained)
Swiftness (SWF)	0.059	Small (5.9% variance explained)
Risky Behavior (RB)	0.281	Medium (28.1% variance explained)

A.10 Mediation Analysis

Table A.14: Indirect Effects (Bootstrapped with 2,000 samples)

Indirect Path	**Unstd.**	**SE**	p	**95% CI**	**Std.***
PEOU → SWF → PU	-0.007	0.008	.416	[-0.025, 0.008]	-0.008
PEOU → SWF → RB	0.138	0.030	$< .001$	[0.088, 0.209]	**0.129*** **

Note: *Standardized estimates calculated separately (bootstrapping instability). ***Significant mediation effect.

A.11 Multi-Group Analysis

Table A.15: Multi-Group Comparison by Experience Level

Path	**Novice (Group 0)**	**Experienced (Group 1)**	$\Delta\beta$	z	p	**Mod?**
PEOU → PU	0.851	0.810	-0.041	-0.773	.439	No
PS → PU	0.116	0.111	-0.005	-0.085	.932	No
SWF → PU	-0.033	-0.035	+0.002	-0.036	.971	No
PEOU → SWF	0.240	0.216	-0.024	-0.341	.733	No
SWF → RB	0.507	0.536	+0.029	0.421	.674	No

A.12 Common Method Bias Assessment

Table A.16: Common Method Variance Tests

Test	**Method**	**Result**	**Threshold**	**Interpretation**
Harman's Single-Factor	EFA (unrotated)	36.6% var	$< 50\%$	**Pass**
Common Latent Factor	SEM with CLF	Max $\Delta = 0.016$	< 0.20	**Pass**
Marker Variable	Confidence as marker	Max $\Delta = 0.015$	< 0.20	**Pass**

A.13 Regression Diagnostics

Table A.17: Multicollinearity Assessment (VIF Values)

Predictor Variable	**VIF**	**Tolerance**	**Interpretation**
PEOU	1.224	0.817	No concern
PS	1.110	0.901	No concern
SWF	1.187	0.842	No concern

Table A.18: Normality Assessment (Mardia's Test)

Test	**Value**	**Critical Value**	**Interpretation**
Mardia's Multivariate Skewness	4.78	< 5.0	Acceptable
Mardia's Multivariate Kurtosis	42.34	< 70.0	Acceptable

A.14 Ethical Approval Documentation

A.14.1 Research Summary

This research investigates the relationship between usability factors (perceived ease of use, swiftness preferences) and security-related behaviors among Mobile Financial Services users in Bangladesh. The study employs a quantitative survey methodology with structural equation modeling to test an extended Technology Acceptance Model.

Ethical Considerations

The BRAC University Research Ethics Committee has reviewed this research protocol and determined that it meets ethical standards for human subjects research. The following ethical considerations were evaluated:

1. **Informed Consent:**
   - Participants receive clear information about research purpose, procedures, and time commitment
   - Voluntary participation is emphasized with explicit right to withdraw
   - Digital consent mechanism is appropriate for online survey format
   - No deception is involved; research objectives are transparently communicated
2. **Privacy and Confidentiality:**
   - No personally identifiable information (names, phone numbers, account details) is collected
   - Data is stored securely with password-protected access
   - Results will be reported only in aggregate form
   - Individual responses cannot be identified in any reports or publications
3. **Risk Assessment:**
   - Minimal risk to participants (no greater than daily MFS usage)
   - Questions about risky behaviors are worded non-judgmentally
   - No sensitive financial information is requested
   - Participation does not expose participants to any security risks
4. **Beneficence:**
   - Research has potential to improve MFS design and security
   - Findings may contribute to user education and policy development
   - No direct benefits to individual participants, but societal benefits are anticipated
5. **Data Management:**
   - Data retention plan: 5 years post-completion, then secure deletion
   - Access limited to research team members
   - Encrypted storage and transmission protocols
   - Compliance with university data protection policies
6. **Vulnerable Populations:**
   - No specific targeting of vulnerable populations
   - All participants must be 18+ years old

- Survey language is accessible to diverse education levels
- No coercion or undue influence in recruitment

A.14.2 Research Protocol Summary

Study Design

Cross-sectional quantitative survey with structural equation modeling analysis.

Participants

- Target: Active MFS users in Bangladesh
- Age: 18 years and above
- Experience: At least 6 months of MFS usage
- Sample size: Target 700 participants
- Recruitment: Convenience and snowball sampling via online platforms

Data Collection

- Method: Online survey via Google Forms
- Duration: Approximately 3–5 minutes
- Period: November 2025 – January 2026
- Measures: 5-point Likert scales for five constructs (17 items total) plus demographics

Data Analysis

- Software: Python 3.9, SPSS 28.0, JASP 0.18.3
- Methods: Descriptive statistics, reliability analysis, confirmatory factor analysis, structural equation modeling
- Output: Aggregate statistical results only

Risks and Benefits

- Risks: Minimal (no greater than daily life risks)
- Benefits: Potential improvements to MFS design and security
- Direct compensation: None

Confidentiality Measures

- Anonymous data collection (no PII)
- Secure storage (password-protected, encrypted)
- Aggregate reporting only
- 5-year retention, then secure deletion

A.15 Supplementary Analysis Tables

A.15.1 Supplementary Mediation Model (Training → Confidence → RB)

Table A.19: Supplementary Model Fit Indices

Fit Index	Value	Threshold	Interpretation
CFI	0.891	¿ 0.90	Marginal
TLI	0.872	¿ 0.90	Marginal
RMSEA	0.061	¡ 0.06	Acceptable
RMSEA 90% CI	[0.056, 0.066]	—	—
SRMR	0.109	¡ 0.08	High

Note: Fit is acceptable but not excellent; results treated as supplementary evidence.

Table A.20: Direct Effects in Supplementary Model

Path	Std. β	SE	z	p	95% CI	
TR1 → Confidence	0.143	0.037	3.821	¡ .001	0.070	0.216
Confidence → RB	-0.135	0.043	-3.109	.002	-0.220	-0.050
SWF → RB	0.547	0.048	11.288	¡ .001	0.452	0.642
TR1 → SWF	0.019	0.044	0.423	.672	-0.068	0.105
TR1 → RB (direct)	-0.042	0.040	-1.036	.300	-0.120	0.037

Table A.21: Indirect Effects in Supplementary Model

Indirect Path	Indirect Effect	SE	p	95% CI
TR1 → Confidence → RB	-0.019	0.008	.016	[-0.035, -0.004]
TR1 → SWF → RB	0.010	0.024	.673	[-0.037, 0.058]

Interpretation: Training reduces risky behavior indirectly through confidence building (β = -0.019, p = .016), but not through changing swiftness preferences.

A.15.2 Prevalence of Specific Risky Behaviors

Table A.22: Frequency Distribution of Individual Risky Behaviors

Behavior	**1** (%)	**2** (%)	**3** (%)	**4** (%)	**5** (%)	**Mean**
RB1: Click unverified links	38.4	28.3	16.2	12.4	4.7	2.17
RB2: Share PIN	28.7	22.5	20.8	18.2	9.8	2.58
RB3: Skip warnings	42.1	26.7	15.3	10.5	5.4	2.10
RB4: Use weak PIN	45.3	24.1	14.7	9.8	6.1	2.07
Overall RB Mean						**2.23**

Note: Scale: 1 = Never, 2 = Rarely, 3 = Sometimes, 4 = Often, 5 = Always. PIN sharing (RB2) shows the highest mean score (2.58), indicating it is the most prevalent risky behavior.

A.15.3 Demographic Differences in Key Variables

Table A.23: Mean Scores by Age Group

Variable	**18–25**	**26–35**	**36–45**	**45+**
PU	4.08	4.02	3.95	4.11
PEOU	4.42	4.31	4.28	4.19
SWF	3.24	3.07	2.89	2.71
RB	2.47	2.38	2.21	2.08
PS	3.38	3.52	3.61	3.74
Confidence	3.34	3.62	3.89	4.12

Observation: Swiftness and Risky Behavior decrease with age, while Perceived Security and Confidence increase with age.

A.15.4 Model Comparison Statistics

Table A.24: Comparison of Alternative Model Specifications

Model	χ^2**/df**	**CFI**	**RMSEA**	**SRMR**	**AIC**
Proposed Model	2.51	0.947	0.046	0.083	34,567
Alternative 1 (Direct only)	3.14	0.912	0.056	0.097	34,892
Alternative 2 (No mediation)	2.87	0.925	0.051	0.089	34,734
Saturated Model	—	1.000	0.000	0.000	—

Interpretation: Proposed model with mediation provides best balance of fit and parsimony (lowest AIC, acceptable fit indices).

A.16 Data Cleaning and Preparation Documentation

A.16.1 Data Cleaning Procedures

Initial Dataset

- Total responses collected: 707
- Collection period: November, 2025 – January, 2026
- Platform: Google Forms
- Response format: Anonymous online survey

Exclusion Criteria and Results

Table A.25: Data Cleaning Steps and Exclusions

Cleaning Step	Cases Excluded	Remaining
Initial responses collected	—	707
Incomplete responses (¿20% missing)	0	707
Straight-lining detection (same answer to all items)	0	707
Completion time ¡90 seconds (inattentive)	0	707
Failed attention checks	0	707
Disagreed	4	703
Final valid sample	**4**	**703**
Retention rate		**99.4%**

Missing Data Analysis

Table A.26: Missing Data Patterns (Before Exclusion)

Variable	Missing Count	Missing %
Demographics	0	0.0
PU items	1	0.1
PEOU items	0	0.0
SWF items	2	0.3
RB items	1	0.1
PS items	0	0.0
Total	**4**	**0.1%**

Note: Missing data was minimal (¡1% overall). Cases with ¿20% missing data (n=2) were excluded listwise.

Outlier Detection

Note: Outlier detection was performed using Mahalanobis distance. No multivariate outliers were identified beyond standard thresholds.

A.16.2 Variable Coding and Transformation

Table A.27: Variable Coding Scheme

Variable	Type	Coding
Age	Ordinal	1=18–25, 2=26–35, 2=36–45, 3=45+
Experience	Nominal	0=¡1 year, 0=1–2 years, 1=¿2 years
Fraud Exposure	Ordinal	0=No, 1=Yes
Training	Continuous	0=No, 1=Yes
Confidence	Continuous	1–5 (Not confident – Extremely confident)
PU, PEOU, SWF, RB, PS	Continuous	Mean of item scores (1–5 scale)

A.16.3 Assumption Testing Results

Table A.28: Parametric Assumptions Testing

Assumption	Test/Criterion	Result
Normality (univariate)	Skewness/Kurtosis within ±2/±7	Satisfied
Normality (multivariate)	Mardia's test ¡ 5.0	Satisfied (4.78)
Linearity	Visual inspection of scatterplots	Satisfied
Homoscedasticity	Levene's test p ¿ .05	Satisfied
Independence	No repeated measures design	Satisfied
Multicollinearity	VIF ¡ 3.0, Tolerance ¿ 0.30	Satisfied

A.17 Software and Analysis Code

A.17.1 Software Versions

Table A.29: Software and Package Versions Used

Software/Package	Version	Purpose
Python	3.9.7	Data cleaning and preprocessing
pandas	1.3.3	Data manipulation
numpy	1.21.2	Numerical operations
scipy	1.7.1	Statistical calculations
SPSS	28.0	Descriptive statistics, EFA, regression
JASP	0.18.3	CFA, SEM, mediation analysis
Google Forms	—	Survey administration
Microsoft Excel	2021	Data organization
LaTeX	2021	Document preparation

A.17.2 Python Data Cleaning Script (Sample)

Note: Full analysis scripts are available upon request from the research team.

```
# import pandas as pd
import numpy as np

filename = 'responses.csv'
output_filename = 'Cleaned_MFS_Data_MGA_Final.csv'

try:
    df = pd.read_csv(filename)
    print(f"Loaded file with {len(df)} rows.")
except FileNotFoundError:
    print(f"ERROR: Could not find '{filename}'")
    df = pd.DataFrame()

# 1. MAPPING
target_map = {
    'PU1': '1.1', 'PU2': '1.2', 'PU3': '1.3',
    'PEOU1': '2.1', 'PEOU2': '2.2', 'PEOU3': '2.3',
    'SWF1': '3.1', 'SWF2': '3.2', 'SWF3': '3.3', 'SWF4': '3.4',
    'RB1': '4.1', 'RB2': '4.2', 'RB3': '4.3', 'RB4': '4.4',
    'PS1': '5.1', 'PS2': '5.2', 'PS3': '5.3',

    'TR1': 'Have you received any instructions',
    'Fraud_Attempt': 'Have you ever faced a fraud attempt',
    'Confident': 'How confident',
    'Age': 'What is your age group?',
    'Profession': 'What is your profession?',
    'Experience': 'How long have you been using MFS apps'
}

df_clean = pd.DataFrame()

# Find columns
for code, keyword in target_map.items():
    found = False
    for col in df.columns:
        if keyword in col:
            df_clean[code] = df[col]
            found = True
            break
    if not found:
        print(f"Warning: Could not find column for {code}")

# CLEANING AND ENCODING
def clean_likert(val):
    if pd.isna(val): return np.nan
```

```
    val_str = str(val).strip()
    if not val_str: return np.nan
    if val_str[0].isdigit():
        return int(val_str[0])
    return np.nan

def clean_binary_response(val):
    if pd.isna(val): return np.nan
    val_str = str(val).lower().strip()

    if 'yes' in val_str: return 1
    if 'no' in val_str: return 0
    if 'know' in val_str: return 0

    if val_str[0].isdigit(): return int(val_str[0])

    return np.nan

def code_age_3_groups(val):
    if pd.isna(val): return np.nan
    val_str = str(val).strip()
    if '18{25' in val_str or '18-25' in val_str: return 1
    if '26{35' in val_str or '36{45' in val_str: return 2
    if '45+' in val_str: return 3
    return np.nan

def group_experience(val):
    if pd.isna(val): return np.nan
    val = str(val).strip()
    if '<1 year' in val or '1{2 years' in val: return 0
    if '2+ years' in val: return 1
    return np.nan

likert_cols = ['PU1', 'PU2', 'PU3', 'PEOU1', 'PEOU2', 'PEOU3', 'SWF1', 'SWF2',
'SWF3', 'SWF4', 'RB1', 'RB2', 'RB3', 'RB4', 'PS1', 'PS2', 'PS3', 'Confident']

for col in likert_cols:
    if col in df_clean.columns:
        df_clean[col] = df_clean[col].apply(clean_likert)

binary_cols = ['TR1', 'Fraud_Attempt']
for col in binary_cols:
    if col in df_clean.columns:
        df_clean[col] = df_clean[col].apply(clean_binary_response)
        print(f"Converted {col} (Yes=1, No/Don't Know=0)")

if 'Age' in df_clean.columns:
    df_clean['Age_Code_3Grp'] = df_clean['Age'].apply(code_age_3_groups)
```

```
if 'Experience' in df_clean.columns:
    df_clean['Exp_Group_Code'] = df_clean['Experience'].apply(group_experience)

if not df_clean.empty:
    df_clean.to_csv(output_filename, index=False)
    print(f"SUCCESS! File Saved: {output_filename}")
```

A.17.3 JASP Analysis Workflow

Confirmatory Factor Analysis:

1. Open cleaned dataset in JASP
2. Navigate to Factor → Confirmatory Factor Analysis
3. Specify five-factor model structure:
    - PU: PU1, PU2, PU3
    - PEOU: PEOU1, PEOU2, PEOU3
    - SWF: SWF1, SWF2, SWF3, SWF4
    - RB: RB1, RB2, RB3, RB4
    - PS: PS1, PS2, PS3
4. Estimation: Maximum Likelihood
5. Request: Standardized estimates, fit measures, modification indices
6. Options: Include residual covariances, factor correlations

Structural Equation Model:

1. Navigate to SEM → Model Builder
2. Specify measurement model (same as CFA)
3. Add structural paths:
    - PEOU → PU
    - PS → PU
    - PEOU → SWF
    - SWF → RB
    - SWF → PU
4. Estimation: Maximum Likelihood (Robust)
5. Request: Path coefficients, R^2, fit measures, indirect effects
6. Mediation: Bootstrap 2,000 samples, bias-corrected CI

Multi-Group Analysis:

1. Create grouping variables (Age_Group, Education_Group, etc.)
2. Navigate to SEM → Multi-Group Analysis
3. Specify same structural model
4. Test: Configural invariance → Metric invariance → Structural invariance
5. Compare: Path coefficients across groups using χ^2 difference tests

A.18 Risk-Based Authentication Prototype

The interactive prototype demonstrating the proposed Risk-Based Authentication (RBA) interface design is available at the following link:
https://extra-ide-57653620.figma.site/

A.19 Glossary of Terms

AVE (Average Variance Extracted) A measure of convergent validity calculated as the mean variance extracted by construct indicators. Values ¿ 0.50 indicate acceptable convergent validity.

bKash The largest mobile financial services provider in Bangladesh, launched in 2011.

CFA (Confirmatory Factor Analysis) A statistical technique used to test whether measured variables adequately represent hypothesized latent constructs.

CFI (Comparative Fit Index) An incremental fit index in SEM ranging from 0 to 1; values ¿ 0.95 indicate excellent fit.

Common Method Bias Variance attributable to measurement method rather than constructs, a concern in single-source survey research.

Construct An abstract concept or latent variable (e.g., Swiftness, Risky Behavior) measured indirectly through multiple indicators.

CR (Composite Reliability) A reliability measure for latent constructs; values ¿ 0.70 indicate acceptable internal consistency.

Discriminant Validity The extent to which constructs are empirically distinct from one another.

Effect Size The magnitude of a relationship or difference, often measured by Cohen's d or standardized regression coefficients (β).

Endogenous Variable A dependent variable in SEM that is predicted by other variables in the model.

Exogenous Variable An independent variable in SEM that is not predicted by other variables in the model.

HTMT (Heterotrait-Monotrait Ratio) A discriminant validity criterion; values ¡ 0.85 indicate adequate discriminant validity.

Latent Variable An unobserved construct measured indirectly through multiple observed indicators.

Likert Scale A psychometric scale commonly used in questionnaires, typically ranging from 1 to 5 (e.g., Strongly Disagree to Strongly Agree).

MFS (Mobile Financial Services) Digital financial services accessed via mobile devices, including money transfers, bill payments, and merchant transactions.

Mediation A relationship where the effect of an independent variable on a dependent variable operates through an intermediary (mediator) variable.

Moderation A relationship where the strength or direction of an effect depends on the level of another variable (moderator).

Nagad A mobile financial services provider in Bangladesh launched in 2019 by Bangladesh Post Office.

OTP (One-Time Password) A temporary security code sent via SMS for transaction verification.

PEOU (Perceived Ease of Use) A TAM construct measuring the degree to which users believe a system is easy to use.

PIN (Personal Identification Number) A numeric password used to authenticate MFS transactions.

PS (Perceived Security) Users' beliefs about the safety and protection provided by an MFS application.

PU (Perceived Usefulness) A TAM construct measuring the degree to which users believe a system enhances task performance.

RB (Risky Behavior) Security-compromising behaviors such as PIN sharing, clicking unverified links, or using weak PINs.

RMSEA (Root Mean Square Error of Approximation) An absolute fit index in SEM; values ¡ 0.06 indicate excellent fit.

Rocket A mobile financial services provider in Bangladesh operated by Dutch-Bangla Bank.

SEM (Structural Equation Modeling) A multivariate statistical technique combining factor analysis and path analysis to test complex relationships.

SRMR (Standardized Root Mean Square Residual) An absolute fit index measuring the average discrepancy between observed and predicted correlations; values ¡ 0.08 indicate acceptable fit.

SWF (Swiftness) Users' preference for rapid, minimal-step transaction completion in MFS applications.

TAM (Technology Acceptance Model) A theoretical framework explaining technology adoption through Perceived Usefulness and Perceived Ease of Use.

TLI (Tucker-Lewis Index) An incremental fit index in SEM; values ¿ 0.95 indicate excellent fit.

VIF (Variance Inflation Factor) A diagnostic statistic for detecting multicollinearity; values ¡ 3.0 indicate no concern.