I.J. Information Engineering and Electronic Business, **2024, 2, 22-38**
Published Online on April 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2024.02.03

Security Analysis in Online Transaction Systems: A Proposed Framework

Rakin S. Aftab*
Department of Computer Science, American International University-Bangladesh, Dhaka, 1219, Bangladesh
E-mail: rakinsadaftab@gmail.com
ORCID iD: https://orcid.org/0000-0001-7164-5517
*Corresponding Author

Md. Kais K. Emon
Department of Computer Science, American International University-Bangladesh, Dhaka, 1219, Bangladesh
E-mail: emon.kaiskamal@gmail.com
ORCID iD: https://orcid.org/0009-0006-8172-3439

Sanjana F. Anny
Department of Computer Science, American International University-Bangladesh, Dhaka, 1219, Bangladesh
E-mail: annyfariha70@gmail.com
ORCID iD: https://orcid.org/0009-0004-7893-8602

Durjoy Sarker
Department of Computer Science, American International University-Bangladesh, Dhaka, 1219, Bangladesh
E-mail: durjoysarker520@gmail.com
ORCID iD: https://orcid.org/0009-0006-0866-4989

Md. Mazid-Ul-Haque
Department of Computer Science, American International University-Bangladesh, Dhaka, 1219, Bangladesh
E-mail: mazid@aiub.edu
ORCID iD: https://orcid.org/0000-0002-9091-7191

Received: 11 October, 2023; Revised: 30 December, 2023; Accepted: 07 February, 2024; Published: 08 April, 2024

Abstract: The safety of online transactions is paramount in the modern world, mainly since technology develops at a dizzying rate. This study aims to shed light on the numerous threats that users of online transaction systems face. The study used a mixed-methods research strategy to investigate the experiences and perspectives of 400 individuals from various backgrounds. Worryingly, the results show a significant knowledge gap on the many types of cyber hazards. The research reveals a troubling lack of awareness about various cyber risks, including fraud, phishing, and identity theft. It highlights the user's common functional difficulties. The study proposes a novel framework named COTSEF: A Comprehensive Framework for Enhancing Security in Online Transactions to enhance online transaction security alongside these findings. This comprehensive framework aims to provide a safer and more dependable environment for online commerce by mitigating the identified risks and challenges. The demographic breakdown of the users is also investigated, with the results indicating the increased vulnerability of some age groups and professions to various hazards. It also highlights the need for educational activities to address the significant need for more awareness about data protection rules. The study is a critical resource for policymakers, corporations, and educational institutions, offering actionable insights for developing more secure and user-friendly online transaction systems.

Index Terms: Online Transaction System Security, Scams & Fraud, Identity Theft, Phishing, Hacking, Awareness, Framework.

1. Introduction

In today's interconnected world, digital transformation has profoundly impacted daily life. Among the numerous changes, none is as revolutionary as the transformation observed in financial transactions. The internet and digital technologies have brought about an era where online transactions are often the preferred method of monetary exchange. These transactions span a wide range, from routine purchases on e-commerce platforms to complex financial operations. However, an increased risk of cyber threats that jeopardize the security and integrity of online transactions is the price of this convenience. Online transactions present high stakes, which have become ingrained in the fabric of the modern economy. It is not just a concern for individual users; their security is considered a matter of national economic stability. Consumer trust can be eroded, and significant financial losses can be caused by cyber threats like fraud, phishing, hacking, and identity theft, thereby impacting the economic well-being of nations. The current study seeks to address this urgent and growing problem by thoroughly investigating the risks associated with online transactions.

This research aims to accomplish several objectives. An in-depth analysis of the security risks users faces when conducting online transactions is intended to be provided first. Particular focus is given to the experiences and perspectives of a diverse group of 400 individuals to capture a comprehensive view of the challenges involved. This study introduces a novel security framework designed to counteract these risks and enhance the security of online transactions. Beyond its immediate academic contribution, the significance of this research is extended. Its findings offer real-world applications that could benefit various stakeholders, from individual users and businesses to policymakers and regulatory bodies. This study aims to contribute to a more secure and trustworthy digital transaction environment by identifying specific vulnerabilities and offering targeted solutions. In addition, insights into which age groups and professions are most vulnerable to cyber risks are provided by the demographic analysis carried out as part of this research, thereby enabling more focused educational and policy interventions.

The structure of this paper facilitates an accessible yet thorough understanding of the subject matter. This introduction follows a literature review that contextualizes the research within the existing work on online transaction security. A detailed explanation of the research methodology is then provided, after which findings are presented, and the proposed security framework is introduced. The paper concludes by discussing the broader implications of the research and suggesting avenues for future study.

2. Background Study

Mobile banking, a subset of electronic banking, has emerged as a transformative force in the financial sector, reshaping how individuals and businesses conduct financial transactions. The proliferation of smartphones, coupled with the government's encouragement of cashless transactions, has accelerated the adoption of mobile banking services worldwide. This literature review delves into various facets of mobile banking, focusing on factors influencing its adoption, security considerations, and user experiences. Drawing insights from recent research studies, this review highlights the multifaceted landscape of mobile banking, shedding light on the challenges, opportunities, and trends in this dynamic field. This review divides the literature into significant themes: adoption factors and user behavior, security and privacy concerns, technological innovations and solutions, cross-cultural and demographic variations, and methodologies and testing.

2.1. Cross-Cultural and Demographic Variations

Another area of interest is the influence of cultural and demographic factors on mobile banking adoption. This comparative study explores [1] mobile banking perceptions between U.S. and Thai consumers, revealing aspects that encourage or discourage mobile banking adoption in different cultural contexts. This cross-national study examines [2] age- and gender-dependent variations in consumer intentions and use of mobile banking services. It analyzes factors like trust, security, and privacy and their effects on mobile banking adoption among different demographic groups. This research explores [3] factors influencing customer experiences in mobile banking in Bangladesh. It is based on a survey of 231 mobile banking customers from nine private commercial banks. The study identifies factors like system convenience and responsiveness, transaction security, and technological difficulties affecting customer experiences. The results suggest that policymakers and banks should focus on improving these factors to enhance mobile banking services in Bangladesh. The study presents [4] an acceptability model based on the Unified Theory of Acceptance and Use of Technology (UTAUT) extended with factors like perceived risk, security, and trust. The model was tested with data from 460 mobile banking application users in Marrakech, Morocco. It identifies factors significantly impacting user's behavioral intentions to accept mobile banking services, providing insights into mobile banking adoption.

2.2. Adoption factors and user behavior

Various research studies have explored the factors influencing the adoption of mobile banking services. These factors range from trust and user perceptions to ease of use and usefulness. This study [5] extends the Unified Theory of Acceptance and Use of Technology (UTAUT2) to incorporate trust, security, and privacy factors. It reveals that habit, perceived security, privacy, and trust influence consumer’s behavioral intentions toward mobile banking adoption. In Bangladesh [6], factors such as expense, responsiveness, and relative advantage influence young customer satisfaction and retention in mobile banking, highlighting the importance of understanding customer perceptions. This research [7] focuses on the millennial generation's attitudes toward mobile banking services, indicating that trust, attitudes toward AI, religiosity, and relative advantage play critical roles in adoption intentions. The research [8] identifies factors influencing customer's use of mobile banking, including perceived usefulness, ease of use, and trust, except for perceived enjoyment. This study examines the relationships among perceived risk, trust, and intention to use mobile banking. The research model [9] explores how various factors influence consumer preferences for mobile banking services. It finds that factors like perceived risk, trust, and service quality play significant roles in shaping consumer's adoption of mobile banking. The research explores [10] factors influencing consumers to adopt mobile banking apps for various banking services. It investigates perceived usefulness, ease of use, security, and trust in mobile banking adoption. The study provides insights into promoting mobile banking adoption in the banking industry. This study focuses on the initial acceptance of mobile banking by existing online banking users in India. It develops a theoretical model based on the Technology Acceptance Model (TAM) extended with factors such as perceived ease of use, security, mobile self-efficacy, social influence, and customer support. The research finds [11] that these adoption factors significantly impact customers' behavioral intention to use mobile banking and aims to provide insights into digital banking channels and contribute to understanding mobile banking adoption in India. This study [12] analyzes the adoption and use of mobile banking by university students in Mongolia, focusing on factors like performance expectancy, effort expectancy, social influence, facilitating conditions, perceived security, perceived trust, and perceived risk. The results indicate that these factors influence student's acceptance and use of mobile banking, contributing to the understanding of mobile banking adoption among young adults.

2.3. Security and Privacy Concerns

Security is a recurring theme in mobile banking research, covering aspects like vulnerabilities, biometrics, and awareness programs. The security vulnerabilities in mobile banking applications are a growing concern. This study [13] employs a hybrid fuzzing testing technique to analyze data security requirements, emphasizing the importance of securing sensitive financial information. The study investigates [14] the current security status of mobile banking apps. It identifies the need for a consistent understanding of vulnerabilities and improved detection tools to secure mobile banking applications effectively. Security and privacy issues are addressed early in mobile application development. The study explores methodologies for secure mobile application development [15]. The paper highlights [16] the importance of security enhancement in UPI-based mobile apps to detect cybercrimes and fraudulent transactions, emphasizing the need for real-time analysis. The report [17] classifies and analyzes security issues and challenges in mobile banking in Uzbekistan, stressing the need for robust security measures in this rapidly growing sector. This study measures [18] information security awareness among users of Mobile Banking (M-Banking) applications. It uses the Knowledge- Attitude-Behavior (KAB) model to assess the information security awareness of M-banking users in Indonesia. The study finds that while overall security awareness is at a reasonable level, there is room for improvement in the use of social media, which scored lower in terms of knowledge, attitude, and behavior dimensions. The paper discusses [19] the increasing popularity of mobile banking services and the rise in online fraud cases related to the banking industry. It highlights the importance of awareness programs among bank customers to prevent and mitigate online fraud. This study examines [20] security threats and security measures in mobile and online banking systems. It explores the challenges and risks associated with the security of mobile financial services and discusses potential solutions to enhance security.

2.4. Methodologies and Testing

Research methods and frameworks used in the studies also contribute to understanding mobile banking services. This paper discusses [21] the importance of delivering innovative ideas quickly and reliably in core banking applications, particularly in mobile and Internet banking. It highlights the need for a DevOps culture in the financial industry, which combines agile development methodologies with automated processes for rapid application development and deployment. The paper also explores concepts like continuous integration and delivery, automation of testing, and the importance of maintaining security and reliability in these banking systems. This paper investigates [22] the impact of mobile banking service quality dimensions, such as ease of use, usefulness, security/privacy, and enjoyment, on customer's value co- creation intention (CVCCI) in the banking sector. It explores how these dimensions affect CVCCI and examines the roles of attitude toward mobile banking and bank trust in this context. This research investigates [23] consumers' attitudes and behavioral intentions to use mobile banking services at three stages: static, interaction, and transaction. It examines the factors influencing these intentions and the variations based on demographic characteristics, including age and gender. The paper investigates [24] the acceptance of mobile banking services in Malaysia, considering factors like perceived ease of use, usefulness, privacy, and security risks. It explores how these factors influence users' attitudes and behavioral intentions toward mobile banking. This study addresses [25] the adoption of mobile banking services in Jordan, emphasizing the importance of Supportive Access to mobile banking. It explores how this element impacts user satisfaction related to mobile banking. This literature survey reviews research trends [26] in mobile banking, covering various aspects such as customer satisfaction, adoption, perception, behavior, security, and privacy. It analyzes 68 research articles from the last ten years and highlights the importance of safety as one of the least discussed areas in mobile banking research. The review aims to inform future research directions in this field. The study examines [27] customer awareness and satisfaction with cybersecurity in the context of the digital transformation of banking in Saudi Arabia. It analyzes various aspects of cybersecurity, including cyberattacks, phishing, hacking, and customer satisfaction with bank cybersecurity assistance. The study highlights the importance of increasing customer awareness and dignity to enhance the security of digital banking transactions.

2.5. Technological Innovations and Solutions

This theme encompasses the technological solutions proposed or analyzed in research studies, such as personalization, biometrics, and cloud architecture. The personalization of mobile banking interfaces is explored to enhance the user experience. The study highlights [28] the significance of adaptive user interfaces in catering to the diverse needs of users. The study discusses [29] the impact of biometrics on mobile banking security and authentication methods used by EU Member States' banks, emphasizing the need for advanced authentication to secure mobile banking. This research paper explores [30] fingerprint authentication in mobile banking applications. The study involves developing a Java-based mobile application using fingerprint authentication for login and payment options. The research finds that the developed application is secure, user-friendly, and prosperous in terms of security. The paper discusses [31] using mobile cloud architecture to enhance mobile banking services in India. It focuses on processing speed, storage capacity, and security in mobile banking systems and proposes a cloud-based risk architecture to address these challenges. The paper discusses [32] user authentication countermeasures for Internet banking applications, mainly focusing on impersonation attacks. It explores user authentication based on biometrics, specifically touch dynamics biometrics, which considers unique user behaviors when interacting with touchscreen devices. The proposed framework, Bio-Touch, uses supervised machine learning and multiple scopes for continuous user authentication to enhance security for banking applications. This study focuses [33] on improving the efficiency of banking systems using Human-Computer Interaction (HCI) and modern technology in parts of Bangladesh. It discusses the challenges faced by users, bank managers, and agents in the mobile banking field and highlights the best services offered by mobile banking agencies, focusing on AI and machine learning techniques. An Android application has also been developed to summarize the work in this area.

3. Proposed Research Methodology

This study thoroughly examines the security challenges inherent in online financial transactions, which affect a variety of stakeholders, including people from various backgrounds. The study takes a mixed-methods approach, relying on quantitative data to achieve its goals. Fig.1 represents the path followed to enhance the research methodology.

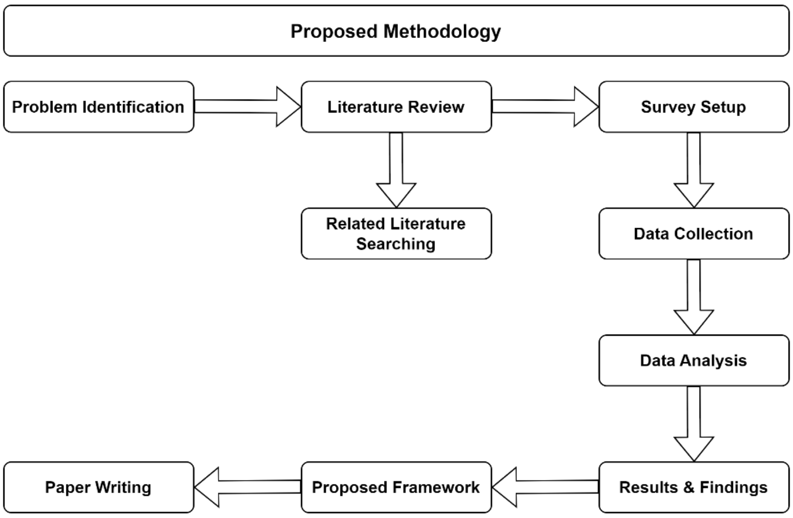

Fig. 1. Proposed Research Methodology

3.1. Problem Identification

While online transactions are simple, they also pose increasing security threats, such as cyber fraud and hacking, which harm individuals from different backgrounds. Existing security measures must be revised, and difficulties occur due to ethical and legal constraints such as data protection and privacy. This study seeks to discover these security flaws and moral challenges to provide a more efficient and compliant security framework, ultimately improving the safety and dependability of online transactions.

3.2. Data Collection

The study employs a quantitative, descriptive research design based on primary data collected via a structured questionnaire. The 20-question survey, based on existing literature and peer-reviewed articles, collects vital demograph ic data - age, gender, educational background, and employment status - as well as participant awareness of data security laws and prevalent cybercrimes such as phishing, identity theft, and hacking. Research advisers monitored the questionnaire's pretesting phase before distribution to ensure reliability and validity. The finalized survey was published across social media channels, including Facebook groups and LinkedIn, and directly with possible responders using Google Forms to increase participation. The participant's responses were scored on a 10-point Likert scale, with 1 indicating extreme discontent and 10 indicating complete satisfaction. The study collected completed questionnaires from 400 people using a convenience sample approach.

3.3. Sampling Method

For this research, a stratified mixed-methods approach was employed to gain a deeper and more comprehensive understanding of complex phenomena of quantitative data and ensure representation from various demographics within the target population. The target population consisted of mobile banking users in the region of interest. To obtain a diverse sample, the population was stratified based on factors such as age, gender, education, and spending level. Within each stratum, participants were randomly selected using a combination of online survey platforms, social media advertisements – different Facebook groups, LinkedIn.

3.4. Rationale for Sample Size

A sample size of respondents was selected to ensure a confidence level with a margin of error. The necessary sample size was determined to be 400 from 430 respondent, which was exceeded to guarantee a strong dataset. This sample size also facilitates rigorous subgroup analyses and improves the applicability of findings to the wider population of online banking users in the region. The survey utilized a stratified random sampling technique and determined an appropriate sample size to gather data that is representative and accurately reflects the viewpoints and experiences of users. This approach enhances the reliability and validity of the study's findings.

3.5. Data Analysis

The data for this study was rigorously evaluated using Python's statistical modules to gain a comprehensive understanding of online transaction security concerns. The analysis began with a demographic breakdown of the respondents to contextualize the study's conclusions. A careful assessment of the data distribution across several characteristics, such as age, occupation, and educational background, followed. The survey then examined participants' knowledge of common online hazards such as scams, fraud, identity theft, phishing, and hacking. In addition, the difficulties encountered by respondents in the realm of online transactions were investigated. Finally, descriptive data assessed customer satisfaction concerning monthly spending and existing security measures.

3.5.1. Overview of the Participants

The demographic profile of the 400 survey respondents in Table 1 reveals a skewed younger population, with 30% aged between 18-24 and 25% under 18. Adults in the 25-34 and 35-44 age brackets represent 15% and 12.5%, respectively, while older age groups of 45-54 and 55-60 make up 10% and 7.5%, respectively. Most respondents are male (61.25%), and the educational landscape is diverse: 47.5% have a high school education or less, 22.5% hold a bachelor's degree, 17.5% have a master's, and 12.5% possess a Ph.D. or advanced degree. Occupation-wise, homemakers form the largest segment at 31.25%, followed closely by employed individuals at 26.25%; students and people in business each account for 18.5%; and retirees comprise the smallest group at 5.5%. Notably, all respondents use online transactions, highlighting the ubiquity of digital financial platforms. In terms of monthly spending, the majority (21.25%) expend between 10,000 and 15000 units of currency, followed by the 1000-5000 and 5000-10000 ranges, which account for 20.5% and 17.75%, respectively. This demographic diversity allows the study to capture various experiences and perspectives on online transaction security.

Table 1. Overview of the Participants

Variable	Category	User Count	Percentage (%)
Age	Under 18	100	25.00
	18 - 24	120	30.00
	25 - 34	60	15.00
	35 - 44	50	12.50
	45 - 54	40	10.00
	55 - 60	30	7.50
Gender	Male	245	61.25
	Female	155	38.75
Education	High School or Less	190	47.5
	Bachelor's Degree	90	22.5
	Master's Degree	70	17.5
	Ph.D. or Advanced Degree	50	12.5

Occupation	Housewife	125	31.25
	Employed	105	26.25
	Student	74	18.50
	Businessman	74	18.50
	Retired	22	5.50
Use online transaction	Yes	400	100
	No	0	0
Spending	10000 - 15000	85	21.25
	1000 - 5000	82	20.50
	5000 - 10000	71	17.75
	500 - 1000	49	12.25
	50000 - 100000	48	12.00
	15000 - 49000	33	8.25
	0 - 500	32	8.00

3.5.2. Analysis of Different Distributions of the Participants

According to Table 2, 39.75% of users required assistance to set up their accounts (AOYA), while the majority (60.25%) did not. Surprisingly, only 11.75% of respondents read the Terms and Conditions (TC), indicating a significant gap in user understanding since 88.25% admitted to not reading them. The fact that 100% of People who don't Read Terms and Conditions (LTAC) participants agree strengthens this argument. Regarding message management (MC), 11.75% need to clear their messages, compared to 88.25% who do. Regarding user choice for Mobile Banking Systems (MBS), bKash and Rocket lead the market with 31.90% and 30.00% usage, respectively, while other platforms, such as CellFin and My Prime, have moderate to low adoption rates. This extensive data provides critical insights into online transaction user behaviors and preferences.

Table 2. Analysis of Different Distribution of the Participants

Variable	**Category**	**User Count**	**Percentage** (%)
AOYA	Yes	159	39.75
	No	241	60.25
TC	Yes	47	11.75
	No	353	88.25
LTAC	Yes	400	100
	No	0	0
MC	Yes	119	11.75
	No	281	88.25
MBS	bKash	268	31.90
	Rocket	252	30.00
	CellFin	176	20.95
	My Prime	60	7.14
	Nagad	50	5.95
	Upay	19	2.26
	SureCash	15	1.78
	Trust Axiata Pay (Tap)	0	0
	City Touch	0	0
	EBL SKYBANKING	0	0
	NexusPay	0	0
	MTB Smart Banking	0	0

3.5.3. Analysis of Public Awareness in Online Security

This study provides essential insights into widespread awareness of online security threats in Table 3. Many respondents have firsthand knowledge of many types of cybercrime. 29.5% of participants reported experiencing scams, and an equal number acknowledged falling victim to fraud, demonstrating a high prevalence of these cyber dangers. Identity theft and phishing were also reported by 30.75% of survey participants, indicating that current security measures may be inadequate.

Table 3. Analysis of Public Awareness on Online Security

Variable	**Category**	**User Count**	**Percentage** (%)
Scams	Yes	118	29.50
	No	282	70.50
Frauds	Yes	118	29.50
	No	282	70.50
Identity Theft	Yes	123	30.75
	No	277	69.25
Phishing	Yes	123	30.75
	No	277	69.25
Hacking	Yes	237	59.25
	No	163	40.75

The most concerning finding is that 59.25% of respondents have been victims of hacking attempts or successful hacks. This figure is dangerously high compared to other types of cybercrime and should serve as a significant red flag for prompt action. While there are legitimate concerns about scams, identity theft, and phishing, hacking is the most pressing issue that requires rapid and extensive responses. These findings highlight the necessity for robust, multi-layered security solutions and enhanced public awareness to protect against these common online risks.

3.5.4. Analysis of Different Problems Faced by the Participants

Table 4 discovered significant challenges beyond security concerns in the detailed investigation of user-reported problems with online transactions. Scams are reported by 18.85% of participants, closely followed by fraud and phishing concerns, which affect 18.17% of the user base. Identity theft is a nearly equal worry, with 18.18% of users reporting it. Hacking involves 15.71% of respondents, although it is slightly less widespread. Intriguingly, a smaller but significant portion of 10.92% said no security difficulties, indicating that present security procedures were adequate or fortunate enough to escape such pitfalls.

The study, however, extends beyond security concerns. Regarding other functional issues, One Time Password (OTP) cases were the most reported, affecting 50.10% of customers. QR scan difficulties were the second most common, affecting 31.10% of respondents. As indicated by 18.81% of respondents, connectivity concerns were significant. Surprisingly, no respondents indicated a complete lack of these "other" difficulties, indicating a widespread need for improvements in the entire user experience of online purchases. This complex insight emphasizes the importance of a comprehensive approach that addresses security issues while improving functional usability to satisfy many user concerns.

Table 4. Analysis of Different Problems Faced by Participants

Variable	Category	User Count	Percentage (%)
Security Problems	Scam	252	18.85
	Fraud	243	18.17
	Phishing	243	18.17
	Identity Theft	243	18.18
	Hacking	210	15.71
	None	146	10.92
Other’s Problems	OTP	277	50.10
	QR Scan	172	31.10
	Connectivity	104	18.81
	None	0	0.00

Table 5 shows the descriptive statistics needed to get critical insights into user behavior and satisfaction levels. The average monthly spending of customers was BDT 16,354.38, significantly more significant than the BDT 7,500.00 median. This disparity shows a skewed distribution, implying that many consumers contribute significantly higher expenditure levels, raising the average. Regarding customer satisfaction, the data shows a reasonable average rating of 5.04 on a 10-point Likert scale, supported by a comparable median value of 5.00. The standard deviation of 1.45, reflecting substantial fluctuations in user satisfaction ratings, adds nuance to this intermediate level of contentment.

Surprisingly, the minimum satisfaction level reported was as low as 2.00, indicating the presence of a significant sector of disgruntled users. Furthermore, the significant standard deviation in spending, equal to BDT 23,204.89, demonstrates a wide range of spending habits within the user population. These findings show a compelling need for customized service offers and intentional improvements in service quality to accommodate users' different needs and degrees of satisfaction.

Table 5. Descriptive Statistics for Spendings & Ratings

	Count	Average Spending (BDT)	Satisfaction Ratings
mean	400	16354.38	5.04
median	400	7500.00	5.00
std	400	23204.89	1.45
min	400	250.00	2.00
max	400	75000.00	8.00

4. Result and Findings

An in-depth study of survey data was used to investigate critical concerns linked to online transaction security. The incidence of security issues, user satisfaction levels, and awareness of privacy legislation were all discovered. Recommendations were developed based on the findings to improve online transaction security and the user experience. The results were summarized to provide practical solutions for enhancing the integrity of online transactions.

Fig. 2 depicts the percentage of users encountering issues based on their educational levels. The data indicates that individuals with a High School or Less educational background face the most challenges, constituting 35.77% of the problem reports. This is followed by those with a bachelor's degree, who account for 28.85% of the reported issues. Master's degree holders experience fewer problems, contributing to 21.15% of the total, while Ph.D. holders encounter the most minor issues at 14.23%. A pattern emerges, suggesting a negative correlation between educational attainment and the frequency of the issues faced. Such insights are crucial for devising strategies tailored to the unique needs of different educational demographics.

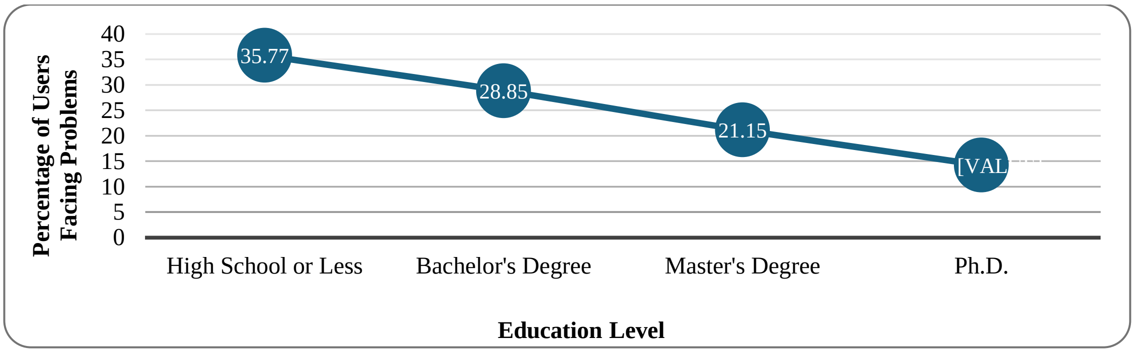

Fig. 2. Number of Users Facing Problems Related with Education Level

Fig. 3 reveals significant disparities in user issues based on gender and educational level. Males with a High School or Less education encounter the highest incidence of problems at 23.85%, notably higher than their female counterparts at 11.92%. Conversely, females with a bachelor's degree experience the most issues at 19.62%, outpacing males in the same educational category at 9.23%. Across both genders, individuals with advanced degrees report fewer issues, suggesting that higher education correlates with an improved user experience. These findings highlight the need for targeted, gender- and education-specific strategies to enhance platform reliability.

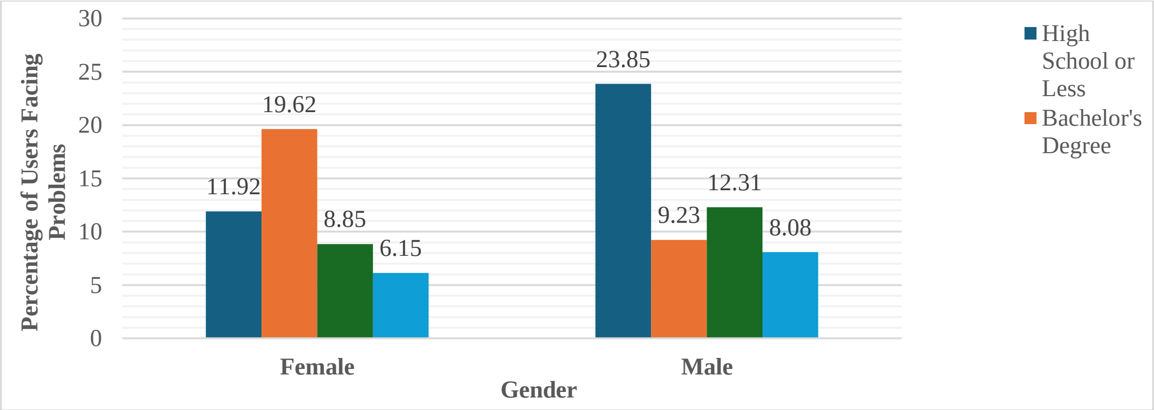

Fig. 3. Visualization of Users Facing Problems Related with Gender and Education Level

When security-related concerns, including categories such as scams, fraud, identity theft, phishing, and hacking, are analyzed, a remarkable pattern appears. This pattern may be broken down into many subcategories. Across the board, a sizeable proportion of those who experienced security vulnerabilities had not shown any signs of knowledge regarding these concerns. For instance, in the categories of scam and fraud, 62.00% and 44.00% of persons who replied no to awareness found them confronted with these situations, but only 1.00% of those who claimed knowledge faced them. In the case of identity theft and phishing, the findings are even more surprising because there was not a single documented instance in which awareness was linked to experiencing these problems. This highlights the significant gap that exists between knowledge and actual incidences. However, hacking has a more equal distribution, with incidences happening among individuals aware of the problem and those oblivious to it. These findings highlight the crucial role that education and awareness play in decreasing security risks since a lack of knowledge tends to correspond with a greater frequency of security concerns in most circumstances. Education and cognition may be achieved through various channels, including formal and informal education, training programs, and public campaigns, referring to the below Fig. 4.

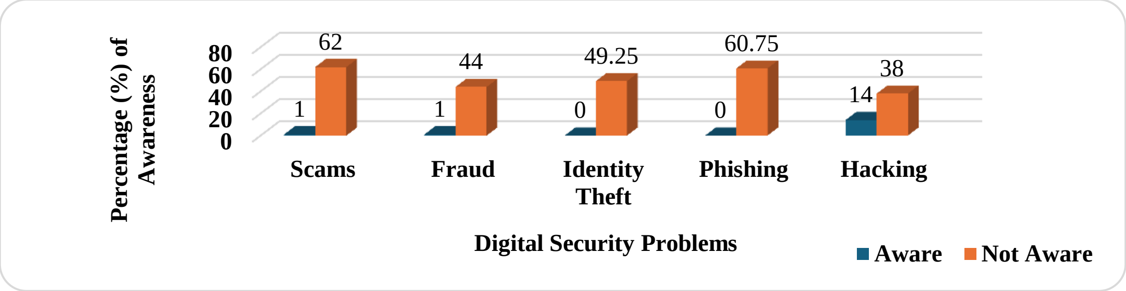

Fig. 4. Public Awareness on digital security problems

Several vital patterns and comparisons emerge in this analysis of security issues reported by users of different mobile banking platforms - bKash, Nagad, Rocket, SureCash, Upay, and CellFin. Fig. 5 reveals that bKash users reported the highest number of security issues across different categories, notably facing a substantial prevalence of hacking, with 69.64% of respondents reporting incidents, and scams, where 2.2% of users encountered fraudulent activities.

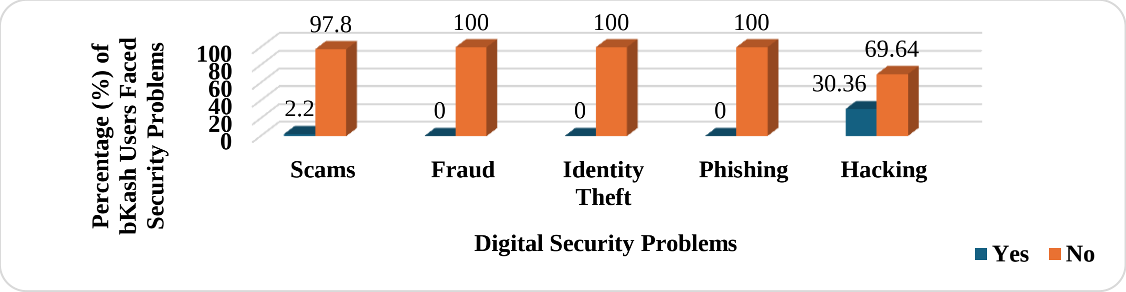

Fig. 5. Digital Security Issues faced by bKash Users.

However, in Fig. 6, 20.47% of Rocket users reported encountering hacking issues. This discrepancy highlights a higher frequency of periodic reports related to hacking among users.

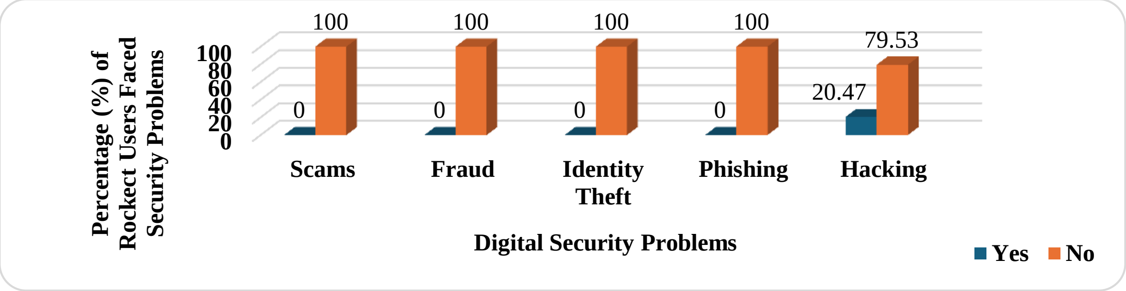

Fig. 6. Digital Security Issues faced by Rocket Users

In Fig. 7, statistics for SureCash users indicate fewer security issues overall, with no reports of fraud, identity theft, or phishing problems. However, 50% of SureCash users encountered hacking issues.

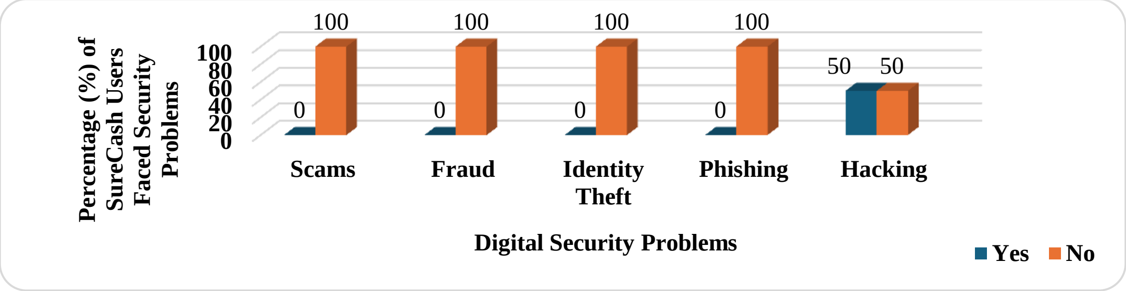

Fig. 7. Digital Security Issues faced by SureCash Users

In Fig. 8, statistics for Upay users reveal fewer overall security issues, with no reports of fraud, identity theft, or phishing problems. However, 16.67% of Upay users experienced hacking issues.

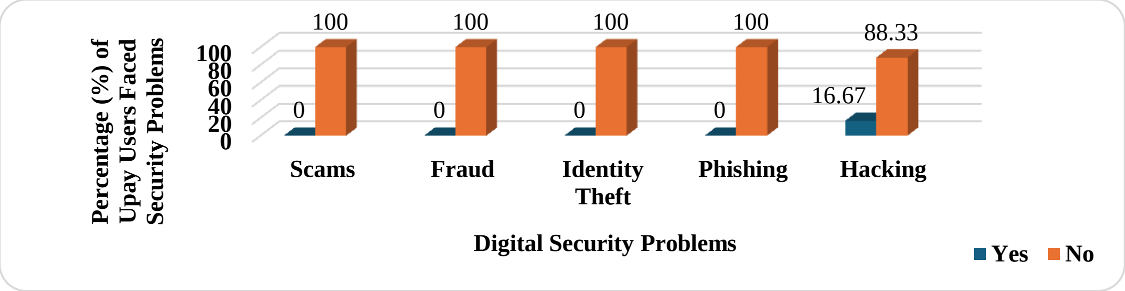

Fig. 8. Digital Security Issues faced by Upay Users

Nagad reported fewer overall security issues, showing similar patterns across categories, except for instances of hacking. Fig. 9 and Fig. 10 reveal an astonishing incident where none of the respondents of Nagad and CellFin users faced any digital threats. This observation is noteworthy because it suggests a commendable level of security resilience within these platforms, indicating robust protective measures or user behaviors that mitigate potential risks. Such findings underscore the importance of further examination into the security frameworks to identify strategies that effectively safeguard users' digital transactions and enhance overall trust in mobile banking services.

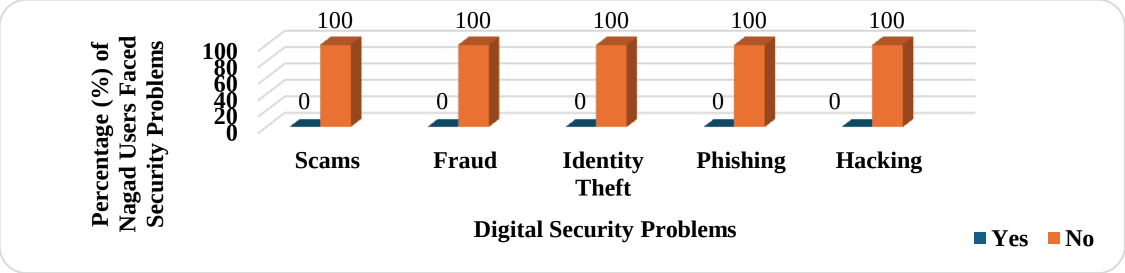

Fig. 9. Digital Security Issues faced by Nagad Users

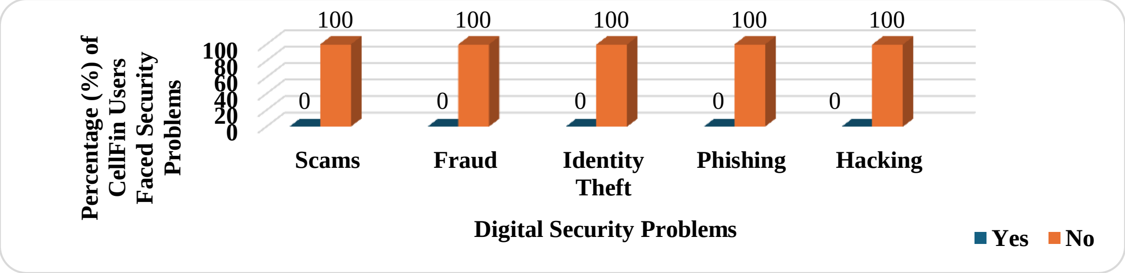

Fig. 10. Digital Security Issues faced by CellFin Users

The distribution of users in Fig. 11, categorized into Don't Clear Messages and Clear Messages, is observed to have experienced OTP problems. In the Don't Clear Messages category, most users (273, or 68.25%) are found, suggesting that most users who did not clear their messages reported facing OTP problems. In contrast, a tiny percentage (1.00%) of users in the Clear Messages category reported OTP problems. This stark contrast indicates a significant disparity in OTP problems between users who clear their messages and those who do not.

Fig. 12 provides a deeper breakdown of OTP problem cases by gender and MC (Message Clearing) response. Among male users who did not clear messages, the reported OTP problems constituted 61.37% of the cases. Similarly, female users who did not clear messages accounted for 37.18% of the OTP problem cases. Notably, there were 1.44% of OTP problems among male users who cleared messages, while there were no reported OTP problems among female users who cleared messages. This analysis highlights that most OTP problem cases are associated with users who do not clear messages, irrespective of gender. Additionally, it suggests a potential correlation between the lack of message clearing and OTP problems, with a gender-specific difference in the response to message clearing. However, given the limited sample size, especially for female users who clear messages.

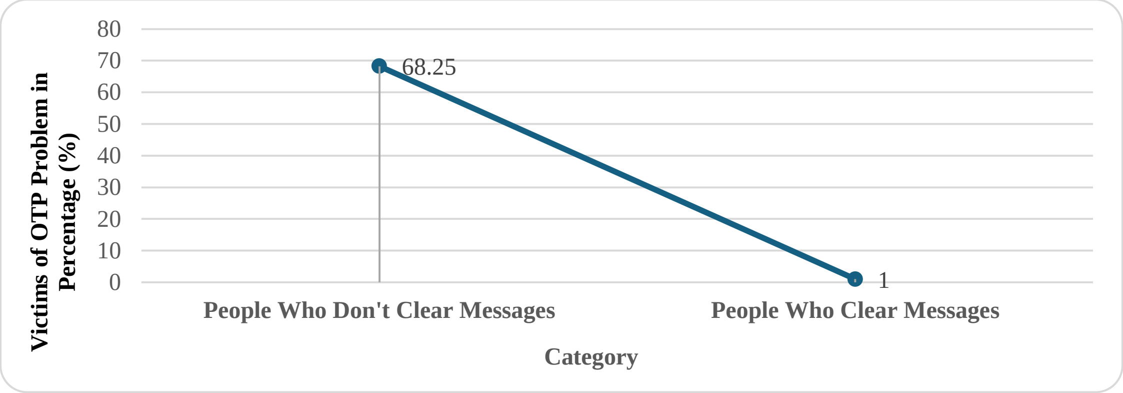

Fig. 11. OTP problems Faced by Users

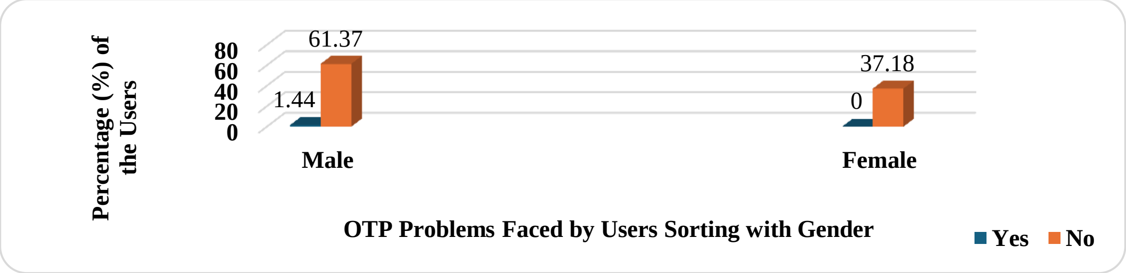

Fig. 12. OTP Problems Faced by Users Sorting with Gender

Fig. 13 provides insights into the distribution of security issues users report and their corresponding percentage levels. Scams and phishing are the most prevalent security concerns, accounting for around 23.42% and 22.58% of all reported issues. Hacking follows closely behind, representing approximately 19.33% of the total. Identity theft and fraud are reported at percentages of about 18.31% and 16.36%, respectively, making them slightly less common but still significant concerns. These findings emphasize the need for robust security measures and user awareness to combat scams, phishing attempts, hacking incidents, identity theft, and fraud in the digital realm. The user's vigilance against these threats highlights the importance of addressing these issues effectively.

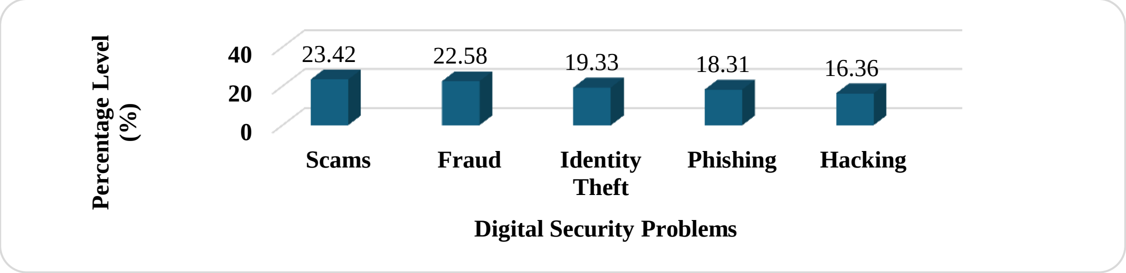

Fig. 13. Digital Security Issues Faced by Users

Fig. 14 presents a breakdown of various problems reported by users, explicitly focusing on OTP, QR Scan, and connectivity issues. OTP-related problems emerge as the most frequently encountered, constituting approximately 50.09% of reported cases. QR-Scan issues follow closely behind, accounting for about 31.10% of the total trials. Connectivity issues, while less common, still hold significance, accounting for an 18.81% share of reported issues. This data underscores the prevalence of OTP problems among users but also highlights the importance of addressing QR scan and connectivity issues to enhance user satisfaction and the overall mobile banking experience.

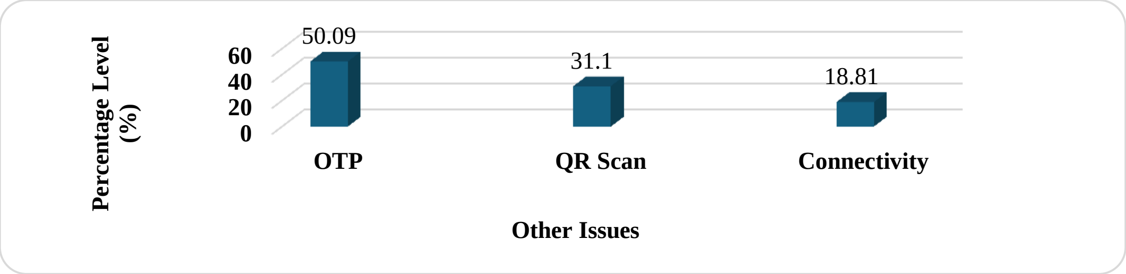

Fig. 14. Other Issues Faced by Users

The Pearson correlation coefficients have unveiled significant patterns in the comprehensive analysis of digital security factors. Firstly, in Fig. 15, in cybersecurity, strong positive correlations were observed among scams and phishing (0.95) and scams and hacking (0.71), indicating that these threats often co-occur.

Secondly, Fig. 16, examining digital authentication methods, noted a substantial negative correlation of -0.89 between connectivity and OTP, suggesting that one-time password (OTP) usage declines as connectivity issues intensify. Lastly, QR scanning, and connectivity exhibit a relatively weak positive correlation of 0.05, implying a modest association between these factors. These findings shed light on the intricate relationships between cybersecurity and digital authentication, emphasizing the importance of holistic security strategies and dependable connectivity in safeguarding against cyber threats and facilitating secure online transactions.

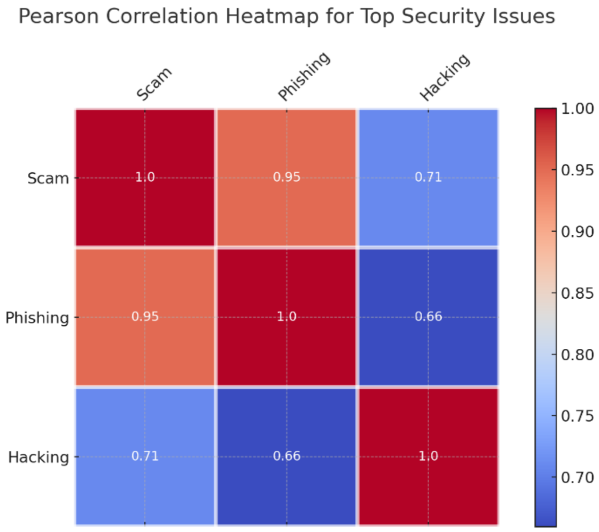

Fig. 15. Correlation Between Major Three Problems

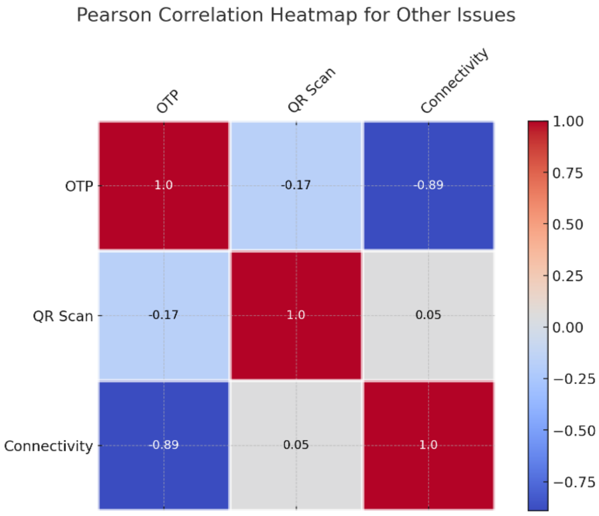

Fig. 16. Correlation Between Other Problems

5. Proposed Framework

In this section, an innovative and comprehensive architecture was created to increase user awareness, safety, and dependability to solve the complex difficulties surrounding the security of online transactions. As the digital world continues to grow, the risks posed by cybercriminals continue to adapt and expand. Because of this, it is imperative to take preventative measures to secure critical transactions. The architecture presented here capitalizes on tried-and-true online transaction security principles while also including forward-thinking components to meet the ever-changing nature of cybersecurity dangers.

This framework in Fig. 17 combines the most effective security techniques with the agility necessary to counteract new hazards successfully. This section introduces the fundamental components and concepts that form the basis of the framework. The section focuses on the potential of the framework to reinforce the digital realm and create confidence among all stakeholders who participate in online transactions. The framework is an example of a preventative and flexible approach to online commerce security, making it well-positioned to address the problems of the digital era head-on.

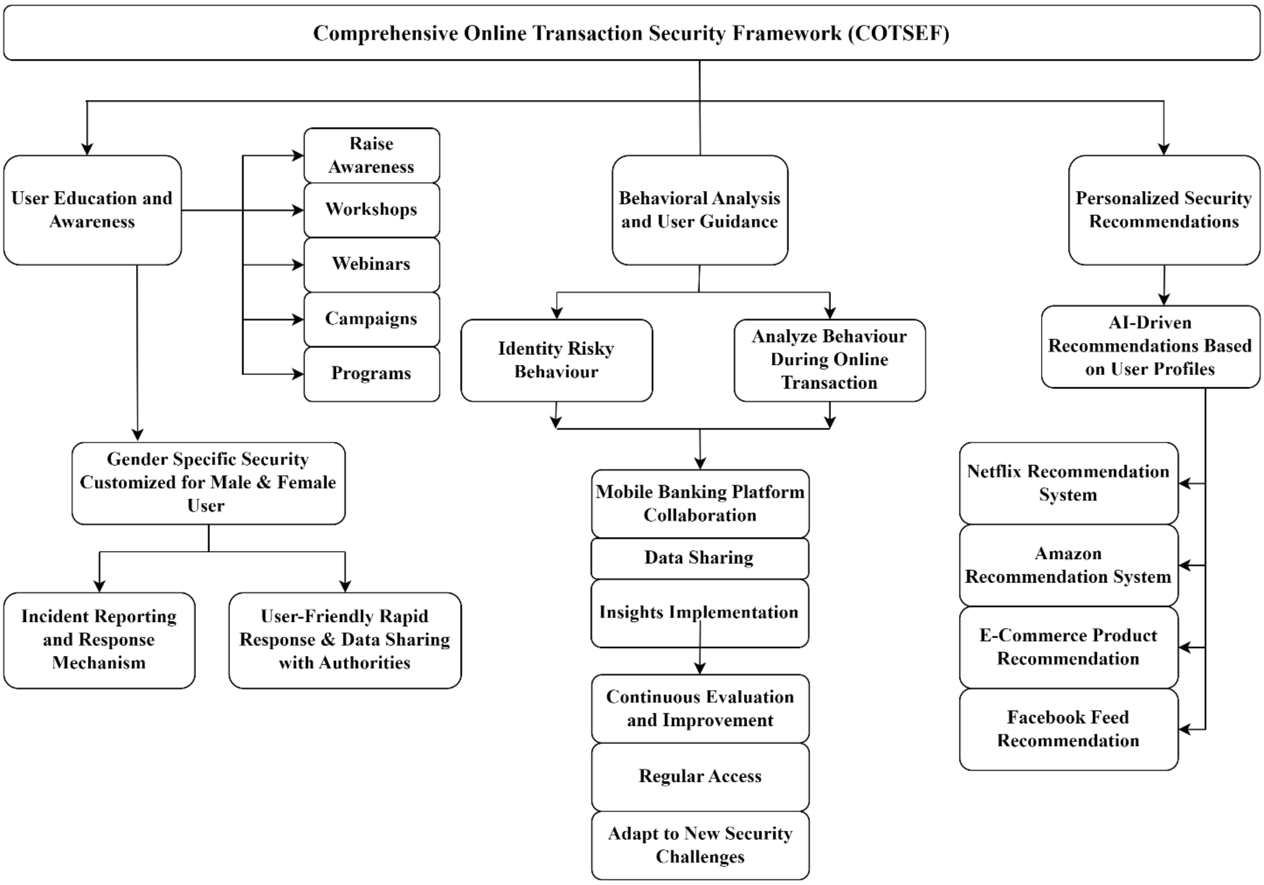
Comprehensive Online Transaction Security Framework (COTSEF)
User Education and Awareness
Raise Awareness
Workshops
Webinars
Campaigns
Programs
Behavioral Analysis and User Guidance
Personalized Security Recommendations
Identity Risky Behaviour
Analyze Behaviour During Online Transaction
AI-Driven Recommendations Based on User Profiles
Gender Specific Security Customized for Male & Female User
Mobile Banking Platform Collaboration
Data Sharing
Insights Implementation
Netflix Recommendation System
Amazon Recommendation System
E-Commerce Product Recommendation
Facebook Feed Recommendation
Incident Reporting and Response Mechanism
User-Friendly Rapid Response & Data Sharing with Authorities
Continuous Evaluation and Improvement
Regular Access
Adapt to New Security Challenges

Fig. 17. Proposed Framework of OTS

User Education and Awareness: Awareness, Workshops, Webinars, Campaigns, and Programs are the different channels through which awareness will be raised by informing users about the risks involved in online transactions and ways to mitigate them. Educated users are less likely to fall for scams, fraud, identity theft, phishing, hacking, or risky behavior.

- **Gender-Specific Security Customized for Male and Female Users:** To address the gender-based differences in experiencing security challenges per research findings. Tailoring education and security measures to gender- specific needs can lead to more effective risk mitigation.
- **Incident Reporting and Response Mechanism:** A system for users to report security incidents. Quick reporting can lead to faster resolution and prevent the spread of specific security threats.
- **User-Friendly Rapid Response and Data Sharing with Authorities:** To make it easier for authorities to act on reported incidents. Streamlining this process can lead to quicker action from authorities, minimizing damage.

Behavioral Analysis and User Guidance: Identify Risky Behaviors to monitor user behavior and identify actions that could lead to security vulnerabilities. Early identification of risky behavior can help prevent security incidents proactively. And Analysis of Behavior During Online Transactions for a deeper dive into user actions during transactions. Understanding the 'why' behind specific actions can lead to more effective educational programs and security measures.

- **Mobile Banking Platform Collaboration and Data Sharing:** Collaboration with different platforms to share insights. Sharing data can lead to industry-wide improvements in security measures.
- **Insights Implementation:** Implementing the learnings from the behavioral analysis. Implementing insights will lead to more robust security systems and user guidelines.

Personalized Security Recommendations: AI-driven recommendations Based on User Profiles to provide security recommendations tailored to individual user behaviors and needs. Customized advice can be more effective than general guidelines.

- **Netflix, Amazon, E-commerce, and Facebook Feeds Recommendations System** to indicate the potential effectiveness of such a personalized system by drawing parallels with successful models in other domains. These examples serve as proof that personalized recommendations work.

The COTSEF: A Comprehensive Framework for Enhancing Security in Online Transactions successfully addresses the issue from multiple angles, targeting systemic and individual behaviors contributing to digital security vulnerabilities.

6. Conclusion

The proposed COTSEF: A Comprehensive Framework for Enhancing Security in Online Transactions offers a multifaceted approach to address these challenges. By focusing on user education and awareness, behavioral analysis, personalized security recommendations, gender-specific security modules, collaboration with mobile banking platforms, incident reporting, and continuous evaluation, COTSEF aims to create a safer and more dependable online transaction environment.

This study has several key insights and takeaways: 1. Online transaction security is a complex and evolving field, with users facing various threats and challenges. 2. Education and awareness are crucial in equipping users with the knowledge to identify and mitigate security risks. 3. Adequate security measures require personalization that considers user behavior and characteristics. 4. Collaboration among stakeholders, including users, educational institutions, and mobile banking platforms, is instrumental in building a secure digital ecosystem. 5. Continuous evaluation and improvement are vital to adapting to threats and user needs.

6.1. Limitations

While research and the proposed framework offer valuable insights and solutions, it is essential to acknowledge certain limitations. The study's findings are based on survey data, which may be subject to biases and inaccuracies inherent in self-reported responses. The proposed framework, COTSEF, is a conceptual framework, and its real-world implementation may face technical, logistical, and adoption challenges. The framework's effectiveness in addressing online transaction security challenges will depend on user engagement, stakeholder collaboration, and the dynamic nature of cybersecurity threats.

6.2. Future Work

Building on this research, several avenues for future work emerge. Conducting in-depth user studies to gather more precise data on online transaction security challenges and user behaviors. Prototyping and testing the COTSEF framework in real-world settings to assess its practicality and effectiveness. Exploring advanced technologies, such as machine learning and artificial intelligence, to enhance the accuracy of behavioral analysis and security recommendations. Expanding collaboration with broader stakeholders, including government agencies, financial institutions, and cybersecurity experts, to create a more robust and holistic security ecosystem. Continuously updating and refining the framework to adapt to emerging cybersecurity threats and user needs.

In conclusion, online transaction security is an ever-evolving field that demands innovative solutions and collaborative efforts. This study and the proposed COTSEF framework represent significant steps toward enhancing the safety and dependability of online transactions. While challenges and limitations exist, the commitment to improving online security remains unwavering with ongoing research, testing, and collaboration to work toward a more secure digital future for all users.

References

[1] C. Changchit, T. Klaus, R. Lonkani, and J. Sampet, “A cultural comparative study of mobile banking adoption factors,” Journal of Computer Information Systems, vol. 60, no. 5, pp. 484–494, 2019. doi:10.1080/08874417.2018.1541724

[2] M. Merhi, K. Hone, A. Tarhini, and N. Ameen, “An empirical examination of the moderating role of age and gender in consumer mobile banking use: A cross-national, Quantitative Study,” Journal of Enterprise Information Management, vol. 34, no. 4, pp. 1144–1168, 2020. doi:10.1108/jeim-03-2020-0092

[3] Islam, N., Mustafi, M., Rahman, M. N., Nower, N., Rafi, M. M. A., Natasha, M. T., Hassan, R., and Afrin, S., "Factors affecting customers’ experience in mobile banking of Bangladesh," Available at SSRN, 2018. [Online]. Available: SSRN 3305925.

[4] Lafraxo, Y., Hadri, F., Amhal, H., and Rossafi, A., "The Effect of Trust, Perceived Risk and Security on the Adoption of Mobile Banking in Morocco," in ICEIS (2), 2018, pp. 497-502.

[5] M. Merhi, K. Hone, and A. Tarhini, “A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and Trust,” Technology in Society, vol. 59, p. 101151, 2019. doi: 10.1016/j.techsoc.2019.101151

[6] N. Jahan and G. Shahria, “Factors effecting customer satisfaction of mobile banking in Bangladesh: A study on young users’ perspective,” South Asian Journal of Marketing, vol. 3, no. 1, pp. 60–76, 2021. doi:10.1108/sajm-02-2021-0018

[7] A. M. Yussaivi, C. Y. Lu, M. E. Syarief, and D. Suhartanto, “Millennial experience with mobile banking and mobile banking artificial intelligence evidence from Islamic banking,” International Journal of Applied Business Research, pp. 39–53, 2021. doi:10.35313/ijabr.v3i1.121

[8] Y. Sulaiman and N. Jauhari, “The factors influencing mobile banking usage among university staff,” WSEAS TRANSACTIONS ON BUSINESS AND ECONOMICS, vol. 18, pp. 179–189, 2021. doi:10.37394/23207.2021.18.19

[9] H. N. Van et al., “Impact of perceived risk on mobile banking usage intentions: Trust as a mediator and a moderator,” International Journal of Business and Emerging Markets, vol. 12, no. 1, p. 94, 2020. doi:10.1504/ijbem.2020.106202

[10] T. Zhang, C. Lu, and M. Kizildag, “Banking ‘on-the-go’: Examining consumers’ adoption of mobile banking services,” International Journal of Quality and Service Sciences, vol. 10, no. 3, pp. 279–295, 2018. doi:10.1108/ijqss-07-2017-0067

[11] S. Singh and R. K. Srivastava, “Understanding the intention to use mobile banking by existing online banking customers: An empirical study,” Journal of Financial Services Marketing, vol. 25, no. 3–4, pp. 86–96, 2020. doi:10.1057/s41264-020-00074-w

[12] S. A. Raza, N. Shah, and M. Ali, “Acceptance of mobile banking in Islamic banks: Evidence from modified utaut model,” Journal of Islamic Marketing, vol. 10, no. 1, pp. 357–376, 2019. doi:10.1108/jima-04-2017-0038

[13] S. Bhatnagar, Y. Malik, and S. Butakov, “Analysing data security requirements of Android Mobile Banking Application,” Lecture Notes in Computer Science, pp. 30–37, 2018. doi:10.1007/978-3-030-03712-3_3

[14] S. Chen et al., “Are Mobile Banking Apps Secure? what can be improved?,” Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2018. doi:10.1145/3236024.3275523

[15] Ş. Şentürk, H. Yaşar, and İ. Soğukpınar, “Model Driven Security in a mobile banking application context,” Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019. doi:10.1145/3339252.3340529

[16] K. K. Lakshmi, H. Gupta, and J. Ranjan, “UPI based Mobile Banking Applications – Security Analysis and enhancements,” 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019. doi:10.1109/aicai.2019.8701396

[17] A. Abdullaev et al., “Security Challenge and issue of Mobile Banking in republic of uzbekistan: A State of Art Survey,” 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019. doi:10.23919/icact.2019.8701952

[18] K. Firsty Arisya, Y. Ruldeviyani, R. Prakoso, and A. Lailatul Fadhilah, “Measurement of Information Security Awareness Level: A case study of mobile banking (M-banking) users,” 2020 Fifth International Conference on Informatics and Computing (ICIC), 2020. doi:10.1109/icic50835.2020.9288516

[19] P. Datta, S. Tanwar, S. N. Panda, and A. Rana, “Security and issues of M-banking: A technical report,” 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2020. doi:10.1109/icrito48877.2020.9198032

[20] N. Yildirim and A. Varol, “A research on security vulnerabilities in online and Mobile Banking Systems,” 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 2019. doi:10.1109/isdfs.2019.8757495

[21] A. S. OZTAS, E. YEMEN, and E. TUZUN, “International Conference on Advanced Technologies, Computer Engineering and Science (ICATCES’18),” in Real-Time Monitoring and Control of The SDLC Process on a Single Automation in Core Banking Applications, 2018, pp. 104–108

[22] R. B. Mostafa, “Mobile Banking Service Quality: A new avenue for customer value co-creation,” International Journal of Bank Marketing, vol. 38, no. 5, pp. 1107–1132, 2020. doi:10.1108/ijbm-11-2019-0421

[23] M. A. Shareef, A. Baabdullah, S. Dutta, V. Kumar, and Y. K. Dwivedi, “Consumer adoption of mobile banking services: An empirical examination of factors according to adoption stages,” Journal of Retailing and Consumer Services, vol. 43, pp. 54–67, 2018. doi:10.1016/j.jretconser.2018.03.003

[24] Z. U. Rehman*, S. S. Omar, S. B. Zabri, and S. Lohana, “Mobile banking adoption and its determinants in Malaysia,” International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 1, pp. 4231–4239, 2019. doi:10.35940/ijitee.l3015.119119

[25] K. Aldiabat, A. Al-Gasaymeh, and A. S. K.Rashid, “The effect of mobile banking application on customer interaction in the Jordanian banking industry,” International Journal of Interactive Mobile Technologies (iJIM), vol. 13, no. 02, p. 37, 2019. doi:10.3991/ijim.v13i02.9262

[26] K. A. Kelly and S. Palaniappan, "Survey on Customer Satisfaction, Adoption, Perception, Behaviour, and Security on Mobile Banking," J. Inform. Tech. Softw. Eng., vol. 9, pp. 259, 2019. doi: 10.35248/2165-7866.19.9.259

[27] A. Johri and S. Kumar, “Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: A study in the era of Banking Digital Transformation,” Human Behavior and Emerging Technologies, vol. 2023, pp. 1–10, 2023. doi:10.1155/2023/2103442

[28] M. Nawaz, L. Motiwalla, and A. V. Deokar, “Adaptive user interface for a personalized mobile banking app,” Adjunct Publication of the 26th Conference on User Modeling, Adaptation and Personalization, 2018. doi:10.1145/3213586.3226209

[29] A. Avdić, “Use of Biometrics in Mobile Banking Security: Case Study of Croatian Banks,” IJCSNS International Journal of Computer Science and Network Security, vol. 19, Oct. 2019

[30] L. Sharma and M. Mathuria, “Mobile banking transaction using Fingerprint Authentication,” 2018 2nd International Conference on Inventive Systems and Control (ICISC), 2018. doi:10.1109/icisc.2018.8399016

[31] P. Rajarajeswari, M. Sreevani, and P. Lalitha Suryakumari, “Secure Cloud Risk Architecture Analysis for mobile banking system and its performance analysis based on machine learning approaches,” Journal of Physics: Conference Series, vol. 2089, no. 1, p. 012007, 2021. doi:10.1088/1742-6596/2089/1/012007

[32] P. M. Estrela, R. de Albuquerque, D. M. Amaral, W. F. Giozza, and R. T. Júnior, “A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications,” Sensors, vol. 21, no. 12, p. 4212, 2021. doi:10.3390/s21124212

[33] M. T. Ahmed, M. T. Imtiaz, and A. A. Kauser, "A comparative study of mobile banking in specific parts of Bangladesh," Int. J. Sci. Bus., vol. 4, no. 6, pp. 129-139, 2020

Authors’ Profiles

Rakin Sad Aftab is a student at American International University-Bangladesh (AIUB) in the Department of Computer Science under the Faculty of Science and Technology. He is interested in research areas, including Machine learning, Deep learning, Artificial intelligence, Blockchain and SDLC. He has experience with machine learning, software engineering, and data science projects. Currently, he is exploring the world of Artificial Intelligence. Because he believes AI would be the end of mankind. He can be contacted at rakinsadaftab@gmail.com

Md Kais Kamal Emon is a dedicated American International University-Bangladesh (AIUB) student pursuing a degree in the Department of Computer Science within the Faculty of Science and Technology. His academic interests revolve around cutting-edge research areas such as Machine Learning, artificial intelligence, Deep Learning, Big Data, and Natural Language Processing. During his educational journey, he gained valuable experience through various machine-learning projects.

Sanjana Fariha Anny is pursuing her studies at the American International University-Bangladesh (AIUB) in the Department of Computer Science, which falls under the Faculty of Science and Technology. Her academic journey is marked by a profound passion for cutting-edge technologies, primarily focusing on Machine Learning, Neural Networks, Computer Vision, and Deep Learning. She has an impressive track record of successfully completing numerous projects related to data analysis, showcasing her expertise in these fields.

Durjoy Sarker studies Computer Science at American International University-Bangladesh (AIUB). He is passionate about Machine Learning, Deep Learning, Data Mining, and Machine Learning Data Analytics. He also delves into problem-solving and research. Throughout his academic endeavors, he has acquired valuable expertise through diverse data analysis and database architecture projects.

Md. Mazid-Ul-Haque is currently working as a Lecturer in the Department of Computer Science at American International University-Bangladesh (AIUB). He has completed his Master of Science in Computer Science and Bachelor of Science in Computer Science and Engineering degrees from AIUB with the highest honor and academic awards. He did his HSC at Notre Dame College, Dhaka. He has a strong passion and dedication for teaching and research work. His research interests include but are not limited to Networks, Wireless Communication, and SDLC. He can be contacted at mazid@aiub.edu.

How to cite this paper: Rakin S. Aftab, Md. Kais K. Emon, Sanjana F. Anny, Durjoy Sarker, Md. Mazid-Ul-Haque, "Security Analysis in Online Transaction Systems: A Proposed Framework", International Journal of Information Engineering and Electronic Business(IJIEEB), Vol.16, No.2, pp. 22-38, 2024. DOI:10.5815/ijieeb.2024.02.03