Open Access Library Journal
2024, Volume 11, e12326
ISSN Online: 2333-9721
ISSN Print: 2333-9705

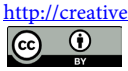
The Legitimacy of Online Banking Transactions as a Value-Added Tool in Rwanda's Banking System

Evariste Nkubito[1], Jean Baptiste Mbanzabugabo[2]

[1]Graduate School, University of Kigali, Kigali, Rwanda
[2]Department of Architecture and Information Technology, University of Kigali, Kigali, Rwanda
Email: nkubax@gmail.com

How to cite this paper: Nkubito, E. and Mbanzabugabo, J.B. (2024) The Legitimacy of Online Banking Transactions as a Value-Added Tool in Rwanda's Banking System. *Open Access Library Journal*, **11**: e12326.
https://doi.org/10.4236/oalib.1112326

Received: September 18, 2024
Accepted: December 22, 2024
Published: December 25, 2024



Abstract

This paper sought to study online banking services' security constraints and transaction legitimacy checks using "two factors authentication or multi factor authentication". The Government of Rwanda introduced a cashless program that had a target of promoting electronic payment and the program was more enforced during COVID-19 insurgency when the general public was strictly encouraged to use electronic payment systems to curb the badly disseminating disease and enforce other existing benefits of online payment schemes. When comes to the issue of security though, for the last five years, the Rwanda Investigation Bureau statistics demonstrated a hiking number of financial crimes varied from 4276 cases (2019) to 11,117 (2023), which involved cyber fraud cases that mainly dominated with two crimes of "unauthorized access to computer or computer system data", and "access to computer or computer systems data with intent to commit a crime varied from 302 to 445cases (fiscal year 2021/2022-2023/2024) and 84 to 200 cases respectively. In this research, security concept on e-banking services were examined using both quantitative as well as qualitative approaches in collecting data and analysis using SPSS. Findings show that the Information Technology knowledge-less on the public is key cause of the increased cyber frauds against online banking. The combination of that low level of knowledge in technology and weak security setups in e-banking systems were the main cause of money defrauding which attracted a recommendation of reminding service providers to periodically remind their customers to deploy a "Two-Factor Verification" scheme into every single online transaction, and regularly train them on any new emerged technologies. This study concludes by suggesting a security model that can be followed by beneficiaries of the integrated banking systems to fight against cyber frauds and timely report them to the respective law enforcement agencies.

Subject Areas

Technology

Keywords

Two-Factors, Verification, E-Banking, Services, Security, Authentication

1. Introduction

In recent years, e-banking services have attracted a variety of stakeholders, primarily due to their quick service delivery, transparent cash exchange processes, and contributions to economic growth through job creation. As of January 2024, Rwanda had 12,940,045 active mobile-cellular telephone subscriptions, reflecting a 1.4% increase from December 2023's 12,763,076 subscriptions. This growth raised the mobile penetration rate to 95.3% of the population.

Bank of Kigali (BK), as a leading financial institution in Rwanda and a front-runner in the digitalization of banking services, was selected as the ideal foundation for this study. Its network of agents across Kigali city, along with its staff, provided a solid starting point for researching the security of e-banking services. However, as the landscape becomes increasingly competitive, concerns regarding security have intensified, particularly given the rapid advancements in technology and related knowledge people have regarding the new emerging technology.

As of 2024, Rwanda has achieved a 96% financial inclusion rate, with 92% of adults formally included in financial services. This significant progress is largely driven by the widespread adoption of digital financial services, particularly mobile money. In 2020, approximately 66% of the adult population (around 7.1 million individuals) were digitally included, with 91% of them using mobile money services and 9% accessing electronic banking services [1] [2]. This highlights the need for additional security measures to combat potential fraud and prevent unauthorized access to systems.

According to Nixon and Dixon [3] banks are facing heightened competition not just from traditional financial institutions but also from a wide range of businesses, which has significantly intensified competition within the global financial services sector. A notable challenge in this environment is account takeover, which poses a significant risk to online user data security. Many banking accounts are often protected by easily memorable or weak passwords, underscoring the necessity for service providers to effectively distinguish legitimate users from account hijackers [4].

Research by Gaw and Felten [5]. has shown that many users of online banking frequently rely on memorable passwords or reuse a single password across multiple platforms. Most studies on user authentication have concentrated on internet services, where numerous financial institutions are directing their operations, despite the low level of end-user awareness regarding security practices. This has

revealed a significant security gap concerning illegitimate transactions between system operators and customers, particularly in terms of privacy [6] [7]. This article is structured to include the following sections: an introduction to the research, literature review, discussion of the conceptual and theoretical framework, a description of the research methodology, data analysis, discussion of findings, an overview of research limitations, conclusion, and recommendations. Additionally, it proposes a security acceptance model that outlines preventive measures to combat e-banking fraud.

2. Literature Review

2.1. Two-Factors Verification on E-Banking Services

In the European Economic Area (EEA), strong customer authentication is essential to ensure that electronic payments are conducted with multi-factor authentication, thereby enhancing the security of these transactions [8] However, vulnerabilities in online banking systems, such as the unavailability of mobile devices, SIM card cloning, and swapping, can grant attackers access to mobile phone connections. These vulnerabilities are further exploited when mobile operators issue duplicate SIM cards to criminals.

Modern smartphones are particularly susceptible to security breaches because they often have active email applications and can receive SMS messages. If a phone is stolen and lacks adequate protection such as two-factor authentication involving both a password and biometric verification, fraudsters can easily gain access to all accounts linked to that number, facilitating identity theft and password acquisition.

Typically, according to O'Brien, and the guidelines of the National Institute of Standards and Technology [9] [10] without physical access to a device, fraudsters cannot easily infiltrate an institution's networks or access sensitive financial information, which prevents them from executing unauthorized transactions. Nonetheless, due to factors like cost, complexity, reliability, and privacy concerns, it is crucial to implement additional security measures in banking services to ensure both security and efficiency.

2.2. Legitimacy of Online Transactions from One End Point to Another

In a mobile environment, attacks can also originate internally, where firewalls offer limited protection. In research of Aljawarneh Shadi [11] highlighted that, due to information security concerns, many small and medium-sized enterprises (SMEs) in Arab countries prefer traditional methods of interaction over transitioning to online operations. This hesitation arises from inadequate technological preparedness, resulting in few secure online transaction platforms, limited information security measures, and scarce credit options. A major security risk noted is the lack of robust data validation; improperly validated data introduces critical vulnerabilities that threaten the security of online banking and e-banking services overall.

2.3. Global History of Multi-Factors Online Banking System Verification

The history of multi-factor authentication (MFA) in online banking reflects the growing need for enhanced security in response to evolving cyber threats. Initially, banks relied solely on password-based systems, but as online banking expanded, especially in the late 1990s and early 2000s, so did the need for stronger authentication methods.

European banks were early adopters, implementing SMS-based codes, while regulatory measures like Europe's Payment Services Directive (PSD2) further mandated strong customer authentication [12] In North America, the Federal Financial Institutions Examination Council (FFIEC) guidelines [13] prompted major banks to adopt MFA, driven by rising concerns over data breaches. Similarly, Asia-Pacific financial institutions embraced mobile and biometric-based MFA, with China and India leveraging smartphone and biometric systems like Aadhar to secure banking access for millions.

In the publication of Alice Kalonzo Zulu [14] highlighted that banking agencies and Mobile banking are the futures of banks. To enhance banking agency efficiency, banks have to heavily invest in technology and systems' security at large.

According to Schmid Dannis [15], 95 percent of the Norwegian population access online banking sites, this has made Norway a country which has a big rate of internet fraud in Europe, before Iceland and Denmark. Banking through the internet becomes most popular in Europe, enabling bank users to exchange money or transact on their personal websites. Over time, the confidence of online transactions increased. Meanwhile, in some European countries such as Germany and Austria hard cashing is experiencing a significant reduction as long as the bank users strongly encourage using cashless transactions. As published by Reserve Bank of India, online payment systems are regulated by the Payment and Settlement Systems Act, 2007 (PSS Act) [16]. According to the bank no individual person other than Reserve Bank can start a payment system in India without granted permission by that bank. It is the only Reserve Bank that has autonomy of giving that authorization and since then has authorized payment system operators of pre-paid payment instruments, card schemes, cross-border in-bound money transfers, Automated Teller Machine (ATM) networks and centralized clearing arrangements.

Emerging markets in Africa also innovated with mobile-based MFA solutions, such as PIN codes and SMS verification, while institutions began to integrate biometric authentication for broader accessibility. Today, MFA in banking has evolved to include sophisticated methods like adaptive authentication, which customizes security measures based on user behavior and risk. The future of MFA is likely to see further advances with the integration of blockchain and AI-driven adaptive systems.

In the East African Community, the member States' central banks are equipped to address risks present within payment systems in the region. Mobile money presents a new set of regulatory challenges involving players that traditionally have not fallen within the purview of central banks. Some of the issues that are of concern

include whether Mobile Network Operators (MNOs), should be directly licensed to issue mobile money; and how the agents, who are critical for mobile money transactions should be regulated [17]. All central banks in the EAC have had to work out how to regulate mobile money in their jurisdictions by learning how the Central Bank of Kenya has handled M-PESA in that country, said Joseph Nyaga. Practically all MNOs with the approval of their respective central banks, have copied the same thresholds/limits in terms of what users can send or receive due to harmonized security regarding mobile money transactions. M-PESA's transaction fee structure has greatly influenced those of other mobile money platforms across the EAC.

2.4. Multi-Factors Security Layers Pursuance in Rwanda

Toroitich, a chairperson of Rwanda Bankers Association [14] highlighted how important technology-based innovations are very paramount in the new era of businesses, including banks, adding that technology enables service providers to distinguish themselves in the digital space with unique product offerings. Technology has now become a familiar tool to most individuals, to an extent that it influences their lifestyle and must be emerged into banking operations.

Financial analyst Jean Damour Nishimwe in his message [14], said that agents have the capacity to offer many bank services, such as registering customers, taking deposits, dispensing withdrawals, fund transfers, and processing payments like utility bills. Vouches for agency banking, saying it is a good example of a "concrete strategy that has the potential to enable customers to carry out transactions in them communities the same way as they would have at their local bank branch". However, this is not enough or granted as long as there are no security measures to protect customers' data stored in bank systems or through transaction vacuums.

According to Lawson Naibo [18], the Bank of Kigali (BK) had about 60,000 customers utilizing the mobile banking platform, with close to a million transactions registered on a daily basis. At least five main commercial banks, Bank of Kigali (BK), Kenya Commercial Bank Rwanda (KCB), Ecobank Rwanda, Commercial Bank of Rwanda and Banque Populaire, are now offering mobile banking. Approximately Banque Populaire registered about 140,000 users by the time. This shows how globally the mobile banking operations increase especially in Rwanda where the government installed network infrastructures all over the country and strongly advised financial institutions to use electronic payment schemes and promote cashless in Rwandan society. Mobile penetration in Rwanda was estimated at 41.8 percent as of December 2011 [18] This put it at second lowest in the East African Community after Burundi.

Again, Timothy and Kate Lauer in their report [19] highlighted that there are three key components of digital financial services: a digital transactional platform, retail agents, and the use by customers of a device most commonly a mobile phone to transact via the platform.

3. Conceptual and Theoretical Framework

3.1. Conceptual Framework

Duo Factor Authentication, is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, like a piece of information only they should know or have immediately to hand such as a token.

Using a username and password combined with a piece of information that only the user knows makes it harder for fraudsters to unauthorizedly gain access to the bankers' accounts.

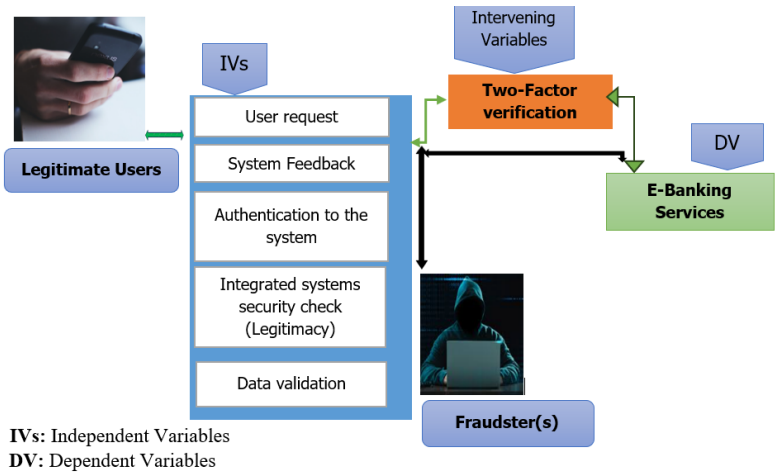


Figure 1. Conceptual framework illustrating the weak security breach deviation (designed by author).

As shown in the above Figure 1, the diagram illustrates the concept model of a two-factor verification breach process in e-banking services.

It incorporates various steps from legitimate user actions to cyber frauds masquerading interferences when the user's account is not protected enough.

Independent Variables (IVs): These variables represent the actions initiated by legitimate users while executing the normal transaction processes.

User Request: Legitimate users initiate requests for e-banking services.

Data Validation: Additional verification of the data provided during the transaction to ensure consistency and accuracy.

Intervening Variable: The "Two Factors Verification" process acts as an intervening variable between user actions (IVs) and the final e-banking services. This crucial step requires the user to pass an additional layer of security typically, something they know (like a password) and something they possess (like a mobile OTP or biometric data). Whenever use the skip this option, the account remains vulnerable for fraud attacks.

Dependent Variable (DV): The final outcome or dependent variable is **E-Banking Services**. Whenever the fraudsters manage to access partially protected accounts, they immediately get a full access to the financial data.

3.2. Theoretical Framework

The use of one-time passwords as a second step to logging in seems to be getting more popular recently. According to Dhanashri [20] There are two main approaches to OTPs, the first being delivery of the OTP over SMS setups, and the other changes every time you use it to log in or on a predefined time schedule based on a predefined algorithm. For the first type use should possess a physical device in order to receive SMS and the device must have full connectivity. The second type which is considered to be more secure is to use devices such as RSA Secure ID tokens. The usage of the second type helps the user to manually generate the code using the handset instead of using a phone message generator which should be easily hijacked. Most mobile operating systems like Apple, Android, Windows and blackberry mobile users are compatible with OTPs. Again, OTPs can be generated through an application without internet connection. Activation of this application simply involves two steps: Downloading Mobile OTP application "CA MOBILE OTP" on handsets.

Another challenge of SMS delivery is the possible delay of the message based on the location of the sender or receiver and this area connectivity results in message delivery delay. The message delay and weak connectivity also should be caused by handset type cross-borders coverage area which may cause weak signals to the both ends of transmitters. In their research, Dhanashri and Patil [20] shaded light on many other messages for causes like mobile phones with weak batteries, or unknowingly phone switched off. The difficulties also should be experienced through devices with adjustable antennas which should result in failure or delay of message transmission.

According to Nexmo [21] A text sender and receiver using different networks may have a greater chance of experiencing texting delays than those using the same network, because of communication between networks or the carrier prioritizing their own traffic. With the above experiences, banks and other financial institutions should give priority to the advanced security of their online businesses and the security of their customers' information.

4. Methods

4.1. Data Collection

In this study, both quantitative and qualitative data collection methods were utilized. Quantitative data was collected in the form of numeric and quantifiable information, representative samples, and findings, which were presented and analyzed statistically to assess the security level of online banking services. The qualitative approach, on the other hand, involved descriptive and categorization techniques to interpret responses, analyzed narratively and deductively. Secondary data was gathered from existing literature on e-banking security and related topics, forming the basis of the literature review. Additionally, in-depth interviews were conducted with a small number of participants to gain insight into their perspectives on online banking security. Comprehensive questionnaires, consisting

of structured questions, were administered to obtain specific viewpoints from knowledgeable respondents using bipolar Likert scale ranging from strongly disagree, disagree, agree, strongly agree. A total of 60 questionnaires were distributed, and all were completed and returned, resulting in a 100% response rate.

4.2. Sampling and Sample Size

The study employed a random sampling approach, as recommended by Kothari [22], ensuring that each individual in the population had an equal chance of selection. The sample was drawn from a diverse group of Bank of Kigali (BK) users, including IT staff, tellers, and the bank agents within Kigali City, to achieve a representative sample. A total of 60 respondents were selected, deemed sufficient to represent the security landscape within e-banking services especially in BK, and indicative of similar institutions in the financial sector in general.

4.3. Validity and Reliability of Instruments

The validity of the research instruments was ensured by having at least two experts assess and judge the relevance of each item on the questionnaire against the study's objectives. This approach was chosen to guarantee the adequacy and comprehensiveness of the content, ensuring that the questions effectively address the research goals. Reliability was assessed by measuring the consistency and stability of the instrument, with improvements made until achieving a Kaiser-Meyer-Olkin (KMO) score greater than 0.5. The data was analyzed using IBM SPSS Statistics, a versatile statistical tool popular in social science research, which offers capabilities for data transformation, descriptive analysis, and prediction, as well as data visualization through graphical tools.

5. Data Analysis

5.1. Statistical Analysis

The respondents' education levels are presented in Table 1. The majority of participants held a graduate degree or higher, representing 45.0% of the valid sample, followed by those with a secondary education at 41.7%. The least represented groups were those with primary (11.7%) and diploma (1.7%) education levels. This distribution suggests that individuals with higher education are more likely to seek employment and utilize online banking services, reflecting the broader employment trends within Rwanda. The low number of diploma holders in this sample may indicate that many diploma graduates proceed to higher education immediately, contributing to the low representation among online banking users.

Table 1. Respondents' Level of Education.

Academic Levels		Frequency	%	Valid %	Cumulative %
Valid	Primary	7	11.3	11.7	11.7
	Secondary	25	40.3	41.7	53.3
	Diploma	1	1.6	1.7	55.0

Continued

	Graduate and above	27	43.5	45.0	100.0
	Total	60	96.8	100.0	
Missing	System	2	3.2		
Total		62	100.0		

Source: Primary Data: Descriptive level of respondents' education.

As shown in Table 2, most respondents had 3 - 5 years of experience in online banking during the study, accounting for 55.0% of the valid sample, followed by those with 1 - 2 years of experience at 30.0%. Only 15.0% have been using online banking for 6 - 10 years. This distribution may indicate a recent increase in employment and online banking adoption among new users in the past few years. Those with longer experience in online banking are often more familiar with the systems, suggesting that these users may also engage in business-related online transactions.

Table 2. Respondents Experience in the e-banking services.

Serving Experience (years)		Frequency	%	Valid %	Cumulative %
Valid	1 - 2 yrs	18	29.0	30.0	30.0
	3 - 5 yrs	33	53.2	55.0	85.0
	6 - 10 yrs	9	14.5	15.0	100.0
	Total	60	96.8	100.0	
Missing	System	2	3.2		
Total		62	100.0		

Source: Primary Data: Respondents serving experience.

Below is Table 3, illustrates respondents' views on the role of IT knowledge in preventing online banking fraud. A significant majority (55% agree and 15% strongly agree) collectively, believe that a lack of public IT knowledge is a primary cause of online banking fraud. This sentiment underscores the need for increased public awareness and education on cybersecurity practices to enhance user safety in online banking.

Table 3. Public IT knowledge-less as a key contributor to e-banking Fraud.

		Frequency	%	Valid %	Cumulative %
Valid	Strongly Disagree	7	11.3	11.7	11.7
	Disagree	11	17.7	18.3	30.0
	Neutral	0	0.0	0.0	30.0
	Agree	33	53.2	55.0	85.0
	Strongly Agree	9	14.5	15.0	100.0
	Total	60	96.8	100.0	
Missing	System	2	3.2		
Total		62	100.0		

Source: Primary data: Respondent perceptions regarding less knowledge in Information Technology as contributor to the fraud.

According to the below Table 4, a substantial portion (61.7%) of respondents rely solely on Password or PIN for account security, while 38.3% utilize a combination of Password and One-Time Password (OTP) for enhanced protection. Users with IT knowledge are more likely to be aware of and use layered security measures like OTPs. This highlights a knowledge gap in cybersecurity practices among general users, who may rely on less secure authentication methods due to limited familiarity with advanced security measures provided by their service providers.

Table 4. Types of accounts authentication & verification.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Password/PIN	37	59.7	61.7	61.7
	Password & OTP	23	37.1	38.3	100.0
	Total	60	96.8	100.0	
Missing	System	2	3.2		
Total		62	100.0		

Source: Primary data: respondents' level of security onto online banking operations.

Table 5. Possible solution to mitigate/prevent e-banking frauds.

	Variables	Frequency	Percent	Valid Percent	Cumulative Percent
Valid	general Awareness campaigns	4	6.5	6.7	6.7
	Banks to educate their customers about new Apps	22	35.5	36.7	43.3
	Use of other specific device for mobile banking	11	17.7	18.3	61.7
	1 & 2	7	11.3	11.7	73.3
	Public awareness & education about new apps & specific device	16	25.8	26.7	100.0
	Total	60	96.8	100.0	
Missing	System	2	3.2		
Total		62	100.0		

Source: Primary data: Possible solution to mitigate/prevent e-banking frauds.

Among possible solutions from respondents' perceptions, banks should persistently educate their customers about new emerging technology and how to safely use it. Using two factors verification can contribute much to deter e-banking based frauds.

Among possible solutions, respondents gave out their perceptions in the following rates: 36.7% of respondents suggest that financial institutions should persistently educate their customers about new emerged technologies and related security measures. The other perceptions from 27.7% suggest that collaboration of related organizations to curry out general public awareness campaigns should be of productive when combined with individual banks education to their customers.

17.7% of all respondents suggest that using a specific mobile device should be the best solution.

The study reveals that experience regarding online banking matters a lot where those who served long had experienced this kind of attack which definitely leads to the concept of IT knowledge-less as a key cause of the increased cyber frauds against online banking. For durable solutions in terms of ICT infrastructures, deployment of key token devices is considered as a very appropriate tool to curb down illegitimate transaction since it combines more than two security concept such as username, login PIN, confirmation PIN and lastly one-time password (OTP) generated by the device.

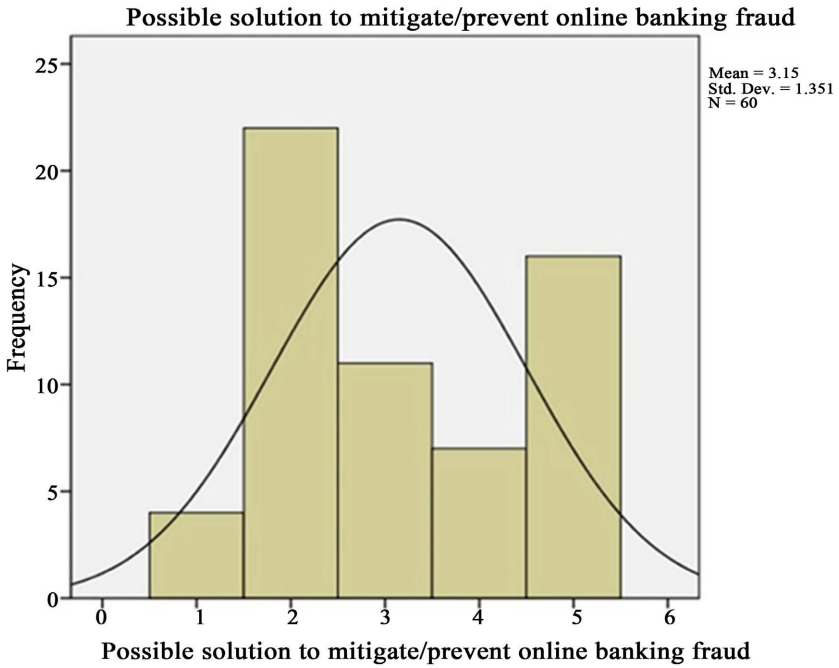


Figure 2. Variables frequencies (corresponding to **Table 5**).

The above **Figure 2**, in correspondence with **Table 5**, highlights the significance of ongoing education and awareness for clients regarding new banking apps, emphasizing the effectiveness of teaching clients how to use security devices for generating self-authenticated one-time passwords.

5.2. Measure of Sampling Adequacy

A Kaiser-Meyer-Olkin (KMO) test is used in research to examine sampling adequacy of data and for Factor Analysis [23]. In research, Factor Analysis is used to determine if variables used to measure a particular study give the intended results. The KMO measurements help to ensure that the data we have are suitable with a Factor Analysis and used to determine if the settled dataset result is what we have intended to measure. 0 and 1 range measurements are used to measure statistical data. Interpreting the statistic is relatively straightforward; the closer to 1, the better. The adequacy of the study is considered to be reasonable since it is as long as

KMO > 0.5 study adequacy is considered as reasonable. In our study, the KMO is equal to 0.538 and the Chi-Square is equal to 118.497 (See Table 6 and Table 7).

Table 6. Kaiser-Meyer-Olkin (KMO) and Bartlett's Test.

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.538
Bartlett's Test of Sphericity	Approx. Chi-Square	118.497
	df	36
	Sig.	0.000

Table 7. Kaiser-Meyer-Olkin (KMO) value for each variable.

Variables	Initial	Extraction
Online banking services used by respondents	1.000	0.783
Are there any related cyber frauds ever interfered with?	1.000	0.885
On any registered fraud attempts, have you received any possible intervention from your Bank?	1.000	0.838
Public IT knowledge-less should be the key cause of Online Banking Fraud	1.000	0.687
Are Banking applications fully secure?	1.000	0.643
Use of any other specific online banking device should be helpfully to mitigate the fraud	1.000	0.371
Possible solution to mitigate/prevent online banking fraud	1.000	0.868
Types of accounts authentication & verification	1.000	0.625
Using two factors verification as a solution	1.000	0.596

Extraction Method: Principal Component Analysis.

6. Discussion on the Findings

The study reveals that respondents use various account authentication methods, including passwords, OTPs, and other security measures. Although 86.1% confirmed the effectiveness of two-factor verification for securing accounts, its adoption remains low. About 33.9% of respondents had encountered cyber fraud attempts, with 25.8% receiving support from their banks to recover accounts and enhance security measures. The findings suggest that experience with online banking impacts vulnerability, as those with longer service tend to experience more fraud attempts.

Additionally, 54% of respondents attributed cyber fraud to limited ICT knowledge, especially among bank agents, with 35.5% recommending that banks regularly educate customers on IT security practices.

Concerns about the security of online banking applications were voiced by 40.3% of respondents, who highlighted exploitable gaps that both insiders and outsiders can manipulate. To address these issues, many respondents suggested that banks, in partnership with the National Bank, should increase public awareness of new security measures to protect customers' financial data and preserve the banks' reputation. On fraud prevention, 77.5% advocated for a dedicated device solely for Internet banking, as SIM cards are a common attack vector without

adequate protective measures from telecoms and banks. Additionally, 60.5% emphasized the importance of public education and awareness to further mitigate these risks.

7. Research Limitations

During the study period, the researcher faced financial constraints and limited timeframe which restricted the number of respondents that could be involved. Balancing this study with other daily work commitments further reduced the time available for research activities. Despite these challenges, the researcher maximized the short time available to gather respondents, collect relevant data, and perform a comprehensive analysis. Additionally, the lack of sufficient resources posed a challenge, but the researcher effectively worked within the available resources to overcome this limitation. There is a need for future research to extend the study to the big number of respondents with a strict emphasis on the matter under study.

8. Conclusions and Recommendation

With the objective of conducting a thorough study on the increase of fraudulent banking transactions, this study was carried out to assess and recommend the best security suit against the legitimacy of online banking transactions.

A significant number of users use only Password/PIN as a common security measure; a few of them have knowledge about other additional security layers such as OTP and other setups. It is apparent that this routine of using one way of security puts on security vulnerability many accounts and when experienced fraudsters bypass that one single gate, they immediately grab off the victim's money. However, if two-factor verification security layers were effectively introduced into banks systems and services, there would be very positive and beneficial online transactions. The study recommends that e-banking service providers should thoroughly identify, assess and prevent the specific risks associated with global use of provision settings and strongly request their customers to deploy "two-factor verification" as an additional security layer for their personal financial data.

Where possible, the institutions should invest in secure elements and other specific mobile devices such as token devices that can be linked with the user's account and personally used to perform a very single transaction securely.

Security Acceptance Model for prevention and reporting e-banking fraud incidents.

Figure 3 demonstrates a security acceptance model for two-factor verification in e-banking services. It is possible and recommended to adopt the "**Time-based One-Time Password (TOTP)**" model along with "**Biometric authentications**". This combination enhances security while ensuring that incidents can be reported promptly to law enforcement. In addition, two layers of verification significantly reduce unauthorized access. Automated systems can quickly notify not only the victim but also law enforcement to minimize potential losses.

Lastly, this model can enhance streamlines of incident reporting and fair incident management in e-banking services, hence providing robust security measures helps build customer confidence in e-banking services.

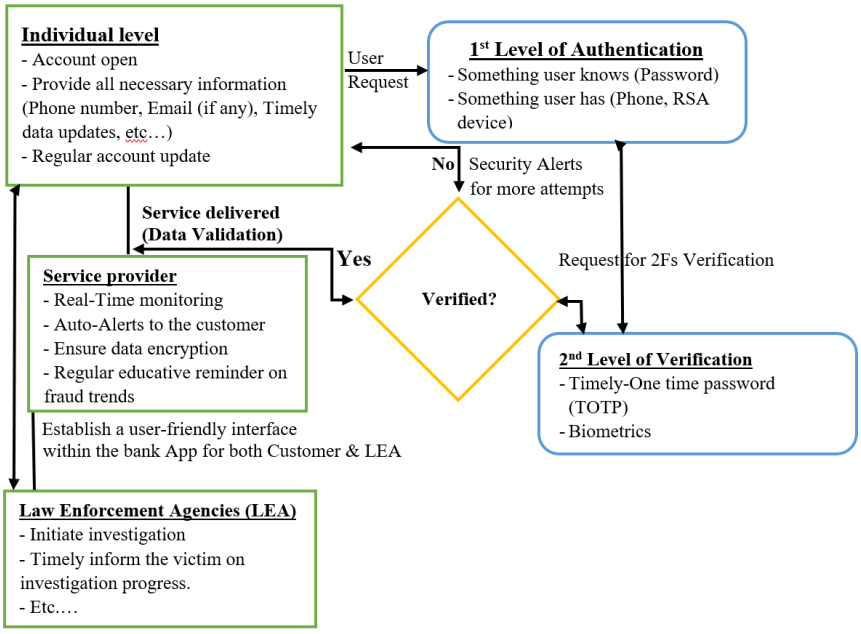


Figure 3. Acceptance model design from the research viewpoints.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] National Institute of Statistics Rwanda (2024) Rwanda FinScope. National Institute of Statistics Rwanda, Kigali.

[2] Access to Finance Rwanda (AFR) (2020) The State of Digital Financial Inclusion in Rwanda. Access to Finance Rwanda (AFR), Kigali.

[3] Mohammad, U.J., Mohani, A. and Mohammad, R.M. (2015) Trends and Challenges of E-Banking Services. *International Journal of Science and Research*, **5**.

[4] Alexei, C., Dirk Balfanz, B., Marius, S., Juan, L. and Sampath, S. (2017) Security Keys: Practical Cryptographic Second Factors for the Modern Web. *Financial Cryptography and Data Security*, Christ Church, 22-26 February 2016, 422-440. https://doi.org/10.1007/978-3-662-54970-4_25

[5] Gaw, S. and Edward, W.F. (2006) Password Management Strategies for Online Accounts. *Proceedings of the Second Symposium on Usable Privacy and Security*, Pittsburgh, 12-14 July 2006, 44-55. https://doi.org/10.1145/1143120.1143127

[6] Vishal, G., Pandey, U. and Batra, S. (2012) Mobile Banking in India: Practices, Challenges and Security Issues. *International Journal of Advanced Trends in Computer Science and Engineering*, **1**, 56-66.

[7] Alkhowaiter, W.A. (2020) Digital Payment and Banking Adoption Research in Gulf Countries: A Systematic Literature Review. *International Journal of Information Management*, **53**, 102102. https://doi.org/10.1016/j.ijinfomgt.2020.102102

[8] Adyen (2019) Strong Customer Authentication Guidelines. Understanding Strong Customer Authentication & PSD2, 14 September 2019. https://www.adyen.com/knowledge-hub/psd2-understanding-strong-customer-authentication

[9] Wazid, M., Zeadally, S. and Das, A.K. (2019) Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions. *IEEE Consumer Electronics Magazine*, **8**, 56-60. https://doi.org/10.1109/mce.2018.2881291

[10] Institute of National Standards and Technology (NIST) (2022) Special Publication 800-63B: Digital Identity Guidelines.

[11] Aljawarneh, S. (2017) Online Banking Security Measures and Data Protection. IGI Global. https://doi.org/10.4018/978-1-5225-0864-9

[12] EU Commission (2019) Payment Services Directives. Payment Services Directive (PSD2)-Directive (EU) 2015/2366.

[13] Federal Financial Institutions Examination Council (FFIEC) (2001) Authentication in an Internet Banking Environment. FFIEC.

[14] Zulu, K. (2017) Why Banks Are Rushing to Embrace Agency and Mobile Banking Services. https://www.newtimes.co.rw/article/147081/News/why-banks-are-rushing-to-embrace-agency-and-mobile-banking-services

[15] Dannis, S. (2020) Online Banking Penetration in European Markets. Statista Research Department, Norwegian.

[16] Reserve Bank of India (2020) Payment and Settlement Systems Act, 2007 (PSS Act).

[17] Nyaga, K.J. (2014) Mobile Banking Services in the East African Community (EAC): Challenges to the Existing Legislative and Regulatory Frameworks. *Journal of Information Policy*, **4**, 270-295. https://doi.org/10.5325/jinfopoli.4.2014.0270

[18] Lawson, N. (2012) Mobile Banking Takes off in Rwanda. https://pctechmag.com/2012/05/mobile-banking-kicks-off-in-rwanda/#google_vignette

[19] Timothy, L. and Kate, L. (2015) What Digital Financial Inclusion and Why Does It Matter. Consultative Group to Assist the Poor (CGAP), Washington DC.

[20] Dhanashri, G. and Shweta, P. (2019) OTP Over SMS: Time Delay Issues and Causes. *International Journal of Innovative Research in Computer and Communication Engineering*, **7**, 1-7.

[21] Nexmo Support (2022) What Causes a Delay in Delivering SMS Messages? https://api.support.vonage.com/hc/en-us/articles/204014893-What-causes-a-delay-in-delivering-SMS-messages

[22] Kothari, C. (2004) Research Methodology: Methods and Techniques. New Age International (P) Ltd.

[23] Sean, P. and An Gie, Y. (2013) A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis. *Tutorials in Quantitative Methods for Psychology*, **9**, 79-94. https://doi.org/10.20982/tqmp.09.2.p079