Received: 04 Apr 2025 | Revised: 28 May 2025 | Accepted: 12 Jun 2025 | Published: 30 Jun 2025
Volume 3(1) Pages 103-127 DOI: https://doi.org/ 10.56279/jicts.v3i1.378

JICTS
Journal of ICT Systems

Evaluation of the Effectiveness and Awareness of Mobile Money Services among Users in Tanzania: A Case of Iris Biometric Authentication Method

Mustafa Habibu Mohsini[a, 1], Florence Upendo Rashidi[b], Bakari Mega[c]

[a]*Department of Computer Science and Engineering, College of Informatics and Virtual Education, The University of Dodoma, Tanzania*
[b]*Department of Electronics and Telecommunication Engineering, College of Informatics and Virtual Education, The University of Dodoma, Tanzania*
[c]*Ministry of Culture, Arts and Sports, Tanzania.*

[1]Corresponding author
Email: mustafa.mohsin@udom.ac.tz

Abstract

This study evaluates user perceptions of a framework proposed by Rashidi et al. [11] that uniquely combines iris biometric authentication (IRBAM) with two-factor authentication (2FA), incorporating liveness detection to enhance security in mobile money services (MMSs) in Tanzania. The IRBAM-2FA combination is novel for Tanzania's MMS, leveraging unique iris patterns and liveness detection to enhance security over prevalent PIN-based systems vulnerable to fraud. Through a survey-based evaluation of a demo application, involving 258 respondents (204 customers, 54 agents) in Dodoma, we assessed the framework's effectiveness in preventing unauthorized access, its convenience, and user acceptance. Findings show that 79.41% of customers are aged 18–35, suggesting a tech-savvy audience likely to embrace IRBAM-2FA, as younger individuals are typically more open to innovative technologies. Additionally, 46.1% of customers and 51.9% of agents strongly agreed that the framework enhances security, while 85.5% of customers and 71.6% of agents expressed willingness to adopt it. Low IRBAM awareness (65.2% of customers, 79.9% of agents), usability issues (20% of agents' disagreement), cost (30%), and health risks (40%), pose barriers, with future work needed on feature phone support and rural testing for inclusivity. These insights underscore the potential of IRBAM to foster trust in MMS.

Keywords

Iris Biometric Authentication Method
Mobile Money Services
Security Challenges
Two- factor Authentication
User Acceptance

1. Introduction

The proliferation of mobile money services (MMS) has significantly transformed financial transactions, especially in regions like Tanzania, where the user base has expanded dramatically in recent years. Mobile money subscriptions increased from 47.3 million in June 2023 to 51.4 million in

September 2023, and from 53 million in March 2024 to 56 million in June 2024, reflecting a 5% growth rate [1]. Transaction volumes have also surged, rising from 3 billion in 2019 to 5.3 billion in 2024 [2]. This rapid expansion underscores the critical role of MMS in Tanzania's economy and highlights security vulnerabilities, particularly in PIN-based authentication systems prone to guessing, forging, or brute-force attacks [3].

Biometric authentication offers a robust solution to these challenges by leveraging unique physiological traits for secure access. Among biometric methods, iris recognition stands out due to its high accuracy and resistance to unauthorized access. Scholars demonstrate that iris patterns are highly distinctive, even among identical twins, with over 81% accuracy in distinguishing twin irises [4, 5]. This uniqueness makes iris biometric authentication (IRBAM) ideal for MMS, where preventing unauthorized access is paramount. Compared with fingerprint authentication, which is vulnerable in unconscious states, or facial recognition, which may falter with lighting variations, IRBAM offers superior reliability, though it requires specific hardware (e.g., high-resolution cameras) [6].

Several studies have explored biometric frameworks for financial services. Lovisotto et al [7]. proposed a five-factor framework (security, usability, inclusivity, robustness, privacy) for evaluating mobile biometrics, emphasizing balanced solutions for user needs and technical constraints. Alrawili et al. [6] provide a survey of biometric user authentication, highlighting the strengths and limitations of methods like fingerprint, iris, and facial recognition. They note that while fingerprint authentication is widely adopted due to its integration in smartphones, it is vulnerable to unauthorized access in unconscious states. Conversely, iris authentication offers high accuracy and uniqueness but faces challenges in user awareness and device requirements. These limitations underscore the need for studies that evaluate the practical effectiveness and user acceptance of IRBAM in the context of MMS in Tanzania.

Furthermore, Mtaho [8] evaluated PIN and fingerprint-based two-factor authentication (2FA) for MMS in Tanzania, reporting enhanced security but lower acceptance due to usability issues. Serhani et al. [9] outlined a framework for secure mobile applications, focusing on standardized protocols, while Solazzo [10] highlighted increasing smartphone adoption in Tanzania, supporting biometric integration. However, these studies do not address IRBAM in MMS or explore user perceptions in Tanzania's context, where cultural and infrastructural factors influence adoption.

Rashidi et al. [11] addressed this gap by proposing the MMS security framework that combines IRBAM with 2FA, incorporating liveness detection to prevent spoofing. They developed a mobile money application with interfaces for Mobile Network Operators (MNOs), Mobile Money Agents (MMAs), and Mobile Money Customers (MMCs), connected via secure web services. While their framework is theoretically robust, it lacks empirical user testing, relying on case studies and technical validation. This knowledge gap leaves critical questions about the framework's practical effectiveness, user convenience, and acceptance, particularly in Tanzania's rapidly growing MMS ecosystem.

This study fills these gaps by conducting a survey-based evaluation of the application developed by Rashidi et al. [11], involving 258 respondents (204 MMCs, 54 MMAs) in Dodoma, Tanzania. It assesses the framework's ability to eliminate unauthorized access, convenience, and user acceptance, providing the first empirical insights into its performance. The findings

highlight user perceptions, demographic influences, and adoption barriers, such as low IRBAM awareness and smartphone dependency, informing strategies for MNOs, policymakers, and users. This study enhances trust and security in Tanzania's MMS ecosystem by addressing these issues.

2. Summary of the Mobile Money Application Based on the Proposed Framework

This study evaluates the mobile money application developed by Rashidi et al. [11]. Unlike existing MMS apps in Tanzania, which primarily use PIN-based authentication, which is vulnerable to guessing or forgery, the framework by Rashidi et al. [11] introduces IRBAM with 2FA and liveness detection, offering enhanced security and resistance to spoofing. The framework, shown in Figure 1, integrates a user-side application (with GUI, APIs, and secure layer interface) and an MNO server (with security system, web services, business logic, and database). Three interfaces were developed for MNOs, MMAs, and MMCs, connected via web services for secure authentication and transactions. This evaluation assesses the framework's effectiveness through user security, convenience, and acceptance feedback.

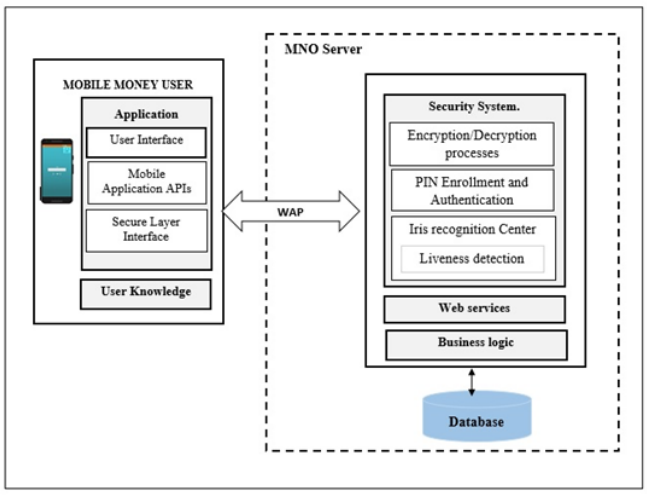

Figure 1. Framework for improving MMS access using 2FA with IRBAM (Source: Rashidi et al. [11]).

Below is a concise overview of the framework's key components:

2.1 Mobile money user (MMU) side

- The Graphical User Interface (GUI) provides intuitive menus and navigation for transactions.
- The application APIs enable camera access for iris capture and interoperability.
- Secure Layer Interface for managing PIN and biometric data with SSL encryption.

2.2 MNO side

- Security System includes PIN enrollment, iris recognition, and liveness detection.
- Web Services facilitate communication between the app and the database.
- Business Logic for handling transaction processing and account management.
- Database for storing user credentials and transaction data securely.

For detailed specifications of the framework, refer to Rashidi et al. [11]. This study assesses the application's effectiveness through user feedback.

3. Methodology

This section provides a detailed explanation of the methodology used in this study, from selecting the study location to testing and evaluating the mobile money application. Figure 2 shows the methodology workflow implemented in this study.

3.1 Study area

This study was conducted in Dodoma Urban in Tanzania, the capital city of Tanzania, where many government services have been relocated during the 2016/2017 government shift to Dodoma. As a result, people from various parts of Tanzania are moving to this city. From that time, this influx of residents has led to an increase in MMUs, which has heightened the challenges associated with accessing MMSs. Therefore, the researchers found Dodoma an ideal location for this study

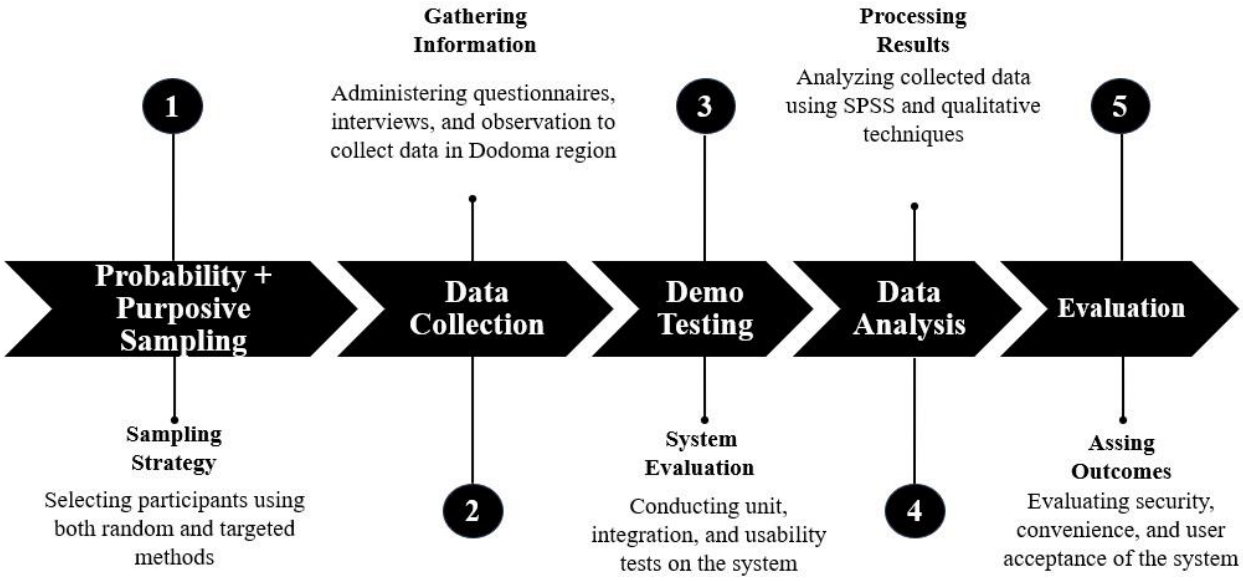

Figure 2: Study Methodology Workflow

3.2 Sampling technique and sample size

Given the nature of this study, it was practically impossible to obtain the entire population of interest; therefore, a sampling technique was employed. Sampling involves selecting a portion of an aggregate or totality to make inferences about the larger group [12]. There are two main types of sampling techniques: probability and non-probability sampling. In this study, both techniques were utilized. Specifically, probability sampling was used to select study areas within the area, ensuring that all areas had an equal chance of being chosen. In contrast, non-probability sampling was employed to identify and select the sample population for the research. Non-probability sampling ensured participants were MMS users, but this method may introduce selection bias, potentially limiting generalizability to non-users or rural populations. Consequently, this study included 258 respondents, comprising 204 MMCs and 54 MMAs. The sample was drawn from various areas within the study area (i.e., Dodoma), including Majengo, Mji Mpya, Kikuyu, Makulu, Area A, Area D, Kisasa, Chang'ombe, and Makole.

The sample size was determined using a mathematical calculation based on the formula provided by Yamane [13]:

$$S = \frac{N}{1+N(e)^2} \quad (1)$$

where N is the total population of Dodoma City Council and e denotes the level of significance given, which is 0.1. According to the Tanzania National Bureau of Statistics (NBS)[1], Dodoma City Council has a total population of 765,179 [14], hence N = 765,179. With these values of N and e, (1) evaluates to the following:

$$S = \frac{765{,}179}{1 + 765{,}179(0.1)^2}$$

$$S = \frac{765179}{7652.79}$$

$$S = 99.99 \approx 100$$

The results from this calculation indicate that the minimum sample size for Dodoma's population of 765,179 is 100 respondents (e = 0.1). However, we selected 258 respondents (204 MMCs, 54

[1] https://www.nbs.go.tz

MMAs) to reduce the margin of error, ensure robust representation of both user groups, and enable subgroup analysis by demographics such as gender and age.

3.3 Data Collection methods

Both qualitative and quantitative approaches were utilized to collect data. Quantitative data was gathered using structured questionnaires, while qualitative data was obtained through unstructured interviews and informal discussions. The questionnaires (Appendices 1 and 2) were designed for both MMCs and MMAs and consisted of three sections:

- Section A: Collected demographic information about respondents, including gender, age, employment status, and education level.
- Section B: Focused on respondents' usage and knowledge of MMSs, exploring various usage variables.
- Section C: Aimed to assess respondents' understanding of biometric authentication, specifically iris biometric authentication, and their opinions on the proposed framework for accessing MMSs.

Unstructured interviews conducted with MMCs provided insights into the functional and non-functional requirements of the mobile money applications, respectively presented in Tables 1 and 2. These interviews and questionnaires helped gather users' perceptions of the developed mobile money application based on the framework.

Additionally, we employed an observation technique to examine the direct interactions between MMAs and MMCs. This observational method provides richer and more accurate information by allowing the researcher to spend sufficient time studying the context [15].

Table 1. Functional requirements for the developed mobile money application based on the proposed framework.

Requirement	Description	Actor
User registration and account management	MMUs (agents and customers) must register with the system application. They must provide their names, Citizenship ID number, PIN, and captured iris biometric template.	MNO
	MMUs (agents and customers) must register with the system application. They must provide their names, Citizenship ID number, PIN, and captured iris biometric template.	MMC / MMA
Two-factor authentication	The application should be able to authenticate users before processing transactions by using both PIN and iris biometric mechanisms.	MMC / MMA
Transactions Processing	The application should be able to send money to another account, pay the bill, buy airtime, and make bundles and money transfers to other financial institutions.	MMC / MMA
Transaction SMS generation	The application should be able to generate and send the SMS to the MMU after allowing the transaction.	MNO

3.4 Data analysis tool and procedure

The Statistical Package for the Social Sciences (SPSS) tool was used to record data from the questionnaires, analyse data, and generate the necessary reports. Before the data entry process, two templates, one for MMCs and another for MMAs, were created in SPSS by configuring the Data View and Data Variable panels. All questions

and their corresponding answers were condensed into concise statements for clarity in the final report. Each question from the questionnaires was then entered into the variable data of the appropriate template, serving as headings for the various responses collected. Next, the responses were coded by assigning a numerical value to each question. Open-ended answers were structured to accommodate the input of such responses. After coding, the researcher entered each questionnaire into SPSS. To prevent duplicate entries, each questionnaire was numbered upon entry. Finally, results were generated from SPSS in percentages, tables, and graphs, clearly presenting the findings.

Table 2. Non-functional requirements for the developed mobile money application based on the proposed framework.

Requirement	Description
Speed	The application should be able to process both biometric authentication and transactions in a short time.
Security	The application should be able to authenticate MMU and prevent hackers from penetrating the system and its data.
Scalability	The application should be easily expandable to add other functions if needed.
Maintainability	The application should be easily maintained without affecting its functionality and customer data, for example, when customers update to a newer version.
Language	The application should support and be accessed in both English and Swahili.
Memory	The application should use less space on the user's phone so that it can be installed on phones with different capacities.
Operating System	The proposed application was implemented on the Android platform.

3.5 Testing and evaluation procedure of the mobile money application

The mobile money application developed by Rashidi et al. [11] implementing a 2FA framework with IRBAM was subjected to rigorous testing to ensure functionality and evaluate user perceptions. The testing process comprised unit testing, integration testing, and usability evaluation, following established software testing methodologies [16]. It is important to note that no new application was developed for this study; the evaluation focused on the existing application's performance and user experience through a demo version. Participants used a demo version of the application for 15–20 minutes, performing tasks such as sending money, checking balances, and authenticating with PIN and simulated iris scans. Feedback was collected through structured questionnaires (Appendices 1 and 2) and unstructured interviews, focusing on security, convenience, and acceptance. To protect participant privacy, the demo used anonymized data, ensuring no real sensitive information (e.g., citizenship ID numbers, PINs, and iris biometric templates) was collected, in line with ethical protocols presented in Section 3.6 of this paper.

3.5.1 Unit testing

Unit testing verified the functionality of individual components of the application. Key features tested included the following:

- Iris Scan Success Rate: The IRBAM module's ability to capture and process iris images was tested under controlled conditions (e.g., optimal lighting, 20–35 cm distance). The success rate, the percentage of successful iris recognitions, averaged 92% across 100 test cases, indicating high reliability.
- PIN Entry Validation: The PIN input interface was tested for correct validation

and error handling, achieving a 100% success rate in rejecting invalid PINs (e.g., incorrect formats or lengths).

- Transaction Initiation: Basic transaction functions, such as initiating a money transfer, were tested, with a 98% success rate in processing requests without errors.

3.5.2 Integration testing

Integration testing assessed the seamless operation of combined modules after unit testing. Examples of tested integrations included the following:

- Authentication-to-Transaction Flow: The integration of IRBAM and PIN authentication with transaction processing was tested to ensure users could authenticate and complete transactions without system crashes. This flow achieved a 95% success rate across 100 test cases, with minor delays attributed to network latency.
- Web Service Connectivity: The connection between the application's secure layer interface and MNO web services was tested, confirming 100% uptime and secure data transmission using Secure Socket Layer/Transport Layer Security encryption.
- Error Handling: The system's response to failed authentications (e.g., mismatched iris scans) was tested, with a 90% success rate in providing clear error messages (e.g., "Please rescan iris").

3.5.3 Usability testing

Usability testing was conducted to assess user perceptions of the application's security, convenience, and acceptance, using a survey-based method [16]. A total of 258 respondents (204 MMCs and 54 MMAs) interacted with a demo version of the application for approximately 15–20 minutes. Participants performed standardized tasks to simulate real-world MMS usage, including the following:

- Sending Money: Users initiated a mock money transfer, requiring PIN entry and a simulated iris scan for authentication.
- Checking Balance: Users access account balances and test the authentication and interface navigation.
- Withdrawing Cash (MMAs): Agents performed a mock cash withdrawal, simulating customer-agent interactions.

3.6 Ethical consideration

To observe research ethics, we provided detailed information about the purpose of the study to the participants and the importance of their participation. The researchers also ensured that the participants understood that the information obtained from them is confidential and kept securely secret. Furthermore, they were informed that the information collected from them was used only for academic purposes and not otherwise.

4. Results and Discussions

While Rashidi et al. [11] developed a theoretically robust framework combining IRBAM with 2FA, their study did not include empirical testing with users; instead, it relied on case studies and technical validation. This study addresses this gap by assessing the framework's practical effectiveness through feedback from 258 respondents (204 MMCs, 54 MMAs) in Dodoma, focusing on its ability to prevent unauthorized access, convenience, and user acceptance. These findings provide the first empirical insights into the framework's performance and adoption potential in Tanzania's rapidly growing MMS ecosystem.

4.1 Distribution of respondents

The demographic profile of respondents provides insights into the framework's potential effectiveness and adoption. The high proportion of younger users (79.41% MMCs, 72.2% MMAs aged 18–35) presented in section 4.1.2 suggests a tech-

savvy audience likely to embrace IRBAM, as younger individuals are typically more open to innovative technologies. The educated user base (47.55% MMCs with bachelor's degrees, 37.04% MMAs with diplomas) presented in section 4.1.3 indicates the capacity to understand and trust biometric authentication, potentially enhancing acceptance. However, the gender disparity (63.24% male MMCs) presented in Section 4.1.1 highlights the need for targeted outreach to female users to ensure equitable adoption.

4.1.1 Gender of respondents

The results shown in Table 3 indicate that among 54 MMAs, 53.70% (i.e., 29) were male, while 46.30% (i.e., 25) were female. Among 204 MMCs, 63.24% (i.e., 129) were male and 36.76% (i.e., 79) were female.

Table 3. Gender distribution of the respondents.

Gender	Agent		Customer	
	Count	%	Count	%
Male	29	53.70	129	63.24
Female	25	46.30	75	36.76
Total	**54**		**204**	

The gender distribution, with 63.24% of MMCs and 53.7% of MMAs being male, highlights a notable disparity that has implications for adopting the IRBAM framework. This male predominance may reflect broader trends in MMS usage, where men are often primary financial decision-makers or have greater access to smartphones in Tanzania. However, the underrepresentation of female users, particularly among customers (36.76% female MMCs), suggests potential barriers such as limited device ownership, lower digital literacy, or cultural norms restricting technology engagement. For the framework to achieve widespread adoption, targeted outreach to female users is essential, including women-focused education campaigns and partnerships with community organizations to promote inclusivity. Addressing this gender gap could enhance overall acceptance, ensuring the framework benefits all MMS users equitably.

4.1.2 Age of respondents

Table 4 shows the results regarding the age distribution of MMAs and MMCs in this study, revealing that 72.22% (39 respondents) of the MMA participants were aged 18–35. In contrast, 22.22% of respondents (i.e., 12 respondents) were in the 36–50 age group, while only 5.56% of them (3 respondents) aged 51 years and above. For the MMCs, 79.41% of the respondents (i.e., 162 respondents) fell within the youth age group of 18 -35 years, while 17.65% of them (36 respondents) aged between 36 - 50 years, and 2.94% of the respondents (6 respondents) were at least 51 years.

Table 4. Age distribution of the respondents.

Age	Agent		Customer	
	Count	%	Count	%
18 - 35	39	72.20	162	79.41
36 – 50	12	22.22	36	17.65
> 51	3	5.56	6	2.94
Total	**54**		**204**	

The age distribution, with 79.41% of MMCs and 72.2% of MMAs aged 18–35 years, indicates a predominantly young user base, which is necessary for adopting the IRBAM framework. Younger users are typically more tech-savvy and open to innovative technologies like biometrics. This demographic's digital literacy likely contributes to the strong acceptance rates and positive perceptions of security. However, the underrepresentation of older users (>51 years: 2.94% MMCs, 5.56% MMAs) suggests potential challenges, such as lower smartphone familiarity or skepticism about biometrics. To ensure inclusive adoption, MNOs should offer simplified interfaces and training for older users, addressing usability concerns and broadening the framework's reach.

4.1.3 Education level of respondents

The level of education among respondents was categorized into six groups (Table 5): primary, secondary, college certificate, diploma, bachelor's degree, and master's degree. The results indicate that 9.26% (5 respondents) of MMAs and 4.41% (9 respondents) of MMCs had completed primary education. Additionally, 18.52% (10 MMAs) and

6.86% (14 MMCs) had completed secondary education. Regarding college certificates, 12.96% (7 MMAs) and 0.98% (2 MMCs) reported having this level of education. A significant portion had completed diploma programs, with 37.04% (20 MMAs) and 35.29% (72 MMCs) attaining this qualification; 47.55% (12 MMCs) and 22.22% (97 MMAs) were represented at the bachelor's degree level. Finally, only 4.9% (10 MMCs) had earned a master's degree, while no agents reported this level of education.

Table 5. Education level of the respondents.

Education Level	Agent		Customer	
	Count	%	Count	%
Primary	5	9.26	9	4.41
Secondary	10	18.52	14	6.86
Certificate	7	12.96	2	0.98
Diploma	20	37.04	72	35.29
Bachelor	12	22.22	97	47.55
Master	0	0.00	10	4.90
Total	**54**		**204**	

The education level of respondents, with 47.55% of MMCs holding bachelor's degrees and 35.29% having diplomas, alongside 37.04% of MMAs with diplomas, reflects a relatively educated user base likely to understand and trust the IRBAM framework. Higher education levels correlate with greater awareness of cybersecurity risks and openness to advanced authentication methods, as seen in the 46.1% of MMCs and 51.9% of MMAs who strongly agreed on the framework's security benefits (Section 4.5). However, the relatively lower education levels among some MMAs (18.52% with secondary education) may contribute to their higher disagreement on convenience (20%, Section 4.6), possibly due to challenges navigating the biometric interface. To enhance adoption, MNOs should provide accessible training materials and in-app tutorials tailored to varying education levels, addressing low IRBAM awareness (65.2% MMCs, 79.9% MMAs unaware, Section 4.4) and ensuring user usability.

4.2 Criterion for selecting mobile network operators

Understanding user criteria for selecting MNOs for MMS provides critical context for tailoring the IRBAM framework proposed by Rashidi et al. [11] to user needs in Tanzania. Unlike Sections 4.3–4.7, which evaluate the framework's security, convenience, and acceptance, this section focuses on broader MMS preferences to inform framework design and adoption strategies. Criteria are organized into four thematic categories: service quality factors, economic factors, engagement incentives, and security prioritization. The analysis of MNO selection criteria reveals a clear hierarchy: service quality (speed, coverage) and economic factors (cost, commissions) dominate, followed by engagement incentives, with security unexpectedly marginalized. This pattern reflects practical user needs in Tanzania's MMS ecosystem, driven by a young, cost-sensitive demographic, but poses challenges for promoting IRBAM's security focus. By addressing these priorities through optimized authentication, cost-neutral implementation, and targeted incentives, MNOs can enhance the framework's convenience and acceptance, as further explored in Sections 4.6, 4.7, and 5.2.

4.2.1 Service quality factors

Service quality, particularly transaction speed and network coverage, is a primary driver of MNO selection. Figure 3 shows that 31.8% of MMCs prioritize speed, reflecting the need for rapid transaction processing in daily financial activities, such as bill payments or peer-to-peer transfers. MMAs, with 25.9% prioritizing speed, also value efficiency in handling high transaction volumes. Network coverage, essential for reliable MMS access, is prioritized by 16.2% of MMCs and 18.5% of MMAs, as agents require consistent connectivity to serve customers across urban areas like Dodoma. These findings align with the observation by Solazzo [10] of urban users' demand for seamless MMS (Section 4.8) and correlate with the young, tech-savvy demographic (79.41% MMCs aged 18–35, Section 4.1.2), who expect digital services to be fast and dependable. For the IRBAM framework, these priorities underscore optimizing authentication processes to

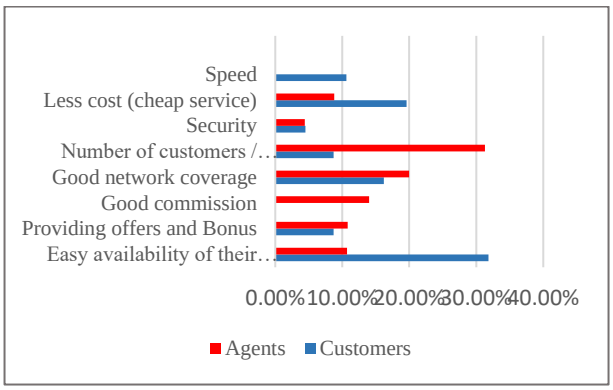

Figure 3. Criterion for selecting MNO.

maintain transaction speed. Furthermore, MNOs should ensure IRBAM's integration does not compromise speed or coverage, aligning with user expectations for convenience (50.2% MMCs strongly agree, Section 4.6).

4.2.2 Economic Factors

Economic considerations, including service cost and agent commissions, significantly influence MNO selection, reflecting financial constraints in Tanzania's MMS ecosystem. Figure 3 indicates that 19.6% of MMCs prioritize low transaction costs, a critical factor for younger users (79.41% aged 18–35 years, Section 4.1.2) with limited disposable income. MMAs emphasize economic factors more, with 22.2% prioritizing commissions, as their livelihood depends on transaction-based earnings. This aligns with findings in Section 4.7, where 30% of reluctant respondents cited smartphone costs as a barrier to framework adoption, particularly for MMAs reliant on feature phones. The predominance of male users (63.24% MMCs, 53.7% MMAs, Section 4.1.1) may reflect gender disparities in financial decision-making or device access, further amplifying cost sensitivity. To enhance framework adoption, MNOs should integrate IRBAM without increasing transaction fees, as suggested in Section 5.2.1, and offer subsidies to address device costs. These economic priorities highlight the need for cost-effective MMS solutions to ensure inclusivity and support the framework's acceptance (85.5% MMCs, 71.6% MMAs, Section 4.7).

4.2.3 Engagement incentives

Engagement incentives, such as promotional offers and bonuses, play a notable but secondary role in MNO selection, with greater appeal to MMCs than MMAs. Figure 3 shows that 10.3% of MMCs prioritize offers, such as cashback, loyalty rewards, or discounted transactions, reflecting the influence of marketing strategies on younger, digitally engaged users (79.41% aged 18–35 years, Section 4.1.2). MMAs, however, rank offers lower (5.6%), focusing instead on commissions and coverage, as their primary concern is operational efficiency over promotional benefits. This trend suggests that incentives can drive framework adoption among MMCs, particularly those with higher education levels (47.55% with bachelor's degrees, Section 4.1.3), who may respond to rewards enabling IRBAM. For example, MNOs could offer bonus credits for biometric authentication, as recommended in Section 5.2.1, potentially boosting acceptance rates (85.5% MMCs, Section 4.7). The lower MMA engagement with incentives indicates that agent-focused strategies should prioritize usability training (Section 5.2.1) over promotional campaigns.

4.2.4 Security prioritization

A critical finding from Figure 3 is the low prioritization of security, with only 4.5% of MMCs and 4.4% of MMAs ranking it as a key criterion, despite the IRBAM framework's emphasis on preventing unauthorized access (46.1% MMCs, 51.9% MMAs strongly agree, Section 4.5). This contradiction suggests users undervalue security due to familiarity with PIN-based authentication, perceived as sufficient, and low awareness of cyber risks (65.2% MMCs, 79.9% MMAs unaware of IRBAM, Section 4.4). Qualitative interview data indicates users may overlook risks, such as PIN theft or unauthorized access in unconscious states, which IRBAM mitigates through its high accuracy (92% iris scan success rate, Section 3.5) and liveness detection. These oversights could expose users to financial fraud since MMS transactions often involve significant sums. To align user perceptions with the framework's security benefits,

MNOs should implement education campaigns, such as in-app tutorials, SMS alerts, or community workshops, emphasizing IRBAM's advantages (e.g., unique iris patterns, spoofing resistance) without inducing fear, as recommended in Section 5.2.1. These strategies could increase trust, particularly among less-educated MMAs (18.52% with secondary education, Section 4.1.3), and support the framework's adoption.

These findings suggest that MMS providers should focus on enhancing speed and maintaining competitive costs to meet the demands of both agents and customers.

4.3 Mobile money awareness and usage knowledge

This subsection assesses customers' awareness and knowledge of MMSs. This assessment was based on the number of services customers utilize when accessing MMSs, which include money transfers, bill payments, and accessing financial services, as reported by Subia and Martinez [17].

Figure 4 illustrates the percentage of services that customers use in their typical transactions. The findings reveal that 14.71% (30 respondents) of customers use two services: sending and receiving money, and buying airtime. Additionally, 34.31% (70 respondents) of customers utilize three services: sending and receiving money, buying airtime, paying bills, or accessing financial services. Finally, 50.98% (104 respondents) of customers use four services: sending and receiving money, paying bills, buying airtime, and accessing financial services. The high engagement with MMS (50.98% of MMCs using four services) indicates strong user familiarity with mobile financial transactions, enabling informed feedback on the framework's security, convenience, and acceptance during demo testing.

4.4 Awareness of IRBAM

We evaluated the understanding of IRBAM among both agents and customers in MMSs. The analysis reveals that 79.90% (43 respondents) of MMAs and 65.20% (133 respondents) of MMCs

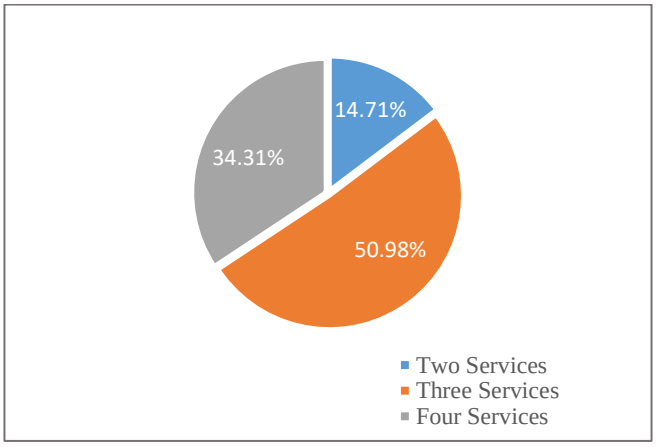

Figure 4. Percentage of the number of services the customers use in MMSs.

are not familiar with IRBAM as a verification method. Conversely, 24.10% (11 respondents) of MMAs and 34.80% (71 respondents) of MMCs are aware of this authentication method (Figure 5).

Low IRBAM awareness (65.2% MMCs, 79.9% MMAs unaware) highlights a barrier to adoption. Still, Section 4.5 discusses users' perceptions of its effectiveness in securing MMS data, where 46.1–51.9% strongly agreed that it prevents unauthorized access. The low awareness of IRBAM may be compounded by cultural skepticism toward biometric data and privacy concerns, as some interviewees expressed unease about storing iris templates. These factors underscore the importance of transparent communication regarding data security and cultural sensitivity to foster trust.

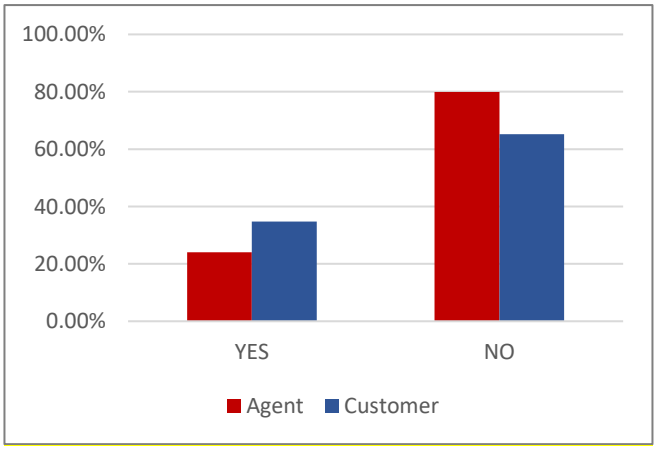

Figure 5. Awareness of iris biometric authentication.

4.5 Elimination of unauthorized access in MMS's

Users tested the framework by performing demo transactions (e.g., sending money, checking balance) and authenticating via PIN and simulated iris scans. Their perceptions of security presented in Figure 6, with 46.1% (94 respondents) of MMCs and 51.9% (28 respondents) of MMAs strongly agreeing that the framework prevents unauthorized access, were based on the robustness of the 2FA process and the perceived uniqueness of iris biometrics. MMAs' perceptions consistently exceed those of customers across all categories, except for the "strongly disagree" category. Specifically, 3.92% (8 respondents) of customers strongly disagree that the framework effectively eliminates unauthorized access, whereas no agent expressed strong disagreement. These findings suggest a higher level of confidence among agents regarding the effectiveness of the authentication framework proposed by Rashidi et al. [11] compared to customers. It is important to note that no real unauthorized access attempts were tested, as the evaluation focused on user feedback

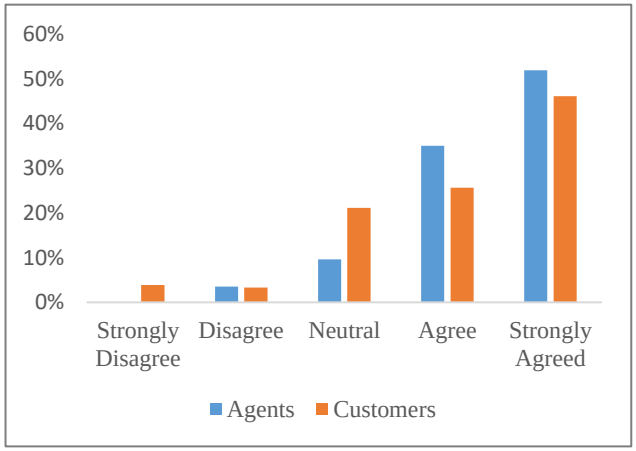

Figure 6. The MMU's perception of the elimination of unauthorized access to the mobile money app.

4.6 Convenience of Usage of the mobile money application based on the framework

The results from Figure 7 indicate that 50.2% (103 respondents) of MMCs and 35.6% (19 respondents) of MMAs strongly agree that the application is convenient for their use. Additionally, 13.10% (27 respondents) of MMCs and 7% (4 respondents) of MMAs expressed a neutral stance on the application's convenience. However, 10.9% (22 respondents) of customers and 20% (11 respondents) of agents disagreed that the application is convenient for them. The higher disagreement among MMAs (20%) on convenience, compared to MMCs (10.9%), may stem from workflow disruptions, as interviews revealed that iris authentication slowed agent transactions compared to PIN-based systems. Limited training and reliance on smartphones, which many MMAs lack, also contributed. Targeted training and streamlined authentication processes could address these issues.

4.7 The usage acceptance of the framework with IRBAM

The researchers aimed to understand customer acceptance of the framework, as this will significantly impact the market's success when adopted to enhance security in accessing MMSs. The findings on the acceptance of the framework with IRBAM, shown in Figure 8, reveal that 85.5% (174 respondents) of MMCs and 71.6% (39 respondents) of MMAs are willing to use it to access MMS. However, some agents and customers expressed reservations about adopting the framework. Among 41 reluctant respondents, 40% (17 respondents) cited health concerns about iris scanning, 30% (12 respondents) noted high smartphone costs, and 30% (12 respondents) reported usability issues. These concerns raised by a subset of agents and customers highlight potential barriers to adoption that must be addressed. To ensure successful integration of the framework, researchers suggest strategies to mitigate these concerns, such as offering education on usability, addressing health implications, distributing health information leaflets clarifying IRBAM safety, and exploring cost-effective solutions, may be used. This can help foster greater acceptance and enhance security in accessing MMSs.

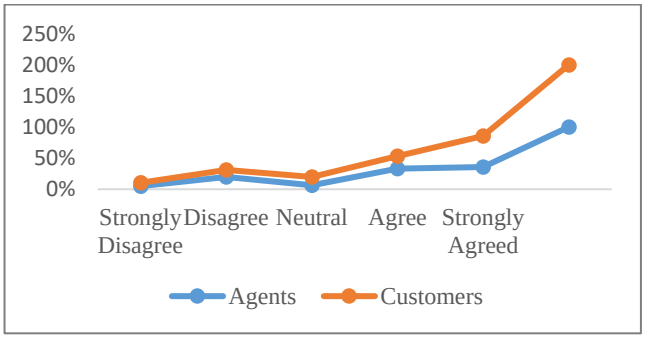

Figure 7. Convenience of usage of the mobile money application based on the framework.

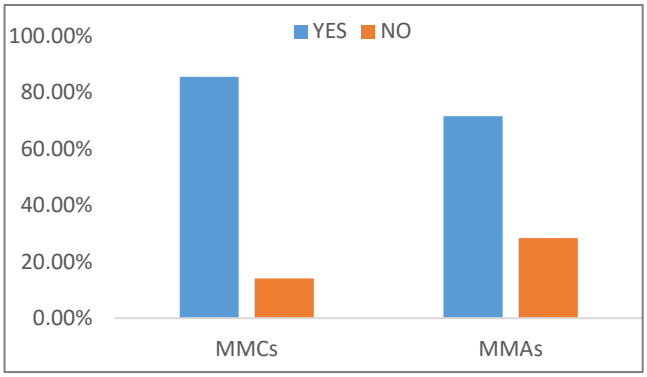

Figure 8. The usage acceptance of the proposed framework with IRBAM

4.8 Results Comparison with other studies

We evaluated the proposed framework's effectiveness by analyzing data gathered from MMUs. The criteria for evaluating the effectiveness of the mobile money application based on the framework incorporating the IRBAM included eliminating unauthorized access, convenience, and user acceptance. These same criteria were utilized by Subia and Martinez [17] in their evaluation of frameworks for designing, developing, and using secure mobile applications, and by Mtaho [8] in his study aimed at improving mobile money security with two-factor authentication (2FA) using PIN.

This study's findings align with and diverge from prior research on biometric authentication in financial services. Table 6 summarizes the comparison of this study's findings with ten (10) other studies focused on security, convenience, user acceptance, and adoption barriers [9], [18]. This comparison validates our findings on IRBAM's potential to enhance MMS security while highlighting unique adoption challenges in Tanzania, such as low awareness and health concerns. Data on sample characteristics, cultural context, and framework design are analyzed to contextualize our contributions.

4.8.1 Analysis of Findings Alignment

Serhani et al. [9] proposed a secure mobile app framework (Eivom Cinema Guide), reporting high security (HTTPS, authentication) and usability (UI, offline capabilities) via UAE contest feedback, likely exceeding our 46.1–51.9% security and 50.2–35.6% convenience due to mature interfaces versus IRBAM's biometric constraints (65.2–79.9% unaware). Their high acceptance aligns with our 85.5% MMCs but surpasses 71.6% MMAs. Resource constraints align with our cost barrier (30%), but health concerns (40%) are absent in their non-biometric model.

Belkhede et al. [18] explored iris biometrics for banking, reporting 88% user acceptance in controlled settings with high-end devices. Our lower acceptance (71.6–85.5%) reflects real-world constraints, such as varying smartphone quality and environmental factors in Dodoma. Their 90% security satisfaction contrasts with our 46.1–51.9%, likely due to their smaller, tech-savvy sample versus our diverse user base (47.55% MMCs with bachelor's degrees, 18.52% MMAs with secondary education). Health concerns, absent in the study by Belkhede et al. [18], emerged in ours (40% of reluctant respondents), highlighting cultural differences between India and Tanzania.

SMS-based security model for mobile banking in Tanzania, using symmetric encryption (AES) and message digests (SHA-1) to ensure end-to-end security over GSM networks, was proposed by Nyamtiga et al. [19]. They reported improved security through PIN enhancements (e.g., alphanumeric PINs, periodic changes) and encryption, but did not quantify user perceptions.

Table 6. Comparison of study's findings with other prior studies.

Study	Security	Convenience / Usability	Acceptance	Adoption Barriers	Limitations
This study	46.1% MMCs, 51.9% MMAs strongly agree on unauthorized access prevention	50.2% MMCs, 35.6% MMAs strongly agree; 20% MMAs disagree	85.5% MMCs, 71.6% MMAs willing to adopt	Low IRBAM awareness (65.2–79.9%), health concerns (40% = 17 respondents), cost (30% = 12 respondents), usability (30% = 12 respondents)	Urban focus, demo-based, feature phone exclusion
[9]	Not evaluated.	High (user-friendly, user interface, offline)	High (contest feedback)	Resource constraints	Non-Tanzanian, contest-based, non-MMS
[18]	90% security satisfaction	Not directly measured	88% acceptance	Device quality	Small, tech-savvy sample, no health concerns
[19]	Not evaluated	Usability goal measured	Not evaluated	Device capability, costs	Simulation based, no user data
[8]	82% perceive fingerprint 2FA as secure	78% find it convenient	85% acceptance	Cost, device compatibility	Mixed urban-rural sample, no health concerns noted
[10]	Not evaluated	Not evaluated	Not evaluated; cost as key barrier	Low smartphone penetration (45% urban)	No biometric focus, urban bias
[7]	65% security satisfaction for iris biometrics	70% usability satisfaction	Not directly measured	Privacy, inclusivity issues	Generic, not MMS-specific
[20]	86% (authentication), 70% (integrity), 56% (confidentiality)	Not evaluated	Not evaluated	Hardware access, costs	No end-user data
[6]	95% iris authentication accuracy	Not directly measured	60% express privacy concerns	Hardware costs, user trust	Broad survey, no user feedback

[21]	77.9% consider it safe	81.6% (confirm recipient details)	Not directly evaluated	Public internet, awareness	Urban, agent-centric, no acceptance data
[11]	Innovative IRBAM framework use	Not directly measured	Not evaluated	Not evaluated	No empirical testing, limited adoption discussion

Our study's security agreement (46.1–51.9%) provides empirical user feedback absent in the study by Nyamtiga et al.[19], though their focus on encryption aligns with IRBAM's liveness detection for spoofing prevention. Their model's reliance on Java-enabled phones for the client application mirrors our smartphone dependency, contributing to similar accessibility barriers (e.g., 30% of our respondents cited smartphone costs). They also noted usability as a design goal but did not report convenience metrics, making our 50.2% MMC and 35.6% MMA convenience ratings a novel contribution. Their lack of user acceptance data contrasts with our 85.5% (MMCs) and 71.6% (MMAs), though their model's PIN-based authentication likely benefits from higher cultural familiarity compared with the IRBAM's low awareness (65.2–79.9% unaware). Unlike our study, they did not identify health concerns, as their cryptographic approach avoids biometric-specific barriers.

On the other hand, Mtaho [8] evaluated a fingerprint-based two-factor authentication (2FA) system for MMS in Tanzania, reporting that 82% of users perceived it as secure and 78% found it convenient. Our study's lower security agreement (46.1% MMCs, 51.9% MMAs strongly agreeing) and mixed convenience ratings (50.2% MMCs, 35.6% MMAs strongly agreeing) may reflect IRBAM's novelty and higher hardware requirements compared with fingerprint biometrics, which are widely integrated into smartphones. The higher acceptance rate (85%) in the study by Mtaho [8] contrasts with our 85.5% for MMCs but lower 71.6% for MMAs, possibly due to agents' workflow disruptions (20% disagreement on convenience). The cultural familiarity with fingerprints in Tanzania, versus low IRBAM awareness (65.2% MMCs, 79.9% MMAs unaware), likely explains these differences. Unlike Mtaho [8], we identified health concerns about iris scanning, a unique barrier requiring targeted education. Samsung [22] explained that while there are no health risks associated with using iris recognition devices at a distance of 20–35 cm, potential health issues may arise if the device is used for more than 10 seconds at a distance of 2 cm.

The author in [10] examined MMS adoption in Tanzania, noting that smartphone penetration (45% in urban areas) drives usage but limits accessibility for feature phone users. Our findings align, for example, as 79.41% of MMCs (aged 18–35) used smartphones, but many MMAs relied on feature phones, contributing to lower convenience ratings (15.7% MMAs reported delays). Solazzo [10] reported cost as a primary adoption barrier, consistent with our 30% of reluctant respondents citing smartphone costs. However, the author did not evaluate biometric authentication, making our study's focus on IRBAM's security benefits (46.1–51.9% agreement) a novel contribution. The urban focus of both studies (Dodoma vs. Dar es Salaam) limits generalizability to rural areas, where feature phone usage is higher.

Furthermore, Lovisotto et al. [7] proposed a five-factor framework (security, usability, inclusivity, robustness, privacy) for mobile biometrics in financial services, emphasizing usability as a key adoption driver. Their usability

metric (70% user satisfaction across biometrics) is higher than our 50.2% MMC and 35.6% MMA convenience agreement, likely due to IRBAM's environmental constraints (e.g., lighting, distance). Our security findings (46.1–51.9%) align with their 65% security satisfaction for iris biometrics, but our lower inclusivity (due to smartphone dependency) highlights a gap not emphasized in their multi-biometric approach. Cultural privacy concerns, noted by 30% of our reluctant respondents, align with the privacy factor in the study by Lovisotto et al. [7] but are amplified in Tanzania due to low biometric awareness.

A security model for tracking mobile money creation in Tanzania using Transport Layer Security (TLS) 1.3 protocol and Public Key Infrastructure (PKI) was developed by Rwiza et al. [20]. The model ensures integrity, confidentiality, authentication, and non-repudiation of financial returns transmitted from banks and MNOs to regulators. Evaluators rated security mechanisms highly (86% excellent for authentication, 70% for integrity, 56% for confidentiality), exceeding our IRBAM security agreement (46.1–51.9%). This discrepancy likely stems from focus on technical evaluators (50 information security experts) done in the study by Rwiza et al. [20] versus our broader user base (258 MMCs and MMAs), where low biometric awareness (65.2–79.9%) reduced trust. Rwiza et al. [20] did not report user convenience or acceptance metrics, as their prototype prioritized system-level security over end-user interaction, making our 50.2% MMC and 35.6% MMA convenience ratings and 85.5% MMC/71.6% MMA acceptance rates unique contributions. Their model's reliance on server infrastructure and certificates assumes access to modern hardware, aligning with our smartphone dependency barrier (30% of respondents cited costs). Unlike our study, Rwiza et al. [20] did not identify health concerns, as their cryptographic approach avoids biometric-specific issues. Their focus on regulatory tracking complements our user-facing authentication framework, highlighting different MMS security dimensions.

Alrawili et al. [6] reviewed biometric authentication methods, reporting that iris biometrics achieve 95% authentication accuracy but face adoption barriers due to hardware costs and user trust issues. Our study's 46.1–51.9% security agreement reflects lower user confidence, possibly due to the demo-based evaluation versus real-world implementation. It was noted that 60% of users express privacy concerns, higher than our 30%, suggesting that Tanzania's MMS users may be less aware of privacy risks due to low IRBAM exposure (65.2–79.9% unaware). Their emphasis on hardware costs aligns with our findings, as MMAs' feature phone usage limits accessibility. Our user-centered evaluation adds practical insights into these barriers, which are absent in broader survey done by Alrawili et al. [6].

A framework to address MMS security vulnerabilities in Tanzania, identifying threats such as unintended transaction requests, public internet usage, and application misbehavior was proposed by Mlelwa et al. [21]. The study reported high user confidence in MMS safety (77.9% of 163 respondents, primarily Airtel Money agents and employees in Dar es Salaam), surpassing our IRBAM security agreement (46.1–51.9%). This difference likely reflects focus on existing MMS platforms with familiar interfaces (e.g., USSD, apps) evaluated in [21] versus IRBAM's novel biometric approach, compounded by our respondents' low awareness (65.2–79.9% unaware). The framework proposed by Mlelwa et al. [21] emphasizes stakeholder collaboration and user awareness, but did not quantify convenience, though 81.6% of respondents confirmed recipient details before transactions, suggesting usability familiarity. Our convenience ratings (50.2% MMCs, 35.6% MMAs) provide empirical insights absent in the study by Mlelwa et al. [21], likely lower due to IRBAM's hardware and environmental constraints. Mlelwa et al. [21] reported 55.8% agreement on transaction privacy, higher than our 30% privacy concern rate, possibly due to their focus on non-biometric interfaces less associated with health concerns (40% in our study).

User acceptance was not directly quantified by Mlelwa et al. [21], but their high safety perception aligns with our 85.5% MMC acceptance, though our 71.6% MMA rate is lower, likely due to agents' workflow issues. Mlelwa et al. [21] identified barriers (e.g., public internet risks, lack of awareness), aligning with our smartphone cost (30%) and awareness (65.2–79.9%) barriers, but their non-biometric focus avoids IRBAM's health concerns. Their urban, agent-centric sample limits rural generalizability, similar to our study's urban focus.

4.8.2 Analysis of findings divergences

The lower security and convenience ratings in our study compared with the ratings reported from other studies [8] stem from IRBAM's novelty, higher hardware demands, and real-world testing constraints, contrasted with the familiarity of fingerprints, controlled environments, technical evaluations, established MMS interfaces, or non-financial mobile apps. Nyamtiga et al. [19], Rwiza et al. [20], and Mlelwa [21] share our Tanzania-specific MMS focus but diverge in methodology, as their cryptographic or awareness-based models avoid biometric challenges, such as health concerns, which our study uniquely identifies (40% of reluctant respondents). Serhani et al. [9] offer a broader mobile app framework, not MMS-specific, and their UAE-based, non-biometric context reduces cultural barriers (e.g., health concerns) but limits Tanzania-specific insights. Sample differences also contribute: our diverse, urban sample (258 respondents, 63.24% male, 79.41% aged 18–35) differs from those from previous studies [8], which focused on a mixed urban-rural cohort, tech-savvy group, simulation-based approach, expert evaluators, agent-centric sample, and contest-based evaluators, respectively. Cultural context shapes acceptance, as Tanzania's low biometric awareness and health concerns reduce trust compared with other findings [8], where PIN-based, cryptographic, or non-biometric systems benefit from higher user trust. Framework design further explains divergences: IRBAM's liveness detection addresses spoofing risks not covered by Mtaho [8], Serhani et al.[9], Nyamtiga et al. [18], and Rwiza et al. [19], but its smartphone dependency limits inclusivity compared to multi-biometric approach used by Lovisotto et al [7] or platform-agnostic design used by Serhani et al. [9]. These differences underscore our study's contribution in offering Tanzania-specific, user-centered insights into IRBAM adoption challenges, particularly health concerns and awareness gaps.

5. Conclusion and Recommendations

5.1 Conclusion

This study evaluated the framework's effectiveness in enhancing MMS security using 2FA with IRBAM, which was proposed by Rashidi et al. [11]. Our findings confirm that the framework significantly reduces unauthorized access, with 46.1% of customers and 51.9% of agents strongly agreeing on its security benefits. However, challenges such as low IRBAM awareness and concerns about usability and health risks must be addressed to ensure widespread adoption. In addition, the low prioritization of security (4.5% MMCs, 4.4% MMAs) contrasts with the framework's focus on IRBAM, suggesting users may trust existing PIN-based systems or lack awareness of cyber risks, including unauthorized access. This oversight could expose users to theft, highlighting the need for education campaigns to promote security benefits, such as in-app tutorials or community workshops, without inducing fear.

Furthermore, the low awareness of IRBAM (65.2% MMCs, 79.9% MMAs) may be compounded by cultural skepticism toward biometric data and privacy concerns, as some interviewees expressed unease about storing iris templates. These factors highlight the need for transparent communication about data security and cultural sensitization to build trust.

5.2 Recommendations

The findings from this study, summarized in Table 7, highlight the potential of the IRBAM

framework proposed Rashidi et al. [11] to enhance MMS security, alongside challenges such as low awareness, smartphone dependency, and environmental constraints. To facilitate adoption and maximize the framework's impact in Tanzania's MMS ecosystem, we propose actionable recommendations for key stakeholders: MNOs, Internet Service Providers (ISPs), government and policymakers, and MMUs. These recommendations address user priorities, adoption barriers, and device disparities, ensuring alignment with the study's objectives of improving security, convenience, and acceptance.

5.2.1 Mobile network operators

MNOs should prioritize integrating the IRBAM framework into MMS platforms to enhance security. In addition to addressing low awareness, MNOs should launch education campaigns via in-app tutorials, SMS alerts, and workshops to highlight IRBAM's safety and benefits and counter health concerns. Furthermore, to overcome smartphone barriers for MMAs, MNOs should offer smartphone subsidies or develop USSD-based authentication for feature phones, ensuring inclusivity. Agent training and optimized authentication processes are needed to improve convenience and reduce delays. Lastly, using anonymized data and transparent privacy policies, ethical data practices should be maintained to build trust and address privacy concerns.

Table 7. Summary of key findings.

Criterion	Customers (MMCs)	Agents (MMAs)
Strong Agreement on Security	46.1% (94)	51.9% (28)
Strong Agreement on Convenience	50.2% (103)	35.6% (19)
Willingness to Adopt	85.5% (174)	71.6% (39)
IRBAM Awareness	34.8% (71)	24.1% (11)

5.2.2 Internet Service Providers

ISPs are critical for ensuring the connectivity required for the IRBAM framework's web services, facilitating secure communication between the application and MNO servers. To support framework adoption, ISPs should reduce Internet costs, as high data tariffs amplify economic barriers for MMUs, particularly MMAs reliant on commissions.

5.2.3 Government and policymakers

Government and policymakers can facilitate framework adoption through policy interventions that enhance accessibility and trust. Policymakers should consider funding digital literacy programs targeting older and female users, who are underrepresented in MMS usage. These programs could include biometric authentication workshops addressing low IRBAM awareness and health concerns. To build trust, the government should establish clear regulations on biometric data protection, ensuring compliance with ethical standards and addressing privacy concerns.

5.2.4 Mobile money users

MMUs, including MMCs and MMAs, can optimize their experience with the IRBAM framework by addressing environmental and behavioral factors. To mitigate IRBAM's environmental constraints (e.g., lighting, movement, distance), users should follow in-app prompts, such as "hold steady" or "adjust lighting," to ensure successful iris scans, improving the 92% success rate observed in testing.

MMUs should also engage with educational resources provided by MNOs, such as tutorials or leaflets, to understand IRBAM's safety and security benefits and counter health concerns. To address privacy concerns, users should verify that MNOs use secure, anonymized data practices, as implemented in the demo, and report any

transparency issues to regulators. Finally, MMCs responsive to incentives could advocate for bonus programs tied to IRBAM adoption, boosting acceptance rates.

CONTRIBUTIONS OF CO-AUTHORS

Mustafa Mohsini	[ORCID: 0000-0003-0219-7946]	Conceived the idea, conducted data collection, and wrote the paper.
Florence Rashidi	[ORCID: 0000-0001-6477-8362]	Provided technical assistance on methods and materials.
Bakari Mega		Conducted data collection and results interpretation.

APPENDICES: Questionnaires

Appendix 1: QUESTIONNAIRE TO MOBILE MONEY CUSTOMERS

Dear Respondent,

This questionnaire aims to collect data regarding the evaluation of effectiveness of the iris recognition biometric authentication method to improve security level in accessing mobile money services. The results from this survey will be used in aggregate, without referring to any one individual, and will be used solely for academic purposes. Your response will be kept confidential and there is no right or wrong answer. It is the researcher's hope that you could spend some of your time to answer this survey.

Thanks for your willingness to participate in answering this questionnaire.

Tick the most appropriate response.

A. DEMOGRAPHIC INFORMATION

1. Region…….. District ……..
2. Gender of the respondent

   a) Male b) Female
3. Occupation of the respondent

   a) Employee b) Entrepreneur c) Unemployed d) Student
4. Age group

   a)18-35 b) 36-50 c) >51
5. Education Level

   a) Primary Education b) Secondary Education c) Certificate, d) Diploma,

   e) Bachelor degree/Advance diploma f) Master degree,

B. KNOWLEDGE ON MOBILE MONEY AND ITS USAGE

1. For how long have you being using mobile money services?

   a) < 1 Year b) 1-2 Years c) 3-4 Years d) >5 Years
2. What services you normally use in mobile money services?

   a) Sending/Receiving money b) Bills payment

   c) Buy airtime and bundle d) Accessing financial service (e.g. Bank)
3. How many times do you use mobile money services in a week?

   a) Once b) twice c) thrice d) frequently
4. Do mobile money services have any advantage to you?

   a) Yes b) No

If YES, what are the advantages gained from the use of mobile money services

……

……

5. Which mobile money network operator do you use?

a)Tigo b) Vodacom c) Airtel d) Halotel e) Zantel f) TTCL

6. What reason(s) made you to choose that mobile money operator in question 6 above?

……

……

7. Which type of mobile phone do use to access mobile money services?

a) Featured phone b) Smartphone

C. EVALUATION ON EFFECTIVENESS OF THE IRIS RECOGNITION BIOMETRIC AUTHENTICATION METHOD ON IMPROVING SECURITY LEVEL IN ACCESSING MOBILE MONEY SERVICES.

The following questions assess your experience with a demo mobile money application that uses iris biometric authentication (IRBAM) combined with a PIN for secure access. You were asked to perform sample transactions (e.g., sending money, checking balance) and test the authentication process using a simulated iris scan and PIN entry. Please answer based on your interaction with the demo.

1. What authentication methods (e.g., PIN, password, fingerprint) do you currently use for mobile money services (MMS), and what limitations do you experience with them?

……
……
……
……

2. What are your concerns about MMS security risks (e.g., fraud, unauthorized access), and how much do you trust current authentication systems?

……
……
……
……

3. Do you know about biometric authentication?

a) Yes b) No

4. (If yes in question 3) Are you familiar with the IRBAM?

a) Yes b) No

5. (If yes in question 4) How do you compare IRBAM with other biometric methods (e.g., fingerprint, facial recognition) in terms of perceived security and ease of use?

……
……
……
……

6. Will the use of IRBAM eliminate unauthorized access in mobile money services?

   a) Strongly disagree b) Disagree c) Neutral d) Agree e) Strongly agree

7. Will you accept the proposed IRBAM?

   a) Yes b) No

8. Please give reason(s) for the above (question 7)

   ……
   ……
   ……
   ……

9. Will the use of IRBAM in accessing mobile money services be convenient for you?

   a) Strongly disagree b) Disagree c) Neutral d) Agree e) Strongly agree

10. How would you rate the following aspects of an IRBAM system for MMS

    1) Strongly disagree 2) Disagree 3) Neutral 4) Agree 5) Strongly agree

    a. The system is easy to use.

    b. The system is acceptable for MMS transactions.

    c. The system is trustworthy for securing transactions.

    d. The system is accurate in authenticating users.

    e. The system is reliable for consistent performance.

    f. I am willing to adopt this system for MMS.

Appendix 2: QUESTIONNAIRE TO MOBILE MONEY AGENT

Dear Respondent,

This questionnaire aims to collect data regarding the evaluation of effectiveness of the iris recognition biometric authentication method to improve security level in accessing mobile money services. The results from this survey will be used in aggregate, without referring to any one individual, and will be used solely for academic purposes. Your response will be kept confidential and there is no right or wrong answer. It is the researcher's hope that you could spend some of your time to answer this survey.

Thanks for your willingness to participate in answering this questionnaire.

Tick the most appropriate response.

A. DEMOGRAPHIC

1. Region…….. District ……..
2. Gender of the respondent
   a) Male b) Female
3. Age group
   a) 18-35 b) 36-50 c) 51-above
4. Education Level

   a) Primary Education b) Secondary Education c) Certificate d) Diploma

   e) Bachelor degree/Advance diploma f) Master degree

B. KNOWLEDGE ON MOBILE MONEY AND ITS USAGE

1. For how long have you being serving as mobile money agent?
   a) < 1 Year b) 1-2 Years c) 3-4 Years d) >5 Years
2. What services you normally provide in mobile money services?
   a) Sending/Receiving money b) Bills payment
   c) Buy airtime and bundle d) Accessing financial service (e.g., Bank)
3. Do mobile money services have any advantage to you?
   a) Yes b) No
   If **YES,** what are the advantages gained from the use of mobile money services
   ……
   ……
4. What mobile money network operators do you have?
   a) Tigo b) Vodacom c) Airtel d) Halotel e) Zantel f) TTCL
5. Which mobile money network operator is mostly used?
   a) Tigo b) Vodacom c) Airtel d) Halotel e) Zantel f) TTCL
6. What reason(s) made mobile money operator in question 6 above to be mostly used?

   ……

   ……

7. Which type of mobile phone do you use to provide mobile money services?
   a) Featured phone b) Smartphone

C. EVALUATION ON EFFECTIVENESS OF IRIS RECOGNITION BIOMETRIC AUTHENTICATION METHOD ON IMPROVING SECURITY LEVEL IN ACCESSING MOBILE MONEY SERVICES.

The following questions assess your experience with a demo mobile money application that uses iris biometric authentication (IRBAM) combined with a PIN for secure access. You were asked to perform sample transactions (e.g., sending money, checking balance) and test the authentication process using a simulated iris scan and PIN entry. Please answer based on your interaction with the demo.

1. What authentication methods (e.g., PIN, password, fingerprint) do you currently use for mobile money services (MMS), and what limitations do you experience with them?

   ……
   ……

……
……

2. What are your concerns about MMS security risks (e.g., fraud, unauthorized access), and how much do you trust current authentication systems?

……
……
……
……

3. Do you know about biometric authentication?

a) Yes b) No

4. (If yes in question 3) Are you familiar with the IRBAM?

a) Yes b) No

5. (If yes in question 4) How do you compare IRBAM with other biometric methods (e.g., fingerprint, facial recognition) in terms of perceived security and ease of use?

……
……
……
……

6. Will the use of IRBAM eliminate unauthorized access in mobile money services?

a) Strongly disagree b) Disagree c) Neutral d) Agree e) Strongly agree

7. Will you accept the proposed IRBAM?

a) Yes b) No

8. Please give reason(s) for the above (question 7)

……
……
……
……

9. Will the use of IRBAM in accessing mobile money services be convenient for you?

a) Strongly disagree b) Disagree c) Neutral d) Agree e) Strongly agree

10. How would you rate the following aspects of an IRBAM system for MMS

1) Strongly disagree 2) Disagree 3) Neutral 4) Agree 5) Strongly agree

a. The system is easy to use.

b. The system is acceptable for MMS transactions.

c. The system is trustworthy for securing transactions.

d. The system is accurate in authenticating users.

e. The system is reliable for consistent performance.

f. I am willing to adopt this system for MMS.

REFERENCES

[1] TCRA, "Communication Statistics Tanzania Communications Regulatory Authority," Sep. 2023. [Online]. Available: https://www.tcra.go.tz/uploads/text-editor/files/TCRA%20Communications%20Statistics%202023%20-2024-Q1_1698210303.pdf

[2] TCRA, "Tanzania Communications Regulatory Authority Communications Statistics," Jun. 2024. [Online]. Available: https://www.tcra.go.tz/uploads/text-editor/files/Communication%20Statistics%20report%20for%20end%20of%20June%202024_EN_1721315046.pdf

[3] E. Salveggio, S. Lovaas, D. R. Lease, and R. Guess, "Biometric Authentication," in *Computer Security Handbook*, Wiley, 2012. doi: 10.1002/9781118851678.ch29.

[4] D. Juniati, I. Ketut Budayasa, and C. Khotimah, "The similarity of iris between twins and its effect on iris recognition using box counting," *Communications in Mathematical Biology and Neuroscience*, vol. 2020, pp. 1–13, 2020, doi: 10.28919/cmbn/5148.

[5] K. Hollingsworth, K. W. Bowyer, and P. J. Flynn, "Similarity of iris texture between identical twins," in *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition - Workshops*, IEEE, Jun. 2010, pp. 22–29. doi: 10.1109/CVPRW.2010.5543237.

[6] R. Alrawili, A. Abdullah, S. Alqahtani, and M. Khurram Khan, "Comprehensive Survey: Biometric User Authentication Application, Evaluation, and Discussion," *Computers and Electrical Engineering*, vol. 119, no. Part A, Oct. 2024, doi: https://doi.org/10.1016/j.compeleceng.2024.109485.

[7] G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, and I. Martinovic, "Mobile Biometrics in Financial Services: A Five Factor Framework," 2017. Accessed: May 13, 2025. [Online]. Available: https://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf

[8] A. B. Mtaho, "Improving Mobile Money Security with Two-Factor Authentication," *Int J Comput Appl*, vol. 109, no. 7, pp. 975–8887, 2015, Accessed: May 13, 2025. [Online]. Available: https://www.ijcaonline.org/archives/volume109/number7/19198-0826/

[9] M. A. Serhani, A. Benharref, R. Dssouli, and R. Mizouni, "Toward an Efficient Framework for Designing, Developing, and Using Secure Mobile Applications," *International Journal of Humanities and Social Sciences*, vol. 3, no. 4, 2009, Accessed: May 14, 2025. [Online]. Available: https://publications.waset.org/5042.pdf

[10] L. Solazzo, "Smartphones will surpass feature phone subscriptions in Tanzania by 2024," May 2019. [Online]. Available: https://www.verdict.co.uk/tanzania-smartphones/

[11] F. U. Rashidi, M. H. Mohsini, and B. Mega, "A framework for security improvement on usage of mobile money application based on iris biometric authentication method," *Information Security Journal: A Global Perspective*, vol. 33, no. 6, pp. 678–690, Nov. 2024, doi: 10.1080/19393555.2024.2347240.

[12] J. W. Creswell and J. D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, Fifth Edition. SAGE Publications, 2018. Accessed: May 14, 2025. [Online]. Available: https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf

[13] T. Yamane, *Statistics: An Introductory Analysis*, 2nd edition. New York: Harper and Row, 1967.

[14] NBS, "The United Republic of Tanzania Administrative Units Population Distribution Report," 2022. [Online]. Available: https://www.nbs.go.tz/nbs/takwimu/Census2022/Administrative_units_Population_Distribution_Report_Tanzania_volume1a.pdf

[15] R. Kumar, *Research methodology: a step-by-step guide for beginners*, 3rd Edition. SAGE Publications, 2011.
[16] K. Moumane, A. Idri, and A. Abran, "Usability evaluation of mobile applications using ISO 9241 and ISO 25062 standards," *Springerplus*, vol. 5, no. 1, p. 548, May 2016, doi: 10.1186/s40064-016-2171-z.
[17] M. P. Subia and N. Martinez, "mobile money services: 'A bank in your pocket': Overview and Opportunities," 2014. [Online]. Available: https://publications.iom.int/system/files/pdf/mobile_money.pdf
[18] M. Belkhede, V. Gulhane, and P. Bajaj, "Biometric Mechanism for enhanced Security of Online Transaction on Android system: A Design Approach," in *The 14th International Conference on Advanced Communication Technology(ICACT)*, Feb. 2012. Accessed: May 14, 2025. [Online]. Available: https://www.icact.org/upload/2012/0496/20120496_finalpaper.pdf
[19] B. W. Nyamtiga, A. Sam, and L. S. Laizer, "Enhanced Security Model For Mobile Banking Systems In Tanzania," *INTERNATIONAL JOURNAL OF TECHNOLOGY ENHANCEMENTS AND EMERGING ENGINEERING RESEARCH*, vol. 1, p. 4, 2013.
[20] S. Rwiza, M. Kissaka, and K. Kapis, "Security Model for Tracking Creation of Mobile Money Using Transport Layer Security Protocol," *Tanzania Journal of Science*, vol. 46, no. 3, pp. 791–806, Oct. 2020, doi: 10.4314/tjs.v46i3.19.
[21] K. L. Mlelwa, "A Framework for Addressing Mobile Money Security Vulnerabilities in Tanzania," *Int J Innov Sci Res Technol*, vol. 8, no. 3, 2023, [Online]. Available: www.ijisrt.com
[22] SAMSUNG, "Galaxy S8: Is it Harmful being IR-irradiated on the Eyes for Authentication? ," May 2020. [Online]. Available: https://www.samsung.com/hk_en/support/mobile-devices/galaxy-s8-is-it-harmful-being-ir-irradiated-on-the-eyes-for-authentication/