

Mozambican financial system: Use of AI in ATMs with biometric authentication and chatbots

Yasser Muetirru Omar

Bachelor's degree in Communications Engineering; Lecturer; Researcher and Technological Innovator at the Scientific Directorate of the Military Academy, Research and Technological Innovation Center;
Email: ymuterua@gmail.com

Abstract- The digitalization of financial services has increased the importance of developing banking technologies that are secure, accessible, and user-oriented. This study analyzes the potential integration of Artificial Intelligence (AI), biometric authentication, and conversational chatbots into Automated Teller Machines (ATMs) to address security and accessibility challenges in the Mozambican banking context. The study adopts a qualitative and conceptual research design based on a structured literature review and scenario-based comparative analysis. Relevant literature on AI in banking, biometric authentication, ATM security, banking chatbots, financial inclusion, and digital literacy was analyzed thematically. A conceptual comparison was also developed between conventional PIN-based ATM systems and a proposed AI-biometric ATM model, focusing on authentication security, user assistance, accessibility, and operational usability. The reviewed evidence suggests that biometric authentication can strengthen user verification and reduce vulnerabilities associated with the sharing or observation of PINs, while AI-powered conversational interfaces may improve user autonomy by providing real-time, step-by-step assistance.

Keywords: Financial Inclusion; Digital Banking; ATM Security; User Accessibility; Conversational Banking.

I. INTRODUCTION

Let's imagine a scenario where a user goes to an ATM (Automatic Teller Machine) and finds an elderly lady in front of the machine. After a few minutes, he realizes that she hasn't performed any transaction. When he offers help, the lady, with a smile, explains that she can't transfer an amount received from her late husband's income because she hasn't used the service in a long time. This type of situation, which may seem simple, reveals real difficulties that many users face when interacting with banking equipment. The lack of familiarity with the interfaces, the absence of immediate support, and the complexity of some operations highlight the need for more accessible and intuitive technological solutions, such as the use of AI (Artificial Intelligence) with biometric authentication and chatbots for real-time assistance.

Artificial intelligence is a branch of Computer Science whose interest is to make computers think or behave intelligently Haugeland (1985, as cited in Gomes, 2010). According to Haugeland (1985, cited in Gomes, 2010), this is an effort to create machines with minds in the full and literal sense. In this context, the integration of artificial intelligence with biometric authentication systems and chatbots in

ATMs represents an innovative solution to increase security, accessibility, and trust in banking services. This technological combination reduces the risk of fraud by eliminating the need for third-party assistance and facilitates use by the elderly, people with disabilities, and customers less familiar with technology. The embedded chatbot contributes to financial inclusion by guiding the user step-by-step, offering support in different languages, and allowing direct contact with human agents, while biometric authentication ensures that only the authorized account holder can carry out transactions.

Thus, this research aims to analyze the impacts of applying artificial intelligence, combined with biometrics and chatbots, on the operation of ATMs, highlighting their practical applicability and contributions to the national financial system.

This study adopts the hypothetical-deductive method, as it is suitable for analyzing innovative solutions for ATMs, allowing the identification of gaps in knowledge about the user experience and the formulation of hypotheses regarding the impact of artificial intelligence, biometric authentication, and chatbots. Based on these hypotheses, empirical and theoretical evidence is analyzed to test and

validate the practical applicability of these technologies, seeking to support the improvement of the security, accessibility, and efficiency of banking services. To this end, the bibliographic research technique is used, since, according to Bello (2009, as cited in Almeida, 2021), "it is extremely important that the researcher verifies the veracity of the information from their data source. Practically all research requires a bibliographic study to support their research projects" (p.32).

The review research was carried out using the IEEEExplore, Google Scholar, and ResearchGate databases. For this research, the following keywords were used: chatbots in banks, artificial intelligence, biometric authentication in ATMs, chatbots in banks, and artificial intelligence in banking. From the scientific publications available in these databases, it was possible to compile a set of relevant information.

II. METHODOLOGY

This study adopts a qualitative and conceptual research design based on a structured literature review and scenario-based comparative analysis. The methodological approach was selected to examine how Artificial Intelligence (AI), biometric authentication, and conversational chatbots can contribute to improving the security, accessibility, and usability of Automated Teller Machines (ATMs), with particular attention to the Mozambican banking context.

The literature review focused on scientific publications addressing AI in banking, biometric authentication, ATM security, banking chatbots, financial inclusion, digital literacy, and accessibility in financial services. Relevant publications were identified through searches conducted in IEEE Xplore, Google Scholar, and other academic sources. The search strategy combined terms such as "artificial intelligence in banking," "biometric authentication in ATMs," "banking chatbots," "AI-powered banking services," and "financial inclusion." Publications were considered relevant when they addressed at least one of the technological or social dimensions investigated in this study.

The selected literature was analyzed thematically to identify evidence concerning the potential benefits, limitations, and implementation requirements of AI-based technologies in banking environments. Particular attention was given to issues related to authentication security, user assistance, accessibility, digital literacy, transaction usability, and the reduction of dependence on third-party assistance. In addition to the literature review, a scenario-based comparative analysis was developed to examine the differences between conventional PIN-based ATM interaction and a proposed AI-biometric ATM model.

The comparison considered four analytical dimensions: authentication security, user assistance, accessibility, and operational usability. The conventional ATM model represents the existing interaction paradigm based primarily on cards, PINs, and conventional graphical interfaces, whereas the proposed model incorporates biometric authentication and an AI-powered conversational interface capable of providing step-by-step assistance.

The analysis was conducted conceptually rather than through direct experimentation with ATM users. Therefore, the comparative framework does not claim to measure actual changes in transaction time, fraud rates, user satisfaction, or queue reduction. Instead, it uses findings reported in the literature to assess the potential contribution of the proposed technological combination to the identified challenges. This distinction is important because the study seeks to develop a theoretically grounded framework for future empirical investigation rather than present unobserved outcomes as measured results.

The methodological approach also considered the specific requirements of the Mozambican context, including differences in digital literacy, accessibility needs, rural and urban banking environments, and the potential use of local languages in human-machine interaction. These contextual factors were incorporated into the analysis to determine how solutions documented in other banking environments could potentially be adapted to Mozambique.

Generative Artificial Intelligence was used solely as a language-support tool during manuscript preparation, including grammar correction, translation, and formatting. It was not used to generate empirical data, conduct statistical analysis, determine research findings, or replace the authors' interpretation of the reviewed literature.

III. LITERATURE REVIEW

Artificial Intelligence in Financial Services

Artificial intelligence is related to several factors and areas of study, and is therefore approached in different ways by different thinkers (Gomes, 2010). Bellman (1978, as cited in Gomes, 2010) and Haugeland (1985, as cited in Gomes, 2010), it is associated with the way humans think, constituting an effort to create computers capable of thinking, that is, machines with minds in the full and literal sense, as well as the automation of human activities such as problem-solving and decision-making.

Artificial Intelligence (AI) has progressively become an important component of digital transformation in the financial sector. Its applications include customer service, fraud detection, risk assessment, personalization, process automation, and decision support. A systematic literature review by Kalyani and Gupta (2023) indicates that AI and machine learning are increasingly being incorporated into banking operations, contributing to service efficiency and influencing consumer perceptions of convenience and trust in digital banking environments.

The relevance of AI in banking extends beyond operational automation. AI-based systems can process large volumes of information and support interactions between financial institutions and customers. In customer-facing applications, conversational systems can provide immediate responses to routine requests and assist customers in navigating increasingly digital financial services. However, the adoption of AI in financial services also requires attention to reliability, transparency, security, privacy, and human oversight.

The use of AI is therefore particularly relevant to ATM modernization. Traditional ATMs generally provide customers with a predefined sequence of commands through graphical interfaces. An AI-enabled ATM could potentially provide a more adaptive interaction by interpreting user requests and offering contextual assistance. Such functionality may be particularly valuable for customers who experience difficulties with conventional interfaces, including older users and individuals with limited digital literacy.

Nevertheless, AI should not be considered a substitute for human judgment in all banking situations. Recent research on banking chatbots shows that AI-based customer service is particularly useful for routine interactions, but limitations in accuracy and reliability remain relevant when users present complex requests. Human assistance therefore remains necessary for situations that exceed the capabilities of automated systems (Graham et al., 2025).

Biometric Authentication and Banking Security

"Biometrics is biological authentication, based on certain physical characteristics of the human body" (Satish Tanaji Bhosale, 2012, p. 10). According to the author, there are two categories of biometric identifiers: physiological characteristics, linked to body shape, such as fingerprints, facial recognition, DNA, palm prints, hand geometry, iris, and odor; and characteristics related to behavior, such as typing rhythm, gait, digital signature, and voice. In contrast, traditional access control methods use identifiers based on tokens (e.g., passport or driver's license) or knowledge, such as passwords and PINs (Personal Identification Numbers).

In banking environments, biometric authentication has attracted attention because conventional authentication mechanisms may be vulnerable to credential sharing, observation, theft, or forgetting. Bhosale (2012) discussed the application of biometric authentication to cardless ATM environments, illustrating the potential of biometric technologies to strengthen user verification and reduce dependence on conventional credentials.

However, biometric authentication should not be regarded as inherently immune to security threats. Biometric systems can be affected by false acceptance, false rejection, presentation attacks, privacy concerns, and the potential compromise of stored biometric templates. Consequently, biometric authentication should be understood as one component of a broader security architecture rather than as an absolute replacement for all other security mechanisms.

For ATM applications, the combination of biometric authentication with additional security mechanisms may therefore provide a more robust approach. The literature on hybrid biometric ATM authentication illustrates the possibility of combining different authentication mechanisms to improve security while maintaining practical usability (Arokiasamy et al., 2024). Such approaches are particularly relevant when designing systems intended to serve users with different levels of technological familiarity.

ATM Usability, Accessibility, and Digital Literacy

Automated Teller Machines (ATMs) constitute an important component of modern banking infrastructure because they allow customers to perform basic financial transactions without direct assistance from bank employees. Arokiasamy et al. (2024), describe ATMs as electronic systems that provide customers with access to basic banking services while highlighting the security limitations associated with conventional authentication mechanisms. Their study proposes hybrid biometric authentication as a potential approach to strengthening ATM security and improving the user experience.

Beyond authentication, the evolution of ATM technology raises broader questions concerning usability and accessibility. The expansion of ATM networks has increased the availability of banking services by allowing customers to perform transactions outside conventional bank-counter interactions. In the Mozambican context, the National Financial Inclusion Strategy 2025–2031 identifies branches, ATMs, point-of-sale terminals, banking and non-banking agents, and digital financial services as important channels for accessing

financial products and services (Banco de Moçambique, 2025). The strategy therefore places ATMs within a broader financial-access ecosystem rather than treating them merely as technological devices.

However, the physical availability of an ATM does not necessarily imply effective access to financial services. Financial inclusion also depends on individuals' ability to understand and use available financial channels. Adel (2024), based on evidence from 56 emerging countries, found that digital literacy has a positive effect on financial inclusion in Africa and emphasized the importance of region-specific strategies for addressing differences in digital capabilities. This finding suggests that expanding digital financial infrastructure should be accompanied by measures that enable users to interact effectively with technological systems.

This issue is particularly relevant to ATM usability. Users with lower levels of digital literacy may experience difficulties when interpreting menu structures, understanding transaction instructions, selecting appropriate options, or recovering from input errors. The interaction between digital literacy and financial technology is also supported by research conducted in rural Uganda, where digital literacy was found to positively moderate the relationship between biometric financial technologies and digital financial inclusion among underserved groups, including women, youth, and persons with disabilities. This evidence suggests that the benefits of biometric and other digital financial technologies depend partly on users' capacity to interact effectively with them.

Accessibility represents another important dimension of ATM usability. Users with visual, motor, cognitive, or other disabilities may encounter barriers when ATM interaction depends predominantly on conventional visual displays or physical interfaces. Accessibility-oriented ATM technologies demonstrate that alternative interaction mechanisms can be incorporated into banking machines without eliminating their core financial functions. For example, the Royal Bank of Canada reports that it introduced voice-guidance-

enabled or "talking" ATMs to provide auditory assistance to customers who have difficulty interacting with conventional visual ATM interfaces (Royal Bank of Canada, n.d.).

The development of talking ATMs therefore provides an important precedent for the proposed model. Such systems demonstrate that voice-based assistance can be incorporated into ATM environments to support independent interaction. The Royal Bank of Canada's accessibility implementation further indicates that voice guidance can coexist with conventional ATM functions and can be designed to protect the privacy of users while they conduct transactions.

From this perspective, ATM modernization should not be evaluated exclusively according to processing capacity, transaction availability, or technological sophistication. Usability, accessibility, comprehensibility, user autonomy, and perceived security should also be considered. A technologically advanced ATM that remains difficult for users to understand may not necessarily produce greater financial inclusion.

The literature consequently supports the relevance of features such as simplified interfaces, voice-based interaction, clear instructions, and contextual assistance. These mechanisms may reduce some of the cognitive and operational barriers associated with conventional ATM interaction. Nevertheless, their effectiveness should not be assumed universally. Interface design must take account of users' digital literacy, language, disability status, technological familiarity, and the physical environment in which the ATM operates.

For the proposed AI-assisted ATM, this literature provides a basis for extending existing accessibility mechanisms through conversational interaction. Rather than relying exclusively on predefined audio instructions, an AI-enabled system could potentially provide context-sensitive guidance and respond to simple user questions. However, this constitutes a proposed technological application and requires empirical evaluation before claims concerning

improved usability, autonomy, or inclusion can be established.

Therefore, the literature reviewed in this section suggests that the future development of ATMs should move beyond the traditional objective of merely providing automated transactions. A more inclusive ATM should combine secure authentication with accessible interaction mechanisms, while taking into account digital literacy, user diversity, privacy, and local contextual conditions. In the Mozambican context, this perspective is particularly relevant because financial inclusion depends not only on the availability of financial access points but also on the population's capacity to use them effectively and securely (Adel, 2024; Banco de Moçambique, 2025).

Chatbots

A chatbot is a computer program designed to simulate a conversation with a human user, and has existed since the 1960s. Its popularity increased significantly in 2016, when institutions such as Bank of America and Absa launched bots intended for standard banking procedures (Mills, 2017, as cited in Gary Graham et al., 2025).

Recent research also demonstrates that trust and privacy are important considerations in AI-based banking interactions. Rohita et al. (2025) found that characteristics of smart banking chatbots can influence consumer trust and engagement, while privacy concerns can negatively affect some relationships between chatbot characteristics and trustworthiness.

Voice-based interaction is particularly relevant to the proposed ATM model because it may reduce dependence on visual interfaces. Recent research on banking voicebots indicates that trust plays a central role in users' willingness to adopt AI-enabled conversational banking technologies. The study further suggests that social presence and other characteristics of conversational interaction can influence perceptions of trust and adoption intentions.

These findings suggest that a chatbot integrated into an ATM should not merely reproduce the

information displayed on the screen. Instead, it should function as an interactive assistance layer capable of providing understandable instructions, clarifying user actions, and transferring complex cases to human support when necessary.

IV. ANALYSIS AND DISCUSSION

The results presented in this study derive from the structured literature review and the scenario-based conceptual comparison described in the methodology. Therefore, the findings should not be interpreted as empirical measurements obtained from ATM users or from the implementation of a functional prototype. Instead, they represent literature-informed analytical findings concerning the potential integration of Artificial Intelligence (AI), biometric authentication, and conversational chatbots into Automated Teller Machines (ATMs) in the Mozambican banking context.

The analysis was organized around five main dimensions: authentication security, user accessibility and autonomy, financial inclusion, operational usability, and the integration of AI and biometric technologies. The discussion also considers the privacy, trust, cybersecurity, and implementation challenges that may affect the feasibility of the proposed model.

Authentication Security

The first result of the conceptual comparison concerns the potential strengthening of ATM authentication through biometric technologies. Conventional ATM systems generally rely on a combination of a physical banking card and a Personal Identification Number (PIN). Although this mechanism remains widely used, its effectiveness depends partly on the user's ability to maintain the confidentiality of the PIN. Consequently, situations involving PIN observation, disclosure, theft, or social engineering may compromise the authentication process.

The literature on biometric ATM systems suggests that biometric authentication can provide an additional authentication factor and reduce exclusive dependence on memorized credentials. Moorthy,

Mohd Daud, Arokiasamy, and Tomal (2024), for example, examined hybrid biometric authentication for ATMs and identified biometrics as a promising approach for addressing security weaknesses associated with traditional authentication mechanisms. Their work highlights the relevance of fingerprint-based authentication and hybrid approaches for improving ATM security.

This finding is consistent with the broader understanding of biometric authentication, in which physiological characteristics can be used to verify the identity of an individual. In the context of the proposed model, the use of biometrics may reduce some risks associated with the sharing, forgetting, or observation of PINs. However, this does not mean that biometric authentication eliminates fraud or makes ATM transactions completely secure.

An important finding from the literature is that biometric technologies introduce their own security and privacy challenges. Arokiasamy et al. (2024), discuss biometric authentication as a response to traditional ATM vulnerabilities, but the implementation of biometric systems must also account for authentication errors and attacks against biometric systems. Therefore, the security advantage of the proposed model should be understood as a potential strengthening of the authentication architecture rather than as the elimination of security risks.

This distinction is particularly important because biometric information differs from conventional passwords. A compromised PIN can normally be changed, whereas biometric characteristics are intrinsically associated with the individual. Consequently, the proposed ATM architecture should incorporate complementary security mechanisms, including secure biometric-template protection, encryption, liveness or presentation-attack detection, transaction monitoring, and appropriate mechanisms for handling authentication failures.

Kalyani and Gupta (2023), in their systematic review of AI and machine learning in banking, similarly emphasize that the increasing digitalization of

banking services creates new opportunities while also generating cybersecurity challenges. Their review of 734 articles demonstrates that AI and machine learning have been applied across multiple banking functions, while security remains an important consideration in increasingly digital banking environments.

Therefore, the first conceptual result is that biometric authentication can potentially strengthen ATM security, particularly by reducing dependence on PIN-based authentication. However, its effectiveness depends on the technical quality of the biometric system and on the cybersecurity architecture in which it is implemented.

Role of Artificial Intelligence in Banking Services

The second result concerns the potential role of AI in transforming customer-facing financial services. Hentzen, Hoffmann, Dolan, and Pala (2022) conducted a systematic literature review of 90 studies on AI in customer-facing financial services. Their analysis demonstrates that AI research in financial services has addressed several applications, including automated decision-making, customer interaction, and technology adoption.

Similarly, Kalyani and Gupta (2023) identify AI and machine learning as increasingly relevant technologies within banking, particularly because of their potential to improve banking processes and customer experiences. These findings provide theoretical support for considering AI as an additional layer of functionality within ATM systems. However, the proposed application differs from the traditional use of AI in online or mobile banking. Instead of using AI solely for back-office analytics or digital customer service, the proposed model places AI directly at the physical point of interaction between the bank and the customer. This creates the possibility of transforming the ATM from a predominantly menu-driven transaction machine into an interactive banking interface.

The conceptual result is therefore that AI could expand the role of ATMs beyond transaction execution. An AI-enabled ATM could potentially interpret simple user requests, provide explanations,

guide customers through procedures, and adapt the interaction according to the user's needs.

Nevertheless, this potential should not be confused with demonstrated operational effectiveness. The present study does not provide experimental evidence showing that AI-enabled ATMs are faster, more efficient, or more satisfactory than conventional ATMs. Such claims require direct empirical testing.

Accessibility and User Autonomy

A major finding of the analysis concerns the potential contribution of conversational AI to user accessibility and autonomy. Conventional ATM interfaces require users to interpret menus, identify appropriate options, enter numerical information, and follow a sequence of instructions. These requirements may present difficulties for individuals with limited digital literacy or limited experience with electronic banking systems.

Graham, Nisar, Prabhakar, Meriton, and Malik (2025) found that banking chatbots can provide useful customer-service automation, particularly for simple tasks. Their study identified convenience, speed, and continuous availability as important characteristics of chatbot-based services. At the same time, the authors emphasize limitations associated with accuracy, reliability, and complex customer requests. These findings are relevant to the proposed ATM model because they indicate that conversational AI may be particularly useful when the user requires guidance through routine procedures. Instead of relying exclusively on a graphical menu, the ATM could interact with the user through short questions and instructions.

For example, a user could indicate that they wish to withdraw money, and the system could guide the user sequentially through authentication, amount selection, confirmation, and transaction completion. In conceptual terms, this interaction could reduce the cognitive burden associated with navigating multiple menus.

The potential for voice interaction is also important. A voice-enabled interface could provide spoken

instructions and allow users to communicate with the ATM through natural language. Such functionality may be relevant for users who experience difficulties with conventional visual interfaces. However, the effectiveness of voice-based interaction depends on speech-recognition accuracy, background noise, language coverage, accent variation, and the quality of the underlying AI model.

For this reason, the proposed system should not simply transfer an existing chatbot into an ATM. It should be designed specifically for the physical banking environment and for the characteristics of the target population.

The conceptual result is therefore that conversational AI may increase user autonomy when it provides simple, sequential, and understandable assistance. However, the extent of this benefit remains an empirical question that must be evaluated with actual users.

Trust, Privacy, and Reliability of Conversational Banking

The potential accessibility benefits of AI must be considered together with trust and privacy. Financial transactions involve sensitive information, and users may be reluctant to interact with automated systems if they do not trust their accuracy or the way their data are handled.

Rohita, Kumari, Singh, and Alofaysand (2025) investigated smart banking chatbots and found that conversational agility and ubiquitous connectivity were associated with trustworthiness, while privacy concerns negatively moderated several relationships between chatbot characteristics and trust. Their findings demonstrate that technological functionality alone does not guarantee user trust in AI-based banking services.

This finding has direct implications for the proposed ATM model. If a chatbot provides unclear, incorrect, or misleading instructions, users may lose confidence in the system. Similarly, if users are uncertain about how their conversational

information or biometric data are processed, they may resist adoption.

Graham et al. (2025) also emphasize that chatbots are more appropriate for relatively simple customer-service tasks and may encounter limitations when dealing with complex requests. Consequently, the proposed ATM should include mechanisms for recognizing situations in which automated assistance is insufficient.

The system could, for example, identify an unsuccessful authentication attempt, a disputed transaction, an unusual request, or a question outside the chatbot's knowledge domain and direct the user toward human assistance or an appropriate banking support channel.

Thus, the analysis suggests that trust should be treated as an architectural requirement rather than as an automatic consequence of AI adoption. The proposed system should be transparent about its automated nature, provide understandable instructions, protect user information, and ensure that human assistance remains available when required.

Potential Contribution to Financial Inclusion

The third major dimension of the analysis is financial inclusion. The relevance of this dimension is particularly strong in developing-country contexts because access to financial infrastructure does not necessarily guarantee effective use of financial services.

Adel (2024), examining 56 emerging countries across Africa, Asia, and Latin America, found that digital literacy enhances financial inclusion in the African context. The study also emphasizes that technological strategies need to account for regional differences rather than assuming that the same digital intervention will produce identical outcomes in different environments.

This finding is important for the proposed AI-assisted ATM because the technology is intended not merely to increase automation but also to reduce barriers to effective interaction with banking

services. If conversational guidance makes ATM procedures easier to understand, it may potentially benefit users who experience difficulties with conventional digital interfaces.

The proposed system therefore combines two potentially complementary mechanisms. Biometric authentication may reduce some difficulties associated with remembering and entering PINs, while conversational AI may reduce some difficulties associated with understanding and navigating ATM procedures.

The National Financial Inclusion Strategy of Mozambique for 2025–2031 explicitly places emphasis on access and effective use of quality financial products and services, supported by knowledge, confidence, and security. The strategy also incorporates the digitalization of financial services as part of the broader financial inclusion agenda (Banco de Moçambique, 2025). Therefore, the proposed technological model is conceptually aligned with the broader national direction toward digital and inclusive financial services.

However, the proposed ATM should not be regarded as a universal solution to financial exclusion. Adel (2024) demonstrates that digital inclusion is influenced by regional conditions, while technological adoption can produce different outcomes depending on the context. Accordingly, an AI-assisted ATM deployed in Mozambique would need to consider digital literacy, infrastructure, language, affordability, accessibility, and user trust.

Integration of Biometric Authentication and Conversational AI

One of the central results of this study is the identification of a complementary relationship between biometric authentication and conversational AI.

Biometric authentication and conversational AI perform fundamentally different functions. The former primarily addresses identity verification, while the latter primarily addresses interaction and assistance. Their integration therefore creates a

broader architecture in which security and usability can be considered simultaneously.

The conceptual model proposed in this study can be represented by four interconnected layers:

1. **Authentication layer:** verifies the user's identity through biometric and complementary authentication mechanisms.
2. **Interaction layer:** uses conversational AI to guide the user through available banking services.
3. **Transaction layer:** executes the banking operation after the necessary authentication and authorization procedures have been completed.
4. **Human-support layer:** receives cases that require human intervention or exceed the AI system's capabilities.

The literature supports the importance of maintaining this separation of functions. Graham et al. (2025) demonstrate that banking chatbots have considerable potential for routine customer service but remain limited in complex situations. Rohita et al. (2025) further demonstrate the importance of trust and privacy in AI-driven banking interactions. Consequently, the proposed model should not be designed as a fully autonomous banking system. Rather, it should be conceived as a human-supervised AI banking interface in which automated assistance is combined with conventional banking controls and human escalation.

This distinction also improves the security logic of the proposed model. Biometric authentication does not determine what the customer should do, and the chatbot does not independently establish the customer's identity. Each technology performs a specific function within the broader banking architecture.

Operational Usability and Potential Efficiency

The conceptual analysis also identifies possible implications for operational usability. Graham et al. (2025) found that convenience and speed are among the factors associated with positive perceptions of banking chatbots, particularly in simple customer-service interactions. These findings suggest that conversational assistance could potentially make

some ATM procedures easier to understand and complete.

However, the present study cannot conclude that the proposed system would reduce transaction time, shorten queues, or increase customer satisfaction in Mozambique. Such claims would require empirical testing.

For example, a future study could compare conventional and AI-assisted ATMs using indicators such as:

- Average transaction completion time;
- Number of failed transaction attempts;
- Authentication error rates;
- Frequency of requests for external assistance;
- Task completion rate;
- User satisfaction;
- Perceived ease of use;
- Perceived security; and
- User intention to continue using the system.

Such indicators would allow the conceptual propositions developed in this study to be tested quantitatively.

Therefore, the current finding is limited to the identification of potential operational benefits, rather than demonstrated efficiency gains.

Conceptual Comparison Between Conventional and AI-Biometric ATMs

The preceding analysis permits a conceptual comparison between the conventional ATM and the proposed AI-biometric model.

Table 1. Conceptual comparison between conventional and proposed AI-biometric ATM

Dimension	Conventional ATM	Proposed AI-Biometric ATM
Authentication	Card and PIN	Biometrics combined with complementary security mechanisms
Credential dependence	Relatively dependent on memorized PIN	Potentially reduced dependence on memorized credentials

User interaction	Menu and screen-based	Conversational and potentially voice-assisted
User guidance	Predefined instructions	AI-supported step-by-step assistance
Accessibility potential	Primarily dependent on interface design	Potential for multimodal interaction
Authentication vulnerabilities	PIN theft, observation, disclosure and card-related risks	Biometric errors, presentation attacks and privacy risks
Privacy requirements	Conventional banking and transaction data	Banking data plus potentially biometric and conversational data
Complex assistance	External human assistance	AI assistance with human escalation
Digital-literacy requirements	May require familiarity with ATM menus	Potentially reduced through conversational guidance
Financial-inclusion potential	Dependent on access, literacy and usability	Potentially increased if appropriately designed and localized
Evidence base in this study	Established technology	Conceptual proposal requiring empirical validation

Note. Created by Yasser (2026).

The comparison indicates that the proposed system does not represent a simple technological substitution. Rather, it combines authentication and interaction technologies to address different dimensions of the ATM experience.

The literature reviewed by Hentzen et al. (2022) and Kalyani and Gupta (2023) demonstrates the increasing importance of AI in financial services, while Arokiasamy et al. (2024), provide specific support for the relevance of biometric authentication in ATM security. Graham et al. (2025) and Rohita et al. (2025), in turn, highlight both the

opportunities and limitations of AI-mediated customer interaction.

The contribution of the proposed model therefore lies in the integration of these technological functions within the physical ATM environment.

Implications for the Mozambican Banking Context

The findings have several implications for the potential development of intelligent ATMs in Mozambique.

First, the implementation of such systems should be aligned with the country's financial inclusion objectives. The National Financial Inclusion Strategy 2025–2031 emphasizes access, effective use, knowledge, trust, security, and digitalization of financial services (Banco de Moçambique, 2025). This policy orientation provides a relevant institutional context for examining technologies that simultaneously address security and usability.

Second, implementation should account for differences in digital literacy. Adel (2024) demonstrates that digital literacy is relevant to financial inclusion in African contexts. Consequently, an intelligent ATM should not be designed exclusively for technologically experienced users. The interface should provide clear instructions, simple language, accessible interaction modes, and assistance appropriate to users with different levels of digital competence.

Third, linguistic adaptation should be considered. A conversational system developed for Mozambique would need to be evaluated according to the languages, accents, and communication practices of its intended users. The inclusion of local languages should therefore be treated as a technological and usability research question rather than assumed as an automatic capability of AI.

Fourth, implementation should be gradual. Pilot deployments could allow financial institutions to assess technical reliability, authentication accuracy, cybersecurity, user acceptance, accessibility, and operational costs before broader deployment.

Finally, the implementation of AI-assisted ATMs should involve collaboration among banks, technology developers, regulators, cybersecurity specialists, accessibility experts, and users. Such collaboration would help ensure that technological innovation does not occur independently of regulatory, ethical, social, and usability considerations.

Limitations of the Analysis

The findings of this study must be interpreted in light of its conceptual methodology. First, no primary data were collected from ATM users in Mozambique. Consequently, the study cannot statistically demonstrate relationships between the proposed technology and fraud reduction, transaction speed, customer satisfaction, or financial inclusion.

Second, the proposed AI-biometric ATM has not been implemented as a functional prototype. Its biometric accuracy, speech-recognition performance, AI response reliability, cybersecurity resilience, hardware requirements, and operational costs therefore remain to be empirically established. Third, much of the available literature originates from banking systems and populations outside Mozambique. Hentzen et al. (2022), Kalyani and Gupta (2023), Graham et al. (2025), Rohita et al. (2025), and Adel (2024) provide relevant evidence, but their findings cannot automatically be generalized to the Mozambican population without contextual validation.

Fourth, the proposed model involves technologies that introduce new risks. Biometric authentication creates privacy and security requirements, while conversational AI introduces risks related to inaccurate responses, inappropriate guidance, and user trust. These challenges reinforce the need for empirical and technical validation before practical implementation.

These limitations define the scope of the study rather than undermine its contribution. The study provides a conceptual basis from which future empirical and technological investigations can be developed.

REFERENCES

1. Adel, N. (2024). The impact of digital literacy and technology adoption on financial inclusion in Africa, Asia, and Latin America. *Heliyon*, 10(24), e40951.
<https://doi.org/10.1016/j.heliyon.2024.e40951>
2. Almeida, Í. (2021). *Metodologia do trabalho científico* (23rd ed.). Recife, Brazil: Universidade Federal de Pernambuco.
3. Arokiasamy, S. R., Tomal, M. R. I., Moorthy, K., & Mohd Daud, K. (2024). Hybrid biometric authentication for automatic teller machine. *International Journal of Software Engineering and Computer Systems*, 10(1), 32–39.
<https://doi.org/10.15282/ijsecs.10.1.2024.3.0121>
4. Banco de Moçambique. (2025). National financial inclusion strategy 2025–2031. Maputo, Mozambique: Banco de Moçambique.
5. Bhosale, S. T. (2012). Security in e-banking via cardless biometric ATMs. *ResearchGate*, 10–15.
6. Gomes, D. dos S. (2010). Inteligência artificial: Conceitos e aplicações. *Revista Olhar Científico*, 1(2), 234–246.
7. Graham, G., Nisar, T. M., Prabhakar, G., Meriton, R., & Malik, S. (2025). Chatbots in customer service within banking and finance: Do chatbots herald the start of an AI revolution in the corporate world? *Computers in Human Behavior*, 165, 108570.
<https://doi.org/10.1016/j.chb.2025.108570>
8. Hentzen, J. K., Hoffmann, A., Dolan, R., & Pala, E. (2022). Artificial intelligence in customer-facing financial services: A systematic literature review and agenda for future research. *International Journal of Bank Marketing*, 40(6), 1299–1336.
<https://doi.org/10.1108/IJBM-09-2021-0417>
9. Kalyani, S., & Gupta, N. (2023). Is artificial intelligence and machine learning changing the ways of banking: A systematic literature review and meta analysis. *Discover Artificial Intelligence*, 3, 41.
<https://doi.org/10.1007/s44163-023-00094-0>
10. Rohita, K., Kumari, P., Singh, N., & Aloyfaysand, H. (2025). Smart banking chatbots and consumer engagement: The role of trust and privacy in AI-driven banking. *Journal of Strategic Marketing*.
<https://doi.org/10.1080/0965254X.2025.2481140>
11. Royal Bank of Canada. (n.d.). Accessibility: Talking ATMs. Royal Bank of Canada