ISBN: 978-628-95207-8-1. ISSN: 2414-6390. Digital Object Identifier: 10.18687/LACCEI2024.1.1.201

Systematic Review of Authentication Techniques in Banking Applications in Latin America

Luis R. Puma Herencia*, Glenda Julia Merma Mayhua †, Luis A. Alfaro Casas ‡ and Wilder Nina Choquehuayta§
Computer and Systems Engineering, Universidad Tecnológica del Perú
Arequipa, Perú
Email: *U19314535@utp.edu.pe, †U21308135@utp.edu.pe, ‡C16272@utp.edu.pe, §C18795@utp.edu.pe

***Abstract*—Computer security, especially authentication in banking applications, has become a critical issue to ensure the integrity and confidentiality of users' financial information. The current situation presents significant challenges, such as vulnerability to attacks, lack of strong authentication, and lack of cybersecurity coordination across the region. The objective is to provide a systematic review on the updated and comprehensive perspective on authentication security in banking applications in Latin America, identifying trends, gaps and research opportunities. The methodology used followed a clear approach, using the PICO strategy to formulate the research question. An exhaustive review was carried out on the studies, applying inclusion and exclusion criteria, and following PRISMA guidelines. Having 150 articles as a base quantity from 2019 to 2023, of which 20 articles were selected that met the criteria for inclusion in the systematic review. The results revealed various authentication techniques used in Latin American banking applications, such as microservices, biometrics, multi-factor authentication and tokenization. Multi-factor authentication proved to be the most secure, with an average success rate of 97.9%, on the other hand, knowledge factor authentication proved to be the least secure, with an average success rate of 58%. Trends show an increase in the use of biometrics and multi-factor authentication from 2019 to today. It is important to highlight the critical need for additional authentication systems to guarantee customer trust and the integrity of financial data in the region.**

***Index Terms*—Computer Security, Authentication, Banking Applications, Latin America, Multi-factor Authentication.**

I. Introduction

As smart devices have become commonly used to access internet banking applications, these devices constitute appealing targets for fraudsters [1].The mobile money system (MMS) makes it possible to render diversified services at affordable costs to remote areas and low-income people [2]. In our current context of the growing adoption of financial technologies and rapid digital transformation in Latin America, cybersecurity, particularly authentication in banking applications, has become a critical issue to ensure the integrity and confidentiality of users' financial data.

According to studies conducted in Peru by the newspaper El Peruano [3], 69% of citizens use mobile banking exclusively for transactions or account review. The relevance of this topic is supported by recent developments in the region, such as the implementation of digital wallets like Apple PAY in Peru [4], dual-factor authentication projects [5], and the growth of digital banking in countries like Peru. The rapid adoption of smartphones that comes with in-built biometric fingerprint sensors can enhance mobile money authentication [6]

Cybersecurity is a growing concern in the Latin American banking sector. With the proliferation of mobile banking applications, ensuring the protection of financial data through reliable user authentication has become essential.

However, the current situation presents significant challenges, characterized by vulnerability to attacks, lack of robust authentication, and a lack of coordination in cybersecurity throughout the region. According to research by DPL New [7], 1,188 complaints of computer fraud and identity theft were investigated.

To secure Internet banking activities and maintain the trust and confidence of customers, numerous banks have adopted technical countermeasures, such as two-factor or multi-factor authentication, to prevent cyberattacks, online fraud, and unauthorized access to bank accounts [8].

The desired situation would involve a highly secure environment for banking applications, well-informed users about risks and best practices, and strict compliance with cybersecurity regulations. The security in the cloud authentication server remains vulnerable to the results of threat in JP Morgan Data breach in 2014, Capital One Data Breach in 2019, and manymore cloud server attacks over and over again. These attacks necessitate the demand for a strong framework for authentication to secure from any class of threat [9].

This is essential for the protection of financial data and customer trust in the banking system in Latin America. Hence, the implementation of additional authentication systems in mobile banking applications becomes an urgent need to ensure the protection of customer financial data. An effective authentication System is necessary to avoid financial loss and reputation damage through fraud, identity theft, disclosure of customer information, corruption of data, or unenforceable agreements [10]

Supported by Universidad Tecnología del Perú (UTP)

The motivation behind this research lies in the urgent need to address cybersecurity challenges in the Latin American banking sector due to the high incidence of reported computer fraud and impersonation. Additionally, it is crucial to provide a comprehensive framework for informed decision-making by the financial industry, regulators, and the academic community.

Many researchers have been proposed various models for the online user access authentication for the banking industry. Most of the researches are based on traditional the form of username and password, but with the varying mechanism of password forms [11].

However, they are often considered insufficient to achieve an adequate level of security and their use exposes users to several threats [12]. This systematic literature review aims to fill that knowledge gap and offer an updated and comprehensive perspective on authentication security in banking applications in Latin America. Furthermore, it seeks to provide a solid foundation for identifying emerging trends and areas of improvement in the field of digital financial security in the region.

The main objective of this systematic literature review (SLR) is to analyze and synthesize the current state of knowledge about information security focused on authentication systems in banking applications in Latin America, identifying trends, gaps, and research opportunities.

Additionally, it aims to provide relevant stakeholders in the region with a valuable resource for decision-making and the development of more effective solutions in this constantly evolving field.

In this regard, the study will be organized into sections addressing key aspects of information security in banking applications in Latin America, including authentication methods used, specific challenges in the region, identified trends, and best practices.

These sections will be presented clearly and structured to facilitate understanding and application of the results. Section 2, Methodology, details the approach used to conduct the SLR, from formulating research questions to the specific investigations that led to the selection of material discussed in this document.

Section 3, Results, serves as the space where findings obtained after a comprehensive analysis of primary works are systematically presented and organized. The results are articulated from a perspective focused on developed technologies, particularly highlighting those that merge hybrid models, integrating both symbolic and non-symbolic logic.

Section 4, Discussion, provides a platform for critical and reflective analysis of the selected sources and technologies. It offers an overview of the technologies and techniques used for user authentication in banking applications in Latin America, providing interpretation criteria covering the state of the art, current perspectives, and limitations identified during the investigative process.

Finally, Section 5, Conclusions, serves as a synthesis point for the main findings and limitations derived from this SLR. It offers guidance for future research, indicating possible directions that could deepen and broaden the understanding in the field of study on authentication techniques in banking applications in Latin America. This structural design provides a clear guide for reading and comprehensive understanding of the report.

II. Methods

In the SLR section, a specific structure was followed to ensure clarity and consistency in the presentation of the methods used in the research. The following will describe how the different aspects of this section were developed.

First, the search strategy that would be used to carry out this SLR was established. In this sense, the type of review performed was clearly defined, which in this case was a systematic review, with the inclusion of a meta-analysis. For the formulation of the search strategy, the PICO approach (Population / problem, Intervention, Comparison, Outcomes and Context) was used to delimit the search criteria, this will be of vital importance for the development of the SLR research work since according to TUTFG [13], states that these questions are used in systematic review works and in medical science careers, since they focus on patients or problems to be solved.

The PICO question was formulated as follows: ”What authentication techniques are used to ensure the level of security in applications for banking entities in Latin America?”. The selected keywords were included in the search equation used in two main databases: SCOPUS and Google SCHOLAR.

The following search formulas were used: ”(”BANKING APLICATIONS”) AND (”AUTHENTICATION TECHNIQUES” OR ”TRADITIONAL TECHNIQUES” OR AUTHENTICATION) OR (”Security LEVELS” OR RELIABILITY) AND (”Digital BANKING” OR ”LATIN AMERICA” OR ”South America” OR ”BANKING”)” and ”biometric authentication banking applications”.

Clear criteria were established for article selection, and articles were assigned a nomenclature for identification (IC for inclusion criteria and EC for exclusion criteria). Inclusion criteria were based on accessibility of open access articles, minimum citation, age less than 5 years, and relevance to

SLR research objectives. In contrast, exclusion criteria were applied to articles that did not meet these requirements.

Likewise, the study selection process was carried out following the PRISMA guidelines. It should be noted that, according to a Spanish journal [14], PRISMA helps authors of systematic reviews to transparently document why the review was conducted, what the authors did and what they found. In this regard, we report the total number of results obtained in the SCOPUS and Google SCHOLAR databases, which totaled 150 records. No duplicate articles were found at this stage. We then proceeded to review the title, abstract and keywords of the records and identified 145 articles that complied with the SLR subject matter.

Subsequently, 40 full-text articles were retrieved for a more detailed review. Of these, 5 were excluded according to the previously established criteria, resulting in 35 full-text studies analyzed. Finally, 20 studies that met the inclusion and exclusion criteria were selected for inclusion in the systematic review.

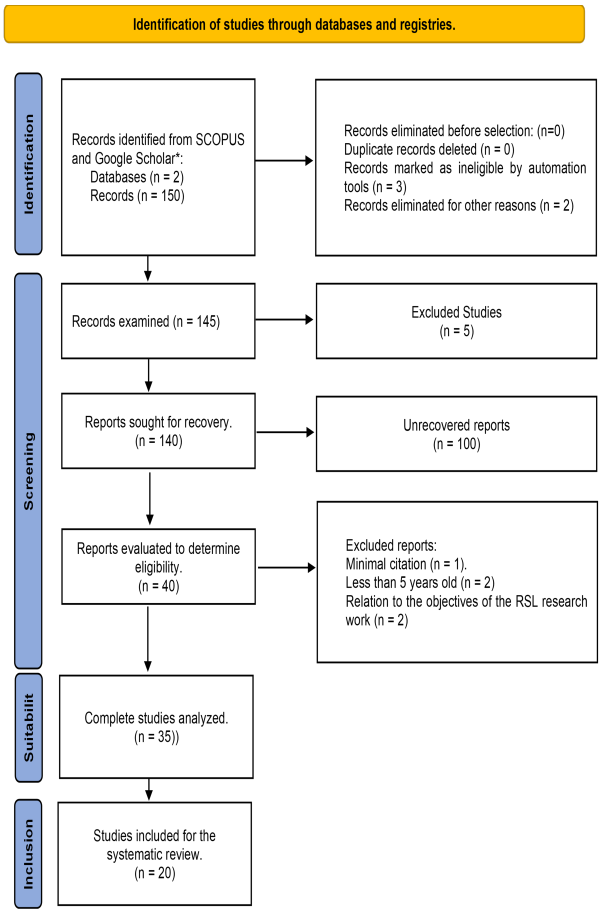

Fig. 1: PRISMA flow chart

III. Results

The comprehensive analysis of the various research papers yielded relevant results in multiple areas. They focus on different authentication techniques, including the implementation of authentication microservices, the use of biometrics for authentication, the importance of multifactor authentication, and the implementation of biometric authentication. The main results of the research work on authentication techniques can be summarized as follows:

- Implementation of authentication microservices: Authentication microservices are a way of implementing authentication that offers several advantages, such as scalability, flexibility, and ease of maintenance. Research work has shown that authentication microservices can be an effective way to implement authentication in mobile banking applications.

- Use of biometrics for authentication: Biometrics is a form of authentication that relies on physical or behavioral characteristics of the user. Biometric systems are playing a key role in the multitude of applications and placed at the center of debate in the scientific research community [15].

- Importance of multi-factor authentication: Multi-factor authentication (MFA) is a form of authentication that requires the user to provide two or more authentication factors to access a system. Research work has shown that MFA can be an effective way to reduce the risk of unauthorized access to systems.

- Implementation of token authentication: Token authentication can be an effective way to provide a secure and efficient user experience in applications. Research has shown that token authentication can be used to provide a secure and efficient way to perform transactions and queries.

Table I below shows the comparison between the different authentication techniques considered in the research papers. It is worth mentioning that the accuracy metric was calculated for each paper with its own research methodology.

It can be seen that it shows the five most common authentication techniques in research, each with its own advantages and disadvantages. Passwords are the easiest technique to implement and use, but they are also the easiest to crack. Biometric authentication is very secure, but can be intrusive for some users. Knowledge and possession factors are easy to use, but can be forgotten or lost. MFA is the most secure technique, but can be complex to implement and use. Also, Fig. 2 shows the level of use of techniques used from 2019 to 2023.

TABLE I: Comparison of authentication methods.

Technique	Description	Advantages	Disadvantages	Metric
Password	The user provides a combination of alphanumeric characters to identify themselves.	Easy to implement and use.	Easy to decipher.	Implementation of a 75% accurate authentication microservice [16]. Implementation of alphanumeric passwords with 87% accuracy [17]. Passwords based on a set of rules established by the financial institution. With an accuracy of 94% [18].
Biometric factor	The user provides a unique physical or behavioral characteristic to identify themselves.	Highly secure.	It can be intrusive.	Facial biometry application and had a result of 67% [19]. Application of fingerprint biometrics with a success rate of 69.8% [20]. Use of ocular biometry technique with a success rate of 79.7% [21].
Knowledge factor	The user provides information that only he or she knows to identify himself.	Easy to use.	May be forgotten	Development of security questions with an accuracy rate of 75% [22]. Development of security responses with 97% accuracy rate [23]. Development of answers to randomly generated security questions with an accuracy rate of 76.4% [24].
Factor per token	The user provides a device or token that they possess to identify themselves.	It cannot be deciphered.	It may be lost or stolen.	Physical token development with an accuracy rate of 76% [25]. Development of SMS authentication with an accuracy rate of 91% [26]. Digital token authentication with an accuracy rate of 85% [27].
Multi-factor authentication (MFA)	The user provides two or more authentication factors to identify themselves.	Highly secure.	Can be complex to implement and use.	Password development with a physical token with 99% accuracy rate [28]. Implementation of password with facial biometrics with 97% success rate [29]. Implementation of password and SMS authentication with an accuracy rate of 96% [30].

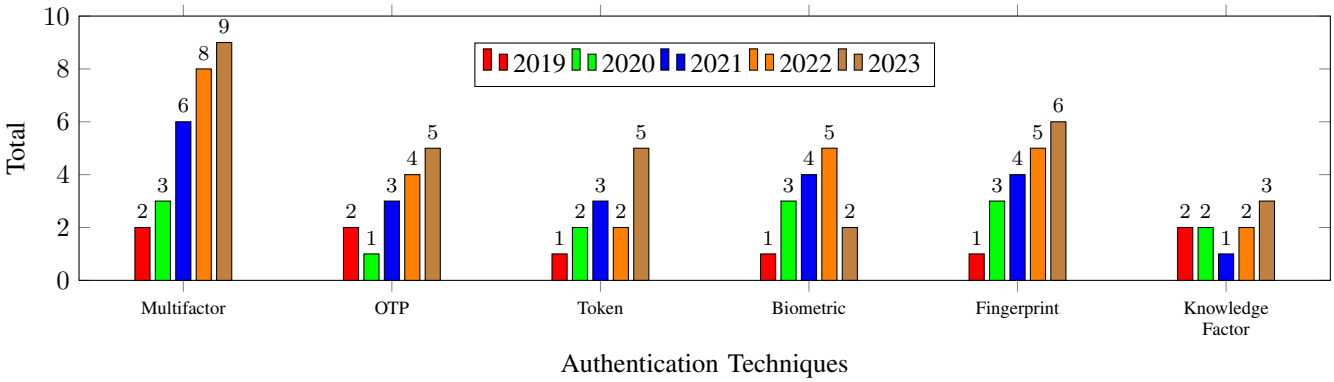

Fig. 2: Level of use of authentication techniques used from 2019 to the present

There has been a significant shift in the preference and adoption of authentication methods over the years. While password authentication has traditionally been the most widely used, the data reveals a clear increase in the popularity of biometrics and multi-factor authentication. These trends suggest a growing awareness of the need to strengthen security and improve the user experience.

In particular, multifactor authentication shows a steady increase from 2 in 2019 to 9 in 2023, evidencing a transition to more secure practices. Likewise, biometric authentication experiences a significant increase from 1 in 2019 to 5 in 2022, demonstrating its growing acceptance. This shift in preferences reflects the evolution of authentication techniques to adapt to contemporary demands for security and convenience in various applications, including virtual reality.

The steady increase in the adoption of more advanced methods highlights a clear trend towards the search for solutions that provide both a higher level of security and a better user experience.

Also, in the specific context of financial environments,

the rising adoption curve of multi-factor authentication is a crucial indicator of the evolution of transaction security. The Table reveals a remarkable increase in the implementation of multi-factor authentication over the years.

This trend reflects a proactive response to the rise of cyber threats in the financial sector. By incorporating additional layers of authentication, such as combining passwords with physical tokens or biometrics, financial institutions seek to strengthen their defenses against unauthorized access and fraud.

This approach is especially relevant in an environment where the protection of sensitive financial data is of paramount importance. The steady growth of multi-factor authentication demonstrates the adaptability of financial institutions to embrace more advanced technologies, prioritizing user security and the integrity of online transactions.

This shift also reinforces the idea that multifactor authentication is not only an essential measure but also a strategic investment in safeguarding user trust in the financial sphere.

In conclusion, the graph shows that multifactor authentication is the authentication method that has gained the most popularity in recent years, as it is the most secure authentication technique to date due to the fact that it combines different authentication techniques, which favors the identification of the person who wishes to log in to mobile banking applications.

In addition, Table II presents a qualitative and quantitative description of the authentication techniques found in the systematic literature review (SLR). The quantitative value calculation was calculated based on the research papers in Table I:

TABLE II: Qualitative and quantitative description of authentication techniques in Latin America

Technique	Qualitative	Quantitative
Multi-factor authentication	Provides an additional level of security that can help protect users' financial data. It is an essential security measure for financial environments.	Average success rate of 97.9%.
ONE-TIME PASSWORD (OTP)	It is a two-factor authentication method that uses a one-time code sent by SMS or generated by a mobile application. It is a secure and efficient authentication method.	Average success rate of 69.9%.
Token authentication	It is a two-factor authentication method that uses a physical or virtual token. It is a secure and efficient authentication method.	Average success rate of 78.9%.
Authentication by biometrics	An authentication method that uses a user's physical or behavioral characteristics. It is a secure and efficient authentication method.	Average success rate of 85.9%.
Fingerprint authentication	A type of biometric authentication that uses a user's fingerprints. It is a secure and efficient authentication method.	Average success rate of 79.9%.
Knowledge factor	An authentication method that requires the user to provide information that only the user knows. It is a simple and easy to use authentication method.	Average success of 58%.

In the Table II shows that multi-factor authentication is the most secure authentication method, with an average success rate of 97.9%. This is because it requires the user to provide two or more authentication factors, which makes it more difficult for an attacker to gain unauthorized access. Two-factor authentication methods, such as one-time password (OTP) and token authentication, are also very secure, with average success rates of 69.9% and 78.9%, respectively.

These methods require the user to provide a knowledge factor, such as a password, along with an additional factor, such as a one-time code or token. Biometric authentication, such as a fingerprint, is another secure authentication method, with an average success rate of 85.9%. This method requires the user to provide a unique physical characteristic, such as a fingerprint or face, to authenticate. It is also important to note that multifactor authentication is not only presented as an additional layer of security but also as an essential measure for financial environments. The need to protect users' financial data is reflected in the choice of highly secure methods such as multifactor authentication and biometric authentication. These techniques not only offer increased security, but also

indicate a proactive response by financial institutions to adapt to growing cyber threats. The combination of success rate and essential quality in financial environments underscores the critical importance of multifactor authentication in the digital and financial security landscape.

Also, taking into account that multifactor authentication is the most secure authentication method, Table III shows the considerations taken into account by the different research works that highlighted the importance of the development of multifactor authentication in a banking environment.

TABLE III: Description of considerations for research using multifactor authentication technique.

Considerations	Description
Methodology	The user provides two or more authentication factors to identify himself [28].
Security	Highly secure [29].
Implementation Complexity	Can be complex to implement and use [5].
Importance in Financial Environments	Provides an additional level of security that helps protect users' financial data. It is an essential security measure for financial environments [5].
Enterprise Implementation	Enhances transaction security. Requires user education for proper use. Increases complexity for attackers [30]..
User Experience Aspects	Increased friction in user experience [30].

Multi-factor authentication (MFA) stands out as a highly secure strategy, where the user provides two or more authentication factors for identification. Although it can present some complexity in its implementation and use, its importance in financial environments is undeniable. By offering an additional level of security, MFA proves to be an essential measure to protect users' financial data, significantly improving the security of transactions and increasing the complexity for potential attackers.

Its enterprise implementation not only reinforces transaction security, but also highlights the need to educate users on its correct use. Although it may generate an increase in friction in the user experience, MFA is presented as a fundamental component to guarantee the integrity and confidentiality of financial operations.

On the other hand, in the framework of the thorough review of the research work developed by García [19] and Gómez [21], the use of DATASETS for its development stands out. In both cases, ocular and facial biometrics required data collection to carry out the work and implementation of the projects. The use of DATASETS was a very important practice in the development of the banking applications of the research works in question, since they allowed training machine learning models that are capable of recognizing patterns in biometric data.

IV. Discussions

The research conducted provides an essential perspective on cybersecurity in the Latin American banking sector. The proliferation of mobile banking applications has transformed the way users interact with their financial services, but at the same time, it has expanded the attack surface for potential cyber threats. The lack of robust authentication emerges as a critical point, highlighting the urgent need for effective strategies to ensure the integrity and confidentiality of users' financial information.

In this context, the implementation of additional authentication systems emerges as an unavoidable necessity. The systematic review highlights that multifactor authentication, with its average success rate of 97.9%, positions itself as the most secure technique. This finding suggests that the combination of different authentication methods, such as biometrics, tokens, and knowledge factors, provides an additional layer of security crucial in the financial environment. The lower success rate associated with knowledge factor authentication, at 58%, underscores the importance of advancing towards more robust and less susceptible-to-attacks methods.

The upward trend in the use of biometrics and multifactor authentication from 2019 to the present reveals a proactive response from financial institutions to the growing cyber threats. This shift towards more advanced methods reflects the industry's adaptability to address emerging challenges and adopt innovative technologies that strengthen the security of banking applications.

It is essential to emphasize that the systematic review not only provides a retrospective analysis but also a solid foundation for future decision-making. Identifying areas for improvement and emerging trends in digital financial security in Latin America allows the industry and the academic community to be prepared for evolving challenges. The expanded discussion here reinforces the urgency of continuous investments in advanced authentication technologies and the need for coordinated cybersecurity collaboration throughout the region.

V. Conclusions

In conclusion, cybersecurity in the context of banking applications in Latin America poses a critical challenge that requires immediate attention. The growing reliance on mobile applications to access financial services has exposed users to an increased risk of cyber attacks, underscoring the importance of implementing robust and additional authentication strategies. The lack of coordination in cybersecurity in the region adds an additional layer of complexity to this scenario, highlighting the need for closer

collaboration between financial institutions and regulators.

The methodology applied in this systematic review, based on the PICO strategy and following PRISMA guidelines, provides a clear and rigorous approach to addressing the research question. The inclusion of 150 articles from 2019 to 2023, with a final selection of 20 articles, ensures the representativeness and currency of the review. This meticulous process offers a solid foundation for informed decision-making in both the financial industry and the academic community.

The results obtained, highlighting various authentication techniques used in Latin American banking applications, are crucial for understanding the current dynamics of security. Multifactor authentication emerges as the most secure technique, with an average success rate of 97.9%, while knowledge factor authentication proves to be the least secure, with an average success rate of 58%. These statistics underscore the need to abandon less secure methods and more extensively adopt advanced techniques, such as biometrics.

The trends identified in the increasing use of biometrics and multifactor authentication from 2019 to the present suggest a positive and proactive response from the financial industry. However, it is clear that the region still faces a significant path to ensure customer trust and the integrity of financial data. The critical need for additional authentication systems is presented as an unavoidable imperative, and the systematic review provides a roadmap for identifying areas of improvement and research opportunities in this direction.

The application of multifactor authentication in Latin American banking applications is the best option to implement, as highly secure authentication techniques can be combined to prevent any form of entity impersonation in the login process.

Thanks to the Systematic Review, we can understand that while the rest of the world shows a greater investment in advanced technologies and a more consolidated collaboration in the fight against cyber threats, Latin America still faces challenges such as underdeveloped technological infrastructure and the need to strengthen awareness and training in cybersecurity to mitigate risks and protect financial stability.

Ultimately, addressing the challenges of cybersecurity in Latin American banking is not only a responsibility of financial institutions but also a priority for regulators and the academic community. The systematic review leaves us with the certainty that continuous innovation in authentication techniques, collaboration among stakeholders, and constant awareness of emerging threats are fundamental to ensuring robust and reliable digital financial security in the region.

ACKNOWLEDGMENT

We are especially grateful to the "Universidad Tecnológica del Perú (UTP)", which has provided us with the conducive environment to conduct this research. The vibrant classrooms, libraries, private rooms and rich culture have enriched our experience, providing us with a unique perspective to address the challenges posed.

We would like to acknowledge and thank those experts and scholars whose work formed the basis of our systematic literature review. Their dedication to the generation and dissemination of knowledge has been essential to the advancement of our understanding in the field of computer security. To the citizens of Latin America, whose growing adoption of financial technologies has highlighted the importance of addressing security challenges. This dedication is made in the hope of contributing to a future where trust in banking applications is a fundamental point in building a robust digital society.

REFERENCES

[1] R. A. D. G. W. J. R. Estrela, P.M.A.B.; Albuquerque, "A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications," Master's thesis, 2021. [Online]. Available: https://doi.org/10.3390/s21124212

[2] M. E. S. A. Ali, G.; Ally Dida, "Two-factor authentication scheme for mobile money: A review of threat models and countermeasures," Master's thesis, 2020.

[3] "El 69% de los ciudadanos utiliza la banca móvil," *EL PERUANO*, 2022.

[4] D. N. R. Orestes, "Implementación de la billetera digital apple pay en perú para las tarjetas visa y mastercard en una institución financiera," Master's thesis, CYBERTESIS, Lima, 2022.

[5] A. I. E. Rosales and G. Y. R. Irias, "Proyecto de implementación de mecanismos de autenticación de doble factor en sistemas financieros en el banco central de honduras," Master's thesis, Universidad Tecnológica Centroamericana UNITEC, Tegucigalpa, 2019.

[6] M. E. S. A. Ali, G.; Dida, "A secure and efficient multi-factor authentication algorithm for mobile money applications," Master's thesis, 2021. [Online]. Available: https://doi.org/10.3390/fi13120299

[7] "Perú — fraudes en aplicaciones bancarias: la otra 'pandemia' que tomó fuerza durante la covid-19," *DPL News*, 2022.

[8] S. P. Tsai, CH., "The application of multi-server authentication scheme in internet banking transaction environments," Master's thesis, 2021. [Online]. Available: https://doi.org/10.1007/s10257-020-00481-5

[9] D. Prabakaran and S. Ramachandran, "Multi-factor authentication for secured financial transactions in cloud environment," Master's thesis, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:239660642

[10] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, "Online authentication methods used in banks and attacks against these methods," Master's thesis, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919306167

[11] W. A. Hammood, R. Abdullah, O. A. Hammood, S. M. Asmara, M. A. Al-Sharafi, and A. M. Hasan, "A review of user authentication model for online banking system based on mobile imei number," Master's thesis, 2020. [Online]. Available: https://dx.doi.org/10.1088/1757-899X/769/1/012061

[12] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, "A survey on multi-factor authentication for online banking in the wild," Master's thesis, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404820300316

[13] (2023) Preguntas pico: ¿qué son y cómo formularlas? [Último acceso: 11 10 2023]. [Online]. Available: https://tutfg.es/preguntas-pico/

[14] "Declaración prisma 2020: una guía actualizada para la publicación de revisiones sistemáticas," *REVISTA ESPAÑOLA DE CARDIOLOGÍA*, 2020, [Último acceso: 11 10 2023]. [Online]. Available: https://www.revespcardiol.org/es-declaracion-prisma-2020-una-guia-articulo-S0300893221002748
[15] N.-S. . R. A. Bibi, K., "Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities," Master's thesis, 2020.
[16] A. A. Khan and A. S. Kumar, "A study of password strength and security," Master's thesis, Universidad de Nueva Delhi, Japan, 2020.
[17] B. S. Bhavesh, "The impact of password complexity on security," Master's thesis, Universidad de Patna, Patna, 2021.
[18] C. D. Kumar, "The effectiveness of password managers in improving security," Master's thesis, Universidad de Allahabad, Allahabad, 2022.
[19] E. F. Garcia, "The performance of biometric authentication systems," Master's thesis, Universidad de Sevilla, Sevilla, 2020.
[20] G. H. Hernandez, "The security of biometric authentication systems," Master's thesis, Universidad de Zaragoza, Zaragoza, 2021.
[21] I. J. Gomez, "The usability of biometric authentication systems," Master's thesis, Universidad de Valencia, Valencia, 2022.
[22] P. Q. Rao, "The effectiveness of knowledge-based authentication systems," Master's thesis, Universidad de Bangalore, Bangalore, 2020.
[23] R. S. Singh, "The security of knowledge-based authentication systems," Master's thesis, Universidad de Hyderabad, Hyderabad, 2021.
[24] S. U. Singh, "The usability of knowledge-based authentication systems," Master's thesis, Universidad de Pune, Pune, 2022.
[25] Y. Z. Wang, "The performance of possession-based authentication systems," Master's thesis, Universidad de Tsinghua, Pekín, 2020.
[26] C. E. Fan, "The security of possession-based authentication systems," Master's thesis, Universidad de Fudan, Shanghái, 2021.
[27] F. G. He, "The usability of possession-based authentication systems," Master's thesis, Universidad de Beihang, Pekín, 2022.
[28] A. A. Khan, "The effectiveness of multifactor authentication in improving security," Master's thesis, Universidad de Nueva Delhi, Delhi, 2020.
[29] G. H. Hernandez, "The security and usability of multifactor authentication systems," Master's thesis, Universidad de Zaragoza, Zaragoza, 2021.
[30] I. J. Gomez, "The impact of multifactor authentication on user experience," Master's thesis, Universidad de Valencia, Valencia, 2022.