UNIVERSIDAD NACIONAL DE SAN MARTIN

RCSI
https://revistas.unsm.edu.pe/index.php/rcsi
e-ISSN: 2709-992X

Original article
Articulo original
Jul-Dec, 2024

Mobile application for the attendance control of university professors with biometric authentication and geolocation verification

Aplicación móvil para el control de asistencia de docentes universitarios con autenticación biométrica y verificación de geolocalización

Montañez-Díaz, Bruno Adrián[1*]
García-Gutiérrez, Willy Francisco[1]
Prieto-Pastor, Raphael Andre[1]
Mendoza-De-los-Santos, Alberto[1]

[1]Faculty of Engineering, Universidad Nacional de Trujillo, Trujillo, Peru

Received: 25 Dec. 2023 | **Accepted:** 04 Mar. 2024 | **Published:** 10 Jul. 2024

Corresponding author*: t453300120@unitru.edu.pe

How to cite this article: Montañez-Díaz, B. A., García-Gutiérrez, W. F., Prieto- Pastor, R. A. & Mendoza-De-los-Santos, A. (2024). Mobile application for the attendance control of university professors with biometric authentication and geolocation verification . *Revista Científica de Sistemas e Informática, 4*(2), e647. https://doi.org/10.51252/rcsi.v4i2.647

ABSTRACT

The absence of an effective attendance recording system presents a formidable challenge for educators and educational institutions, leading to disruptions in class schedules, timetables, and apprehensions regarding faculty information security. This study proposes the development of a mobile application for teacher attendance management, integrating biometric authentication and geolocation verification to bolster security in the registration process. Evaluation of the application, conducted with 24 participants at the National University of Trujillo, underscores a 95% accuracy rate in biometric authentication and a notable reduction in registration time, averaging at 32.68 seconds. Moreover, survey results reflect a favorable perception of security among users, consolidating acceptance and trust in the implementation of this pioneering technological solution.

Keywords: Amazon Rekognition; geopositioning; fingerprint; smart identification; facial recognition

RESUMEN

La carencia de un sistema de registro de asistencias eficiente representa un desafío tanto para los educadores como para las instituciones educativas, generando disrupciones en la planificación de clases y sus horarios, así como inquietudes acerca de la seguridad de la información del personal docente. Este estudio propone el desarrollo de una aplicación móvil para el control de asistencias docentes, integrando autenticación biométrica y verificación de geolocalización para fortalecer la seguridad en el registro. La evaluación de la aplicación, realizada con 24 participantes en la Universidad Nacional de Trujillo, revela un 95% de precisión en la autenticación biométrica y una significativa reducción en el tiempo de registro, con un tiempo promedio de 32,68 segundos. Además, los resultados de una encuesta reflejan una percepción positiva en cuanto a la seguridad por parte de los usuarios, consolidando la aceptación y confianza en la implementación de esta innovadora solución tecnológica.

Palabras clave: Amazon Rekognition; geoposicionamiento; huella digital; identificación inteligente; reconocimiento facial

1. INTRODUCTION

Biometric authentication stands as a paradigm shift in the realm of digital identity verification, fundamentally altering conventional recognition methods. This security paradigm harnesses individuals' distinctive biological attributes to validate their identity, affirming their claimed identity with precision (Ammour et al., 2023). Its primary objective lies in the acquisition of biometric features, encompassing facial imaging, fingerprinting, and vocal recordings, enabling the discernment of concordance between the captured biometric data and the individual's biophysical markers (Kausar, 2020).

The inherent advantage of these security methodologies over conventional password systems lies in their reliance on intrinsic and immutable personal traits, obviating the need for memorization (Silvelo, 2019). Nonetheless, amidst an era characterized by heightened interconnectedness, the imperative for additional layers of security becomes apparent. This exigency finds fulfillment through the integration of geolocation verification protocols. Geolocation, denoting the process of pinpointing the precise spatial and temporal coordinates of a device endowed with this technology, boasts multifarious applications across diverse domains (Moral, 2021). Particularly noteworthy is its utility within professional or scholastic milieus, where it can supplant traditional attendance-recording mechanisms, exemplifying its efficacy in real-world scenarios.

The meticulous monitoring of daily attendance emerges as a pivotal practice in fostering optimal staff performance within both organizational and educational settings, albeit presenting challenges in efficiency, particularly amidst large employee cohorts and deficient registration infrastructures (Salvatierra, 2018). Within the academic domain, the vigilance over faculty attendance assumes paramount significance in the realm of academic governance. This undertaking transcends mere administrative exigencies, extending to the pivotal role it plays in guaranteeing educators' fulfillment of both pedagogical and administrative obligations, thereby safeguarding the caliber and coherence of the educational milieu.

Throughout history, educational institutions have relied upon conventional attendance control methodologies, encompassing manual sign-in sheets, administrative office registrations, and time clock systems. Despite their simplicity, these modalities are susceptible to inaccuracies and often prove inefficient in administering large staff cohorts. Torres (2019) underscores the inherent vulnerabilities of attendance registration systems overseen by designated personnel, exposing instances of alleged favoritism towards certain colleagues juxtaposed with perceived negligence towards others, thereby compromising the system's integrity and fostering discord within the institutional framework.

Within the precincts of the National University of Trujillo (UNT), the biometric-based attendance control system, predominantly reliant on fingerprint and facial recognition, grapples with a significant security conundrum. Despite the system's formidable architecture for logging individuals' ingress and egress, its deployment remains susceptible to the latent peril of compromising exceedingly sensitive data. Moreover, prevalent drawbacks afflict extant attendance systems, including protracted queues at registration terminals and challenges associated with device upkeep and maintenance, as elucidated by Soewito et al. (2016).

To tackle this issue with requisite prudence, a multifaceted strategy is imperative, one that harmonizes operational efficacy with the preservation of data integrity. Novoa et al. (2019) advocate for a remedy in the guise of a mobile application tailored to streamline attendance management for educators, leveraging geolocation data alongside biometric timekeeping functionalities. Similarly, Sulla (2022) has implemented a Biometric System utilizing mobile applications to oversee student attendance at the American Institute of Technology in Cusco, thereby showcasing the viability of such technological interventions in educational settings.

Nevertheless, ensuring the attendance of university faculty members necessitates the integration of an added layer of verification, specifically predicated on geolocation parameters. An exemplary illustration of

this approach is discernible in Valverde's initiative (2018), wherein a mobile application was devised to streamline the tracking of employees irrespective of their work hours or the stability of their internet connectivity. This innovation enables the seamless recording of their attendance throughout the workday, underscoring the efficacy of geolocation-based solutions in bolstering attendance management protocols.

In this context, the study is dedicated to crafting a mobile application tailored for the management of teacher attendance, wherein the integration of biometric authentication and geolocation verification stands as pillars to fortify the security of attendance records. Specific objectives include:

(i) Examining the authenticity of the biometric system during registration.

(ii) Measuring the efficiency of biometric authentication in this process.

(iii) Assessing users' perception of security after the implementation of the application.

2. MATERIALS AND METHODS

2.1. Study Space

The investigation transpired within the precincts of the National University of Trujillo (UNT), situated in the district of Trujillo, Province of Trujillo, within the department of La Libertad, Peru.

Employing a quantitative methodology, the research adhered to a pre-experimental design, a selection rationale underscored by the study's focus on a singular measurement, where evaluation occurs subsequent to the application of the experimental treatment or stimulus.

Initially, the target population comprised all UNT professors. However, for the pilot phase of the application, a non-probability convenience sampling strategy was embraced, enlisting UNT students who volunteered to partake in the study. The sample comprised 24 students hailing from diverse faculties and academic strata, thereby ensuring a heterogeneous representation of the student body.

The general hypothesis was that the implementation of a mobile application for the control of teaching attendance with biometric authentication and geolocation verification contributes significantly to the strengthening of security in the attendance registration process at the UNT.

The implementation of the mobile application was defined as the central stimulus of the research, while security in the attendance registration process was the study variable. To measure the dependent variable, three fundamental dimensions were considered.

First, authenticity was assessed, building on previous research emphasizing the need for biometric authentication to achieve accurate and sustainable identification over time, regardless of possible variations that may arise over time (Li et al., 2023).

Behind the scenes, the need for biometric authentication to be effective was emphasized. Having an efficient attendance tracking system in corporate and educational settings is essential (Sandhya et al., 2022). A biometric attendance system is highly effective, helping to minimize the time spent on administrative tasks (Bhat et al., 2020).

Finally, users' perception of security was explored. It was considered that perceived risk is a crucial factor that can negatively affect the acceptance of biometric technology (Balapour et al., 2020; Nakisa et al., 2023). Therefore, assessing the perceived security of the authentication system is necessary, as a secure system plays a critical role in building strong foundations of trust among users.

In this context, specific indicators were defined to quantify and evaluate the dimensions, as detailed in Table 1.

Table 1.
Assessed dimensions of the dependent variable

Variable	Dimension	Indicator
Security in the attendance registration process at UNT	Authenticity	Accuracy in biometric authentication
	Efficiency	Time in the registration process
	Perception of security	Trust in the privacy of information

Regarding data collection, 2 techniques were used: survey and non-experimental observation. The survey's implementation involved designing a questionnaire, previously validated by experts, based on the Likert scale. This questionnaire addressed four items that represent the four indicators of the security perception dimension. On the other hand, non-experimental observation allowed us to collect information from the records produced using the application, thus obtaining measures regarding the accuracy and effectiveness of authentication. The SPSS Statistics v27 tool was used to analyze the resulting data.

2.2. Software desing and development

For the software development process, the decision was made to adopt Scrum, an agile methodology renowned for its incremental and iterative approach. As Bhavsar et al. (2020) affirm, the judicious application of Scrum in software development endeavors fosters enhancements in productivity and product quality, along with its features.

In the developmental planning phase of the application, paramount consideration was given to fortifying security by incorporating biometric verification functionalities, encompassing both web authentication services and local device authentication. Additionally, the integration of geolocation was deliberated as an auxiliary security measure to ensure the teacher's presence within the university campus. Figure 1 offers a schematic representation of the flow of the teacher attendance recording process.

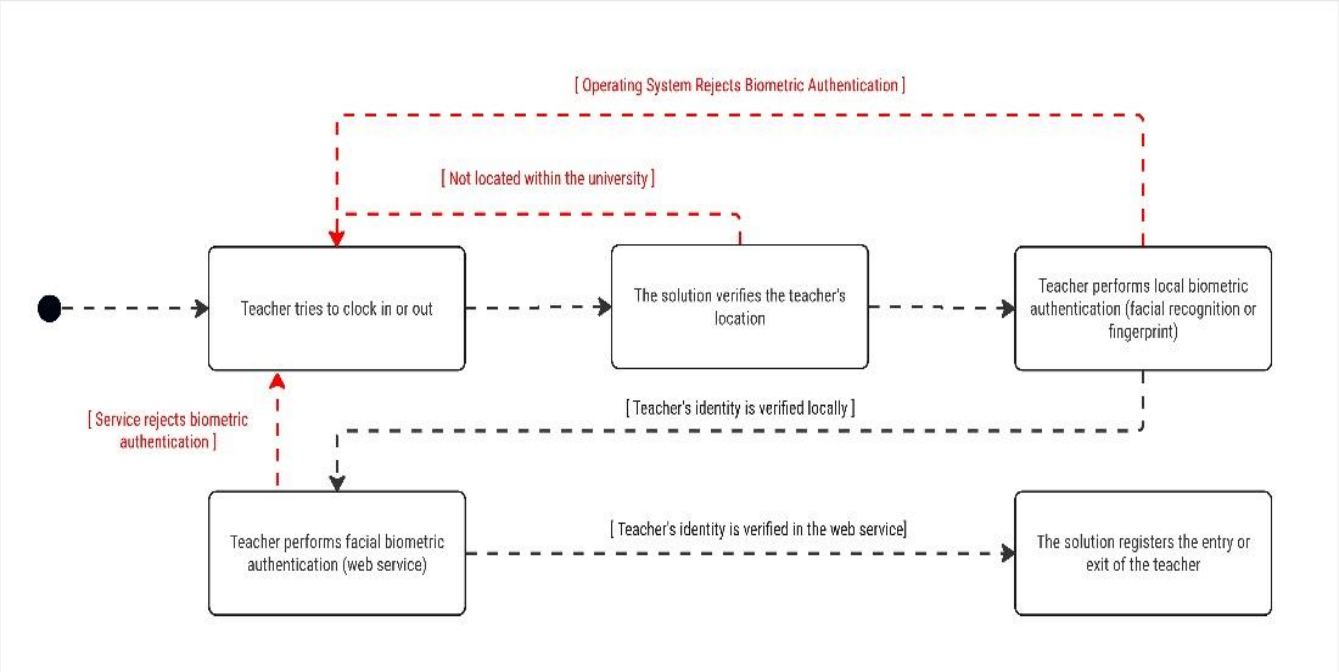

Figure 1. *Representation of the attendance control process in the proposed solution*

Considering the process involved, we proceeded to estimate the product backlog, which included a total of 3 sprints and 13 user stories. A duration of 36 days was projected for its execution, as evidenced in Table 2.

Table 2.
Estimated Project Product Backlog

#Sprint	#US	Description	Size	Points	Time [Days]
First Sprint	US1	Configure Flutter and Supabase development environment	S	2	1 1/2
	US2	Design the Login Screen UI	M	3	2
	US3	Implement Login Logic with Supabase	L	5	3
	US4	Integrate local_auth package for local biometric authentication into the mobile app	M	3	2
	US5	Integrate Google Maps for geolocation verification	L	5	3
Second Sprint	US6	Deploy Amazon Rekognition features to your web service	XL	8	5
	US7	Design and develop the app's user interface	XL	8	5
	US8	Design and develop the user interface of the web management platform	XL	8	5
	US9	Implement the manual administrator intervention functionality in the web management platform	L	5	2
Third Sprint	US10	Develop security policies to prevent unauthorized access in Supabase	M	3	2
	US11	Perform unit and integration testing on the mobile app and web service	L	5	3
	US12	Deploy the mobile app on iOS and Android platforms	S	2	1 1/2
	US13	Deploy the web management platform in a production environment	XS	1	1
Story Points / Estimated Time				**58**	**36**

Considering that, the solution focuses on building a mobile app by implementing Flutter, an open-source framework created by Google that makes it easy to build cross-platform apps from a single codebase (Flutter, 2023). This choice was underpinned by its prominent position as the most widely adopted multi-platform framework today (Lovrić et al., 2023). In addition to its renowned runtime efficiency, numerous evaluations have demonstrated outstanding performance in terms of CPU utilization (Wasilewski & Zabierowski, 2021). These factors were considered determining factors when selecting the tool for the development of the application.

In addition, a backend infrastructure was deployed using Supabase, which is a Backend as a Service (BaaS) platform. Supabase is an open-source platform that provides a wide range of services for application development, including database, authentication, storage, among others (Supabase, 2023). The so-called BaaS development approach allows developers to focus on the functionalities of the application, rather than focusing on the development of the complex backend infrastructure, by establishing connections with sophisticated Application Programming Interfaces (APIs) (Dudjak & Martinović, 2020).

A critical component of this application was the integration with Amazon Rekognition, a fully managed machine learning service that provides the core APIs to enable image and video analytics (Amazon, 2023). It makes it possible to identify objects, faces, text, scenes, and activities, providing a list of labels that describe the objects detected in images and videos (Leotta et al., 2023). Although large platforms such as Google, Azure, and Meta offer similar technologies, Amazon Rekognition stands out as the best in facial recognition and the interpretation of emotional expressions (Saadon et al., 2023).

The capabilities provided by Amazon Rekognition were leveraged through the development of a web service based on Node.js and Express. This service was implemented in a Platform as a Service (PaaS), in this case, Render, for deployment and operation. A PaaS is a cloud computing environment that offers

resources and tools for developing, deploying, and managing applications without the need to worry about the underlying infrastructure (Kounev et al., 2023).

Figure 2 outlines the architecture that was implemented to get the application up and running.

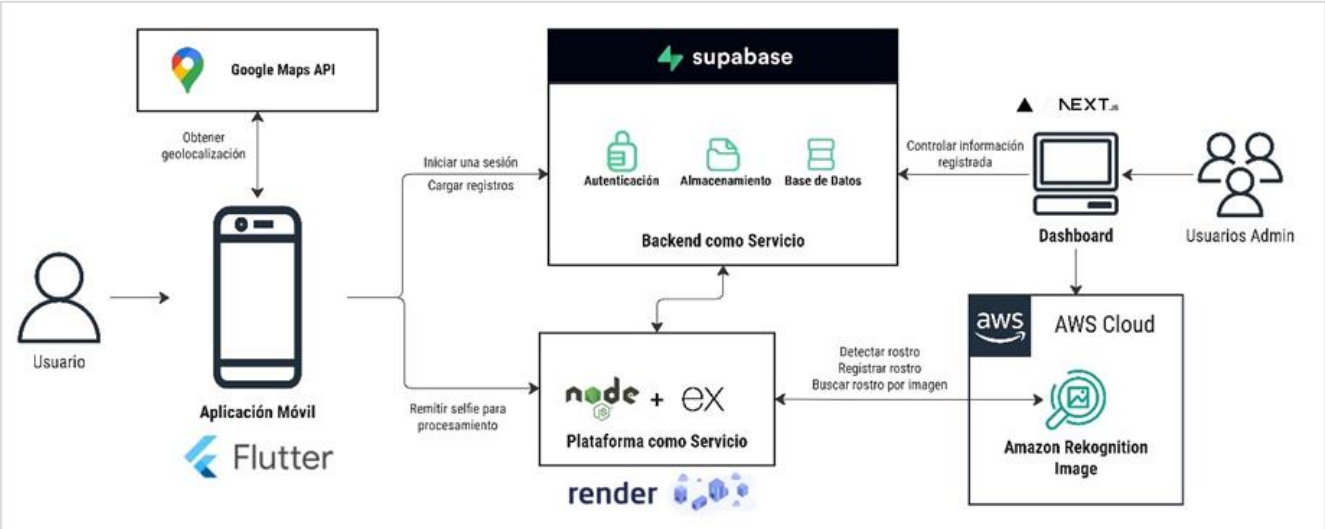

Figure 2. *Proposed Solution Architecture*

For geolocation verification, Google Maps technology was incorporated along with the google_maps_flutter package to access the maps and the precise location of the teacher. This ensured that attendance registration was only allowed when the teacher was on campus.

For local biometric authentication, Flutter's local_auth package was used. This feature allowed for effective biometric verification, depending on the biometric data recorded on the device, such as faces and fingerprints.

To perform biometric verification in the web service, both in registration and in facial biometric authentication, three functionalities provided by Amazon Rekognition were used (Figure 3).

First, the DetectFacesAPI was used to identify and analyze the faces in the submitted image, providing details such as the location and characteristics of the faces, as well as additional information about age, gender, and emotions. This data was used to perform certain quality validations that will be detailed later.

Second, the SearchFacesByImageAPI was leveraged to compare the faces in a reference image with the collection of previously registered faces, allowing verification of face matching. By making use of this functionality, you avoid registering a face that has already been indexed to the collection.

Finally, the IndexFacesAPI was used to perform the indexing of faces in the collection. Indexing involves registering the face in the form of a set of facial features in a collection. In this context, collections refer to organized sets of feature vectors depicting faces previously detected in images (Amazon, 2023).

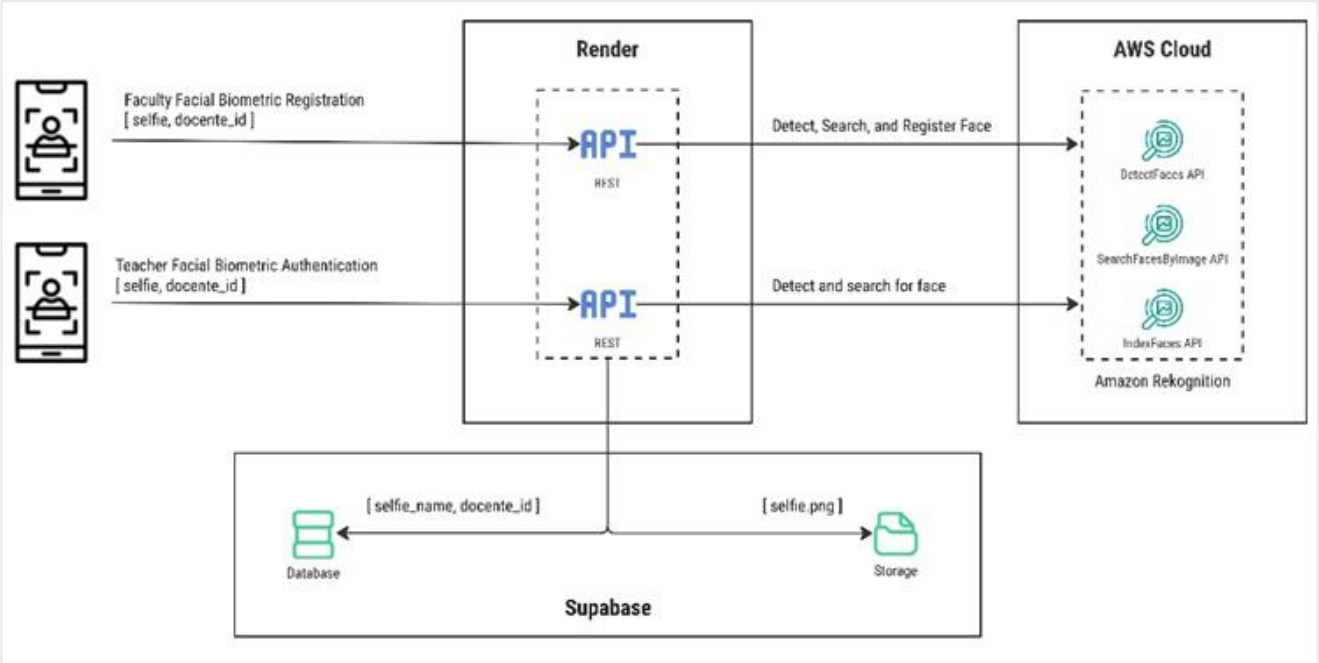

Figure 3. *Referential architecture for identity verification in the web service*

In the facial biometric registration process, a quality threshold must be exceeded, as illustrated in Figure 4. Among the data provided by DetectFacesAPI are confidence level, image quality (brightness and sharpness), presence of lenses or sunglasses, eye opening, mouth opening, relative face size relative to the image, emotion detection, orientation (tilt and swivel), and face position. Based on these criteria, a series of requirements were defined that determine whether the selfie is considered suitable for continuing with the process (Table 3).

Table 3.
Quality Rules for Face Detection in Registry

Rule	Value
Confidence Level	0.95
Face Width (%)	[50, 75]
Face Length (%)	[60, 90]
Displacement of the Face on the horizontal axis (%)	[45, 55]
Position of the Face on the Vertical Axis (%)	[30, 50]
Expected Excitement	Calmada
Tilt (°)	[-5, 5]
Side Orientation (°)	[-5, 5]
Lateral Tilt (°)	[-5, 5]
Minimal sharpness	70
Minimum Brightness	60
Sunglasses Allowed	No
Eyeglasses Allowed	No
Closed Mouth Required	Sí
Open Eyes Required	Sí

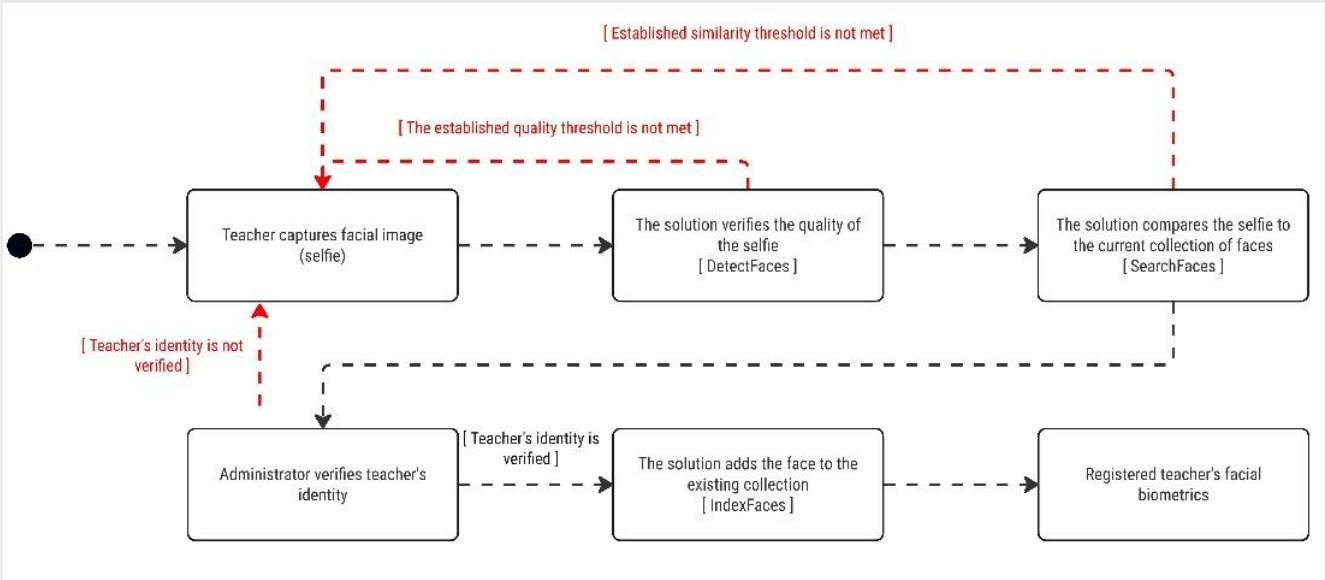

Figure 4. *Representative Flow of Teacher Facial Biometric Registration*

These rules were developed in compliance with the facial image requirements established in the ISO/IEC 19794-5 standard, which are detailed in Table 4. This standard establishes guidelines for facial imaging in biometric applications, addressing environmental constraints, photographic properties, digital attributes, and best practices for face photography (ISO/IEC 19794-5, 2005).

In addition, the decision was made to adhere to the guidelines set by the International Civil Aviation Organization for the capture of facial portraits in machine-readable travel documents. The production of high-quality, standardized portraits by enabling automated inspection of travel documents, which is closely related to facial recognition technology. Table 5 shows the requirements considered to establish the face detection rules in this solution. It should be noted that parameters such as the distance from one side to the center of the face were used to establish the minimum and maximum percentage position that appear in the rules already presented.

Table 4.

Quality requirements for facial imaging in ISO/IEC – 19794-5

Clause	Attribute	Restriction
Scene	Posture	Deflection control from the front end
	Lighting	Uniform illumination without shadows
	Bottom	Light, single-color background
	Eyes	Open and clearly visible
	Mouth	Closed and clearly visible
Photographic	Head Position	Focused
	Distance to camera	Moderate head size
	Color	Neutral color and no red eyes
	Exposition	Appropriate Brightness
Digital	Approach	No blur and with adequate sharpness
	Resolution	Head Width Restriction

Note: Adapted from Face Image Quality Evaluation for ISO/IEC Standards 19794-5 and 29794-5 (p. 234), by Sang et al, 2009, Springer Berlin / Heidelberg

Table 5.
Quality requirements for portraiture according to ICAO

Parameter	Restriction
Tilt of the head in relation to the front position	≥ – 5° ≤ + 5°
Lateral orientation of the head with respect to the frontal position	≥ – 5° ≤ + 5°
Lateral tilt of the head	≥ – 8° ≤ + 8°
Facial expression	**Neutral, no smile**
Width of the head relative to the image	≥ 50% ≤ 75%
Length of the head in relation to the image	≥ 60% ≤ 90%
Distance from the left side of the image to the center of the face	≥ 45% ≤ 55%
Distance from the top of the image to the center of the face	≥ 30% ≤ 50%

Note: Adapted from Portrait Quality Technical Report (Reference Facial Images for MRTD) (p. 41) by ISO/IEC JTC1 SC17 WG3, 2018, International Civil Aviation Organization

Once the selfie has passed the quality threshold, it undergoes a comparison process with the existing faces in the collection, where it must meet a predefined similarity threshold. This information is obtained through the result of SearcFacesByImageAPI. In this way, it was established that the level of similarity between faces should be 95%. Therefore, if the selfie sent exceeds that similarity threshold, the registration is rejected.

The next step involves the manual intervention of an administrator, who verifies the identity of the teacher. This is done to prevent the registration of unauthorized persons and to ensure the authenticity of the registrations. To this end, a web management platform was built where administrators have access to information from attendance records. This platform has been built using state-of-the-art web development technologies, such as NextJs, a full-stack JavaScript framework; TailwindCSS, a CSS framework; and Shadcn UI, a repository of components designed for TailwindCSS. In this way, the administrator examines the list of facial registration requests and proceeds to validate the teacher's identity.

Finally, after the three checks have been carried out, this process culminates with the registration of the face in the collection. To perform this operation, Amazon Rekognition's IndexFaces function is used. Once the face is successfully stored, a unique identifier is generated for that face. Using this identifier and the teacher identifier, a record is created in the Face Registration Requests table in Supabase. In addition, the selfie sent is saved in Supabase's storage system for future reference.

On the other hand, it was also essential to develop the logic for facial biometric authentication, which involves verifying the identity of a teacher who already has their face registered. This process follows a flow illustrated in Figure 5. As in the registration process, the selfie sent must exceed the defined quality threshold. In this case, a smaller set of rules have been established compared to the registration process, which is justified by the need to streamline verification and maintain an efficient process for already authorized teachers, without compromising security. These rules are detailed in Table 6.

Table 6.
Quality Rules for Face Detection in Authentication

Rule	Value
Confidence Level	0.95
Sunglasses Allowed	No
Eyeglasses Allowed	No
Open Eyes Required	Yes

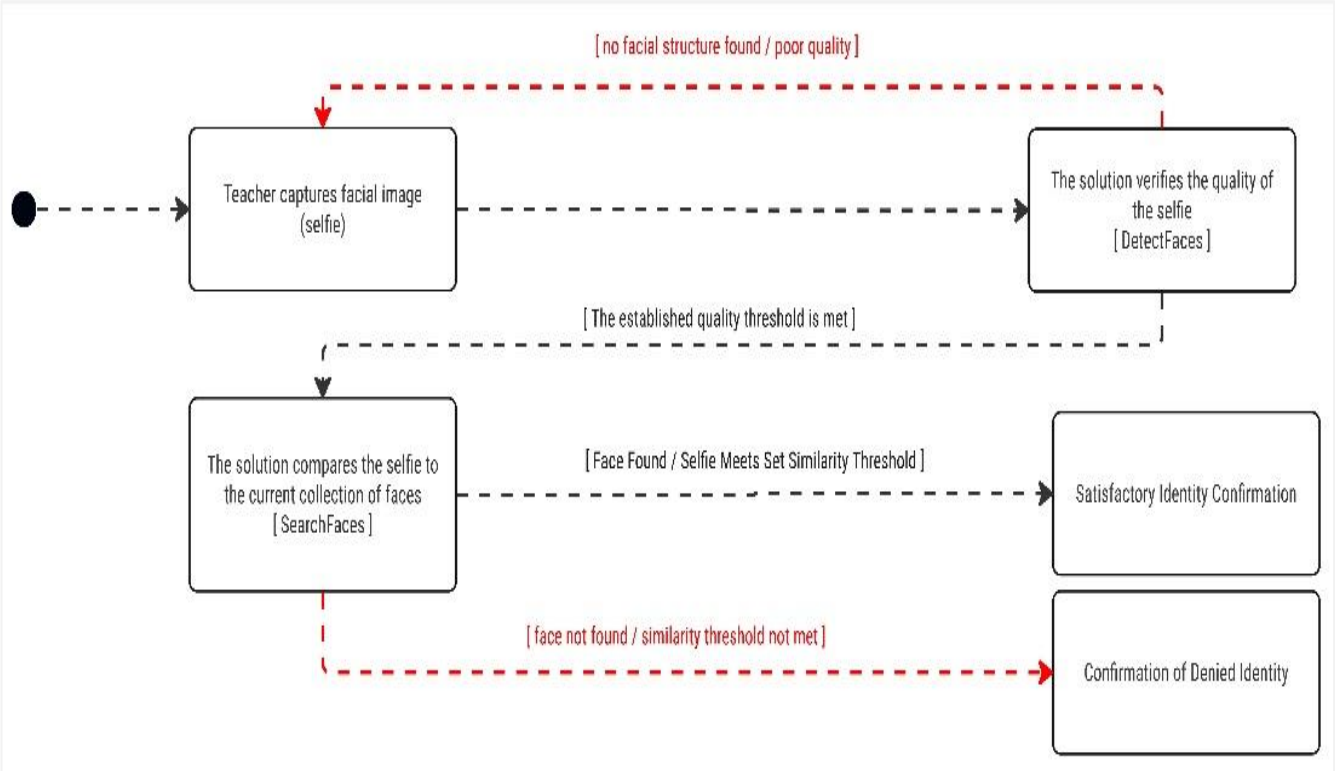

Figure 5. *Representative Flow of Teacher Facial Biometric Authentication*

After having successfully passed the quality threshold, the process continues with the evaluation of the percentage of similarity, which must be at least 95%. This criterion is essential to ensure high accuracy in biometric verification and avoid false positives. Finally, a biometric verification attempt record is generated, where the selfie of the attempt is saved in Supabase storage. This practice aligns with a security policy that was implemented in the backend, which states that if a user has attempted to perform biometric verification more than three times in the last five minutes, they will not be allowed to make any further attempts. This prevents unauthorized access and always ensures the integrity of the authentication process.

3. RESULTS AND DISCUSSION

Preceded by an exhaustive development phase, the prototype of the application resulted in the interface shown in Figure 6, where the screens of the attendance registration flow are presented, detailing each of the elements and functions available to the user. Subsequently, a pilot test was carried out to evaluate the operation of the mobile application with 24 students on the UNT campus, during the period between November 29, 2023, and December 17, 2023.

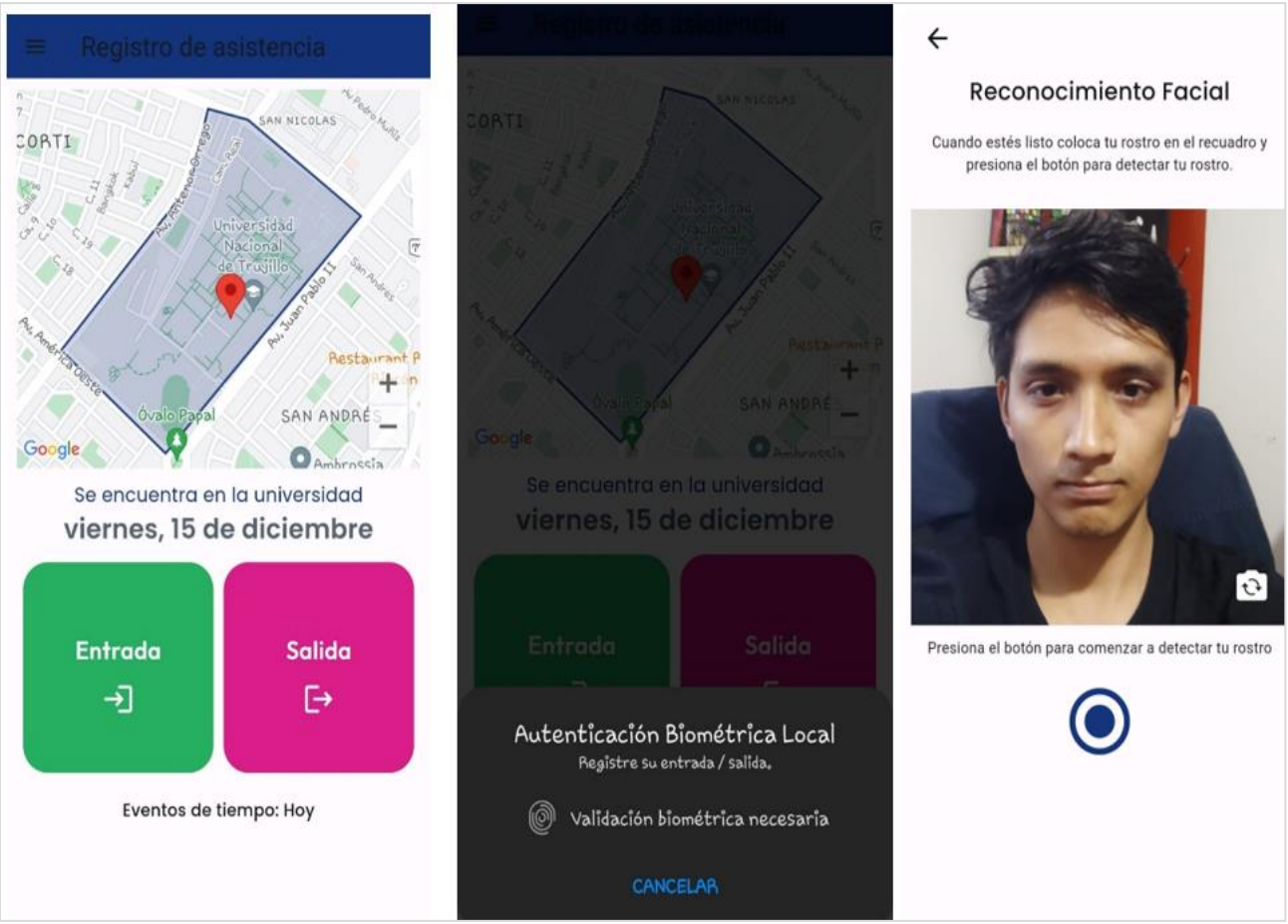

Figure 6. *Geolocation, local biometrics, and facial recognition verification interface*

3.1. Authenticity

During this timeframe, a total of 74 events were logged, denoting instances of users clocking in or out. Among these, 70 entries corresponded to attendance marks necessitating only a singular attempt at facial biometric verification, as delineated in Figure 7. This attests to the application's commendable accuracy, achieving a success rate of 95%, with the remaining 5% constituting failed attempts classified as false negatives. In a comparable experiment, Tee et al. (2020) evaluated their FaceAuth system with a cohort of 40 participants, achieving an accuracy rate of 92.5%. Contrasted with the proposed system, FaceAuth specializes in person identification sans reliance on internet connectivity, leveraging the k-nearest neighbors (k-NN) algorithm. However, this algorithm, while prevalent in facial recognition, encounters challenges in instances of partially obscured faces and typically exhibits an elevated rate of false negatives (Guo, 2021).

In contrast, the proposed attendance logging application employs deep learning algorithms facilitated by Amazon Rekognition. Unlike conventional machine learning approaches, deep learning dissects the process into multiple layers, with each layer tailored to discern specific features (Vardakis et al., 2022). Consequently, the utilization of deep learning algorithms underpins the heightened precision observed in the proposed application as compared to FaceAuth.

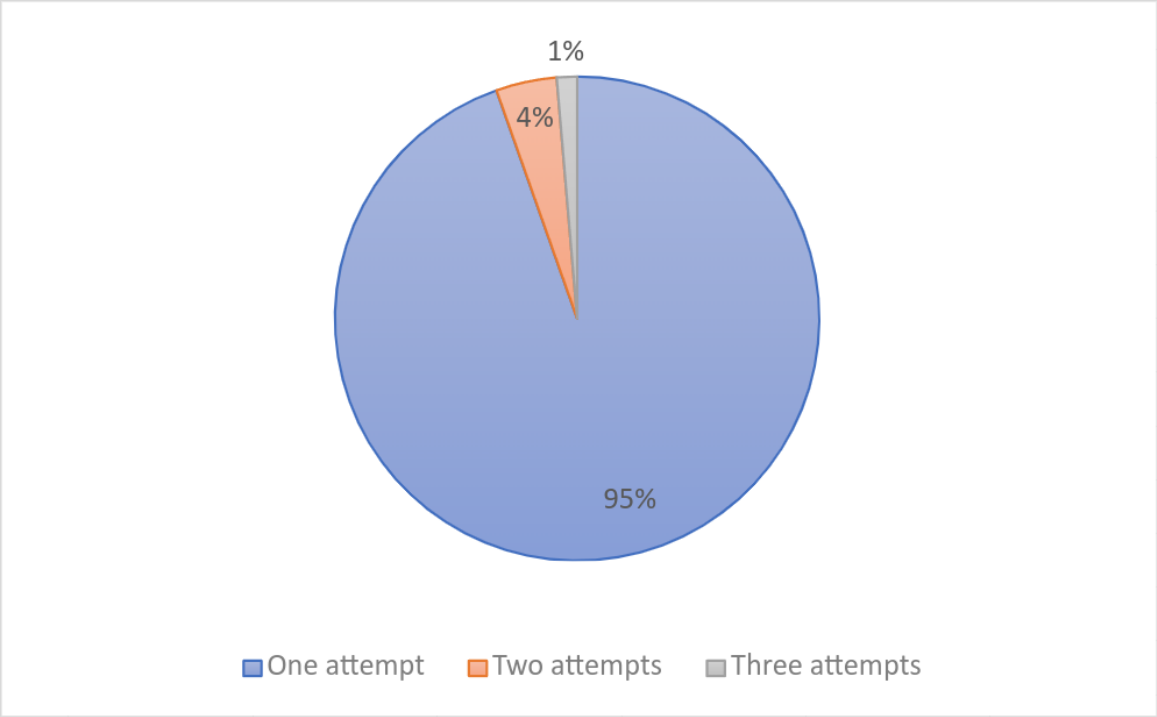

Figure 7. *Attempts by Registration to Achieve Successful Authentication*

3.2. Efficiency

Incorporated within each attendance record is a field denoting the duration in seconds required to finalize the process. To facilitate a more precise comparison, the analysis was restricted to successful authentications on the initial attempt, as multiple attempts typically entail prolonged durations, as illustrated in Figure 8. With a dataset comprising 70 records from single attempts, the Kolmogorov-Smirnov normality test was employed, deemed suitable for samples exceeding 50. The null hypothesis (Ho) posits that the records exhibit a normal distribution, while the alternative hypothesis (Ha) contends that the records deviate from a normal distribution.

Table 7.
Normality test - Kolmogorov-Smirnov

	Statistical	Gl	p
Process Time	0.081	70	0.2

As shown in Table 7, with a p-value of 0.2 in the Kolmogorov-Smirnov test, there is insufficient evidence to reject Ho. Therefore, normality can be assumed for the corresponding analysis.

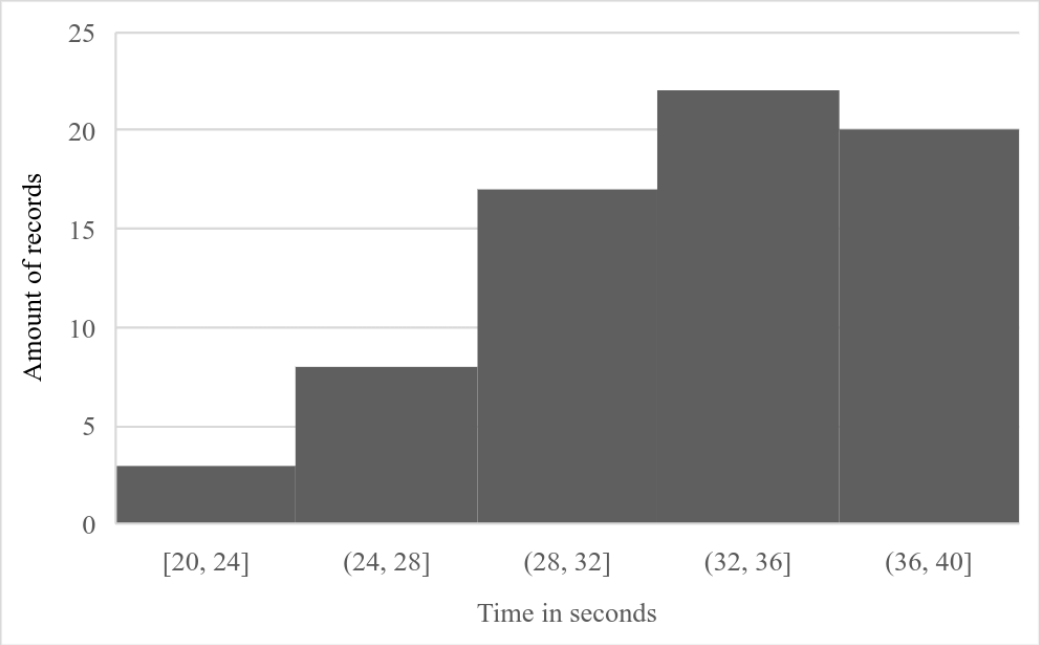

Figure 8. *Time spent in the attendance dialing process during first-attempt authentication*

The analysis of the results begins by introducing the ISO/IEC 25010 standard, which provides a clear definition of characteristics and sub-characteristics, establishing a coherent language for the description and evaluation of the quality of a software (ISO/IEC 25010, 2011). The usefulness of this model lies in its ability to address specific aspects, focusing on efficiency in measuring time.

Once the metrics have been quantified, the results are evaluated. In this context, ISO/IEC 25040:2011 provides a framework that sets out requirements and recommendations for software evaluation. This standard facilitates the definition of satisfaction criteria, aligned with the desired quality objectives (ISO/IEC 25040, 2011). As detailed in Table 8, four measurement ranges are presented, with values from 0 to 10, each with its respective score levels assigned to three degrees of satisfaction.

Table 8.

Measurement Ranges for Metrics

Measured value	Score Level	Degree of satisfaction
7.50 - 10	Meets the requirements	Very satisfactory
5 - 7.49	Acceptable	Satisfactory
2.51 - 4.99	Minimally acceptable	Unsatisfactory
0 - 2.50	Not acceptable	Unsatisfactory

In accordance with the standards outlined in both protocols, it is imperative to stipulate an anticipated value for each metric. In the study conducted by Zambrano-Vega et al. (2020), the bioFace attendance registration application for teachers, integrating geolocation verification and facial recognition, was introduced. Across a four-day testing phase, the average processing times were documented as follows: 1.74, 2, 1.56, and 1.75 minutes. The lowest benchmarked duration recorded was 1.56 minutes, equivalent to 93.6 seconds. The comparative assessment unfolds as follows: if the projected time (A) exceeds the obtained time (B), a score of 10 (X) is allotted; conversely, if B surpasses A, a score of 0 is designated.

Table 9.

Evaluation of the efficiency of the application in the attendance registration process

Feature	Metric	Goal	Formula A/B
	Task Time	<93.6	A = t. planned

Performance Efficiency						B = t. obtained A > B; 0 ; 10		
Data obtained								
A	**B**	**X**	**A**	**B**	**X**	**A**	**B**	**X**
31.997	93.6	10	29.841	93.6	10	30.726	93.6	10
35.009	93.6	10	34.653	93.6	10	31	93.6	10
33.874	93.6	10	38.326	93.6	10	36.333	93.6	10
35.982	93.6	10	39.735	93.6	10	33.348	93.6	10
34.587	93.6	10	26.899	93.6	10	30	93.6	10
39.090	93.6	10	37.374	93.6	10	33.1	93.6	10
32.853	93.6	10	39.243	93.6	10	38.665	93.6	10
30.873	93.6	10	33.014	93.6	10	36.771	93.6	10
33.354	93.6	10	31.1	93.6	10	34.099	93.6	10
32.857	93.6	10	33.906	93.6	10	36.862	93.6	10
38.030	93.6	10	33.232	93.6	10	31.489	93.6	10
24.201	93.6	10	31.222	93.6	10	35.449	93.6	10
23.010	93.6	10	32.484	93.6	10	26.482	93.6	10
20.235	93.6	10	38.892	93.6	10	31.015	93.6	10
36.457	93.6	10	30.598	93.6	10	28.126	93.6	10
26.317	93.6	10	36.354	93.6	10	20.283	93.6	10
38.739	93.6	10	37.951	93.6	10	26.284	93.6	10
30.690	93.6	10	33.828	93.6	10	38.524	93.6	10
26.089	93.6	10	28.239	93.6	10	39.086	93.6	10
34.537	93.6	10	27.035	93.6	10	30.915	93.6	10
34.125	93.6	10	34.228	93.6	10	37.856	93.6	10
32.396	93.6	10	30.019	93.6	10	27.7	93.6	10
31.826	93.6	10	36.52	93.6	10			
28.891	93.6	10	32.496	93.6	10			
Average Score						10		
Degree of satisfaction						Very satisfactory		

As depicted in Table 9, the outcomes uniformly portray positivity, with no recorded timestamps surpassing the anticipated duration. The average time elapsed for attendance recording amounts to 32.68 seconds. This suggests that, in terms of efficiency, the stipulated benchmarks have been adequately fulfilled. This outcome is predominantly credited to the facial recognition service employed. While bioFace leverages Microsoft Face API, the proposed application adopts Amazon Rekognition.

3.3. Perception of Safety

A reliability assessment of the survey findings yielded a Cronbach's alpha coefficient of 0.829. This value signifies robust internal consistency in evaluating perceived safety within the attendance registration application. While this coefficient slightly falls below the threshold of 0.80 documented in a prior study by Balapour et al. (2020) concerning security perception in mobile applications, it remains a notable indicator of internal consistency within the current research context.

Table 10.

Estadísticas de los ítems del cuestionario sobre percepción de seguridad

Items	Media	Some. Est.
I am confident that the private information (facial biometrics and geolocation) that I provided during my registration process with the app will only be stored on your system	4.71	0.464
I am concerned that inappropriate persons may be able to access the private information I provided during my interaction with the attendance registration app.	3.71	0.464
I am confident in the security of facial recognition operations in the attendance log.	4.71	0.550
The security policies in the attendance registration application are appropriate	4.67	0.565

As evidenced in Table 10, the statistics of the responses for each item reveal a positive trend, with the item related to concern about unauthorized access being the one with the lowest average. This perception is understandable, as the respondent is aware that, in the registration process, identity validation is carried out by an administrator on the management platform. To clarify this aspect, it is crucial to first highlight that access to the platform is restricted, requiring credentials for entry.

Second, the information that the administrator has access to is limited exclusively to the selfie sent, which is not even considered confidential. This practice contrasts with the approach of Aza & Rodriguez (2020), whose management dashboard displays images of scanned fingerprints, raising greater concern in case of unauthorized access to such information. In an analogous situation, UNT would face similar risks, as teachers' fingerprints would be left vulnerable if their biometric system were compromised by attackers.

In broad strokes, the application garners acclaim for its commendable robustness in security measures, albeit beset by a notable limitation that could potentially undermine this distinguishing attribute. This constraint pertains to the prerequisite for users to possess a mobile device endowed with facial or fingerprint recognition capabilities. Despite the increasing prevalence and accessibility of mobile devices, the seamless integration of facial authentication systems remains an ongoing evolution. It is imperative to underscore that, notwithstanding technological strides, certain devices still exhibit constraints (Padilha et al., 2020). Educators lacking contemporary devices or lacking these specific functionalities find themselves devoid of an additional layer of authentication, consequently heightening the susceptibility to fraudulent activities in attendance records.

Unquestionably, the intrinsic tethering of an authentication layer to the device's native technology is an incontrovertible reality. Nonetheless, the auxiliary layer of identity verification maintains optimal security, even on devices devoid of such features, owing to the incorporation of Amazon Rekognition. This platform, heralded as a benchmark in security paradigms, substantiates its efficacy by bestowing substantial benefits upon the attendance registration process. Attributes such as augmented security and heightened transparency have been empirically validated, bolstered by recent research elucidating their potential advantages in this domain (Kodali et al., 2023).

CONCLUSIONS

The results of this study indicate that the mobile application for the control of teacher attendance, which incorporates biometric authentication and geolocation verification at the National University of Trujillo, is a tool that strengthens security in the attendance registration process. A 95% accuracy rate has been observed in biometric authentication, there was a significant reduction in the time needed to complete the registration process, with an average of only 32.68 seconds, and the results of the applied survey reveal a positive perception of security by users. consolidating acceptance and confidence in the implementation of this technological solution.

Despite the limitation associated with reliance on facial or fingerprint recognition capabilities on devices, it is undeniable that the facial authentication provided by a service, in this case, Amazon Rekognition, proves to be more than adequate for secure and transparent support management. In the perspective of future research, the replication of the experiment with teachers and administrative staff is contemplated, given that, due to time constraints, it was not possible to include them on this occasion. It is also suggested to investigate the adoption of this technology in the attendance record of students, evaluating its impact on the quality and dynamism of classes.

FINANCING

The authors did not receive sponsorship to carry out this study-article.

CONFLICT OF INTEREST

There is no conflict of interest related to the subject matter of the work.

AUTHORSHIP CONTRIBUTION

Conceptualization, data curation, formal analysis, fund acquisition, research, project management, software, monitoring, validation, visualization, writing - original draft, writing - proofreading and editing: Montañez-Díaz, B. A., García-Gutiérrez, W. F., Prieto-Pastor, R. A. y Mendoza-De-los-Santos, A.

REFERENCES

Amazon. (2023). *Amazon Rekognition Image*. AWS. https://aws.amazon.com/es/rekognition/image-features/

Ammour, N., Bazi, Y., & Alajlan, N. (2023). Multimodal Approach for Enhancing Biometric Authentication. *Journal of Imaging*, *9*(9), 168. https://doi.org/10.3390/jimaging9090168

Aza Poveda, S., & Rodriguez Vanegas, J. S. (2020). *Sistema de control biométrico de asistencia docente* [Universidad Distrital Francisco José de Caldas]. http://hdl.handle.net/11349/28315

Balapour, A., Nikkhah, H. R., & Sabherwal, R. (2020). Mobile application security: Role of perceived privacy as the predictor of security perceptions. *International Journal of Information Management*, *52*, 102063. https://doi.org/10.1016/j.ijinfomgt.2019.102063

Bhat, A., Rustagi, S., Purwaha, S. R., & Singhal, S. (2020). Deep-learning based group-photo Attendance System using One Shot Learning. *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)*, 546–551. https://doi.org/10.1109/ICESC48915.2020.9155755

Bhavsar, K., Shah, D. V., & Gopalan, D. S. (2020). Scrum: An Agile Process Reengineering In Software Engineering. *International Journal of Innovative Technology and Exploring Engineering*, *9*(3), 840–848. https://doi.org/10.35940/ijitee.C8545.019320

Dudjak, M., & Martinović, G. (2020). An API-first methodology for designing a microservice-based Backend as a Service platform. *Information Technology And Control*, *49*(2), 206–223. https://doi.org/10.5755/j01.itc.49.2.23757

Flutter. (2019). *Build beautiful native apps in record time*. Flutter. https://flutter-website-staging.firebaseapp.com/

Guo, X. (2021). A KNN Classifier for Face Recognition. *2021 International Conference on Communications, Information System and Computer Engineering (CISCE)*, 292–297. https://doi.org/10.1109/CISCE52179.2021.9445908

ISO/IEC 19794-5:2005. (2005). *Information technology — Biometric data interchange formats*. International Organization for Standardization. https://www.iso.org/standard/38749.html

ISO/IEC 25010. (2011). *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. Organization for Standardization, Technical Committee ISO/IEC JTC 1/SC 7. https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en

ISO/IEC 25040. (2011). *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Evaluation process*. The International Organization for Standardization, Technical Committee ISO/IEC JTC1/SC7. https://www.iso.org/obp/ui/#iso:std:iso-iec:25040:ed-1:v1:en

ISO/IEC JTC1 SC17 WG3. (2018). *Portrait Quality: Reference Facial Images for MRTD (Technical Report)*. International Civil Aviation Organization. https://www.icao.int/Security/FAL/TRIP/Documents/TR - Portrait Quality v1.0.pdf

Kausar, F. (2020). Cancelable Face Template Protection using Transform Features for Cyberworld Security. *International Journal of Advanced Computer Science and Applications*, *11*(1). https://doi.org/10.14569/IJACSA.2020.0110142

Kodali, R. K., Panda, A., & Boppana, L. (2023). Attendance System using Amazon Rekognition. *TENCON 2023 - 2023 IEEE Region 10 Conference (TENCON)*, 65–70. https://doi.org/10.1109/TENCON58879.2023.10322521

Kounev, S., Herbst, N., Abad, C. L., Iosup, A., Foster, I., Shenoy, P., Rana, O., & Chien, A. A. (2023). Serverless Computing: What It Is, and What It Is Not? *Communications of the ACM*, *66*(9), 80–92. https://doi.org/10.1145/3587249

Leotta, M., Mori, F., & Ribaudo, M. (2023). Evaluating the effectiveness of automatic image captioning for web accessibility. *Universal Access in the Information Society*, *22*(4), 1293–1313. https://doi.org/10.1007/s10209-022-00906-7

Li, L., Chen, C., Pan, L., Zhang, L. Y., Wang, Z., Zhang, J., & Xiang, Y. (2023). A Survey of PPG's Application in Authentication. *Computers & Security*, *135*, 103488. https://doi.org/10.1016/j.cose.2023.103488

Lovrić, L., Fischer, M., Röderer, N., & Wünsch, A. (2023). Evaluation of the Cross-Platform Framework Flutter Using the Example of a Cancer Counselling App. *Proceedings of the 9th International Conference on Information and Communication Technologies for Ageing Well and E-Health*, 135–142. https://doi.org/10.5220/0011824500003476

Moral, P. (2021). *Sistemas de geolocalización, control del trabajador y facultad disciplinaria empresarial* [Universidad de Valladolid]. https://uvadoc.uva.es/handle/10324/50965

Nakisa, B., Ansarizadeh, F., Oommen, P., & Kumar, R. (2023). Using an extended technology acceptance model to investigate facial authentication. *Telematics and Informatics Reports*, *12*, 100099.

https://doi.org/10.1016/j.teler.2023.100099

Novoa, P., Reyes, J., & Cedeño, J. (2019). Aplicación móvil inteligente para asistir el registro de actividades académicas en sistemas biométricos: una experiencia universitaria en el Ecuador. *Revista Científica de La Universidad de Cienfuegos*, *11*(2), 55–60. https://rus.ucf.edu.cu/index.php/rus/article/view/1150

Padilha, R., Andaló, F. A., Bertocco, G., Almeida, W. R., Dias, W., Resek, T., Torres, R. da S., Wainer, J., & Rocha, A. (2020). Two-tiered face verification with low-memory footprint for mobile devices. *IET Biometrics*, *9*(5), 205–215. https://doi.org/10.1049/iet-bmt.2020.0031

Saadon, J. R., Yang, F., Burgert, R., Mohammad, S., Gammel, T., Sepe, M., Rafailovich, M., Mikell, C. B., Polak, P., & Mofakham, S. (2023). Real-time emotion detection by quantitative facial motion analysis. *PLOS ONE*, *18*(3), e0282730. https://doi.org/10.1371/journal.pone.0282730

Salvatierra, G. (2018). *Desarrollo de un sistema de control de asistencia estudiantil mediante reconocimiento facial* [Universidad Internacional de la Rioja]. https://reunir.unir.net/handle/123456789/7425

Sandhya, N., Vijaya Saraswathi, R., Preethi, P., Aarti Chowdary, K., Rishitha, M., & Sai Vaishnavi, V. (2022). Smart Attendance System Using Speech Recognition. *2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 144–149. https://doi.org/10.1109/ICSSIT53264.2022.9716261

Sang, J., Lei, Z., & Li, S. Z. (2009). *Face Image Quality Evaluation for ISO/IEC Standards 19794-5 and 29794-5* (pp. 229–238). https://doi.org/10.1007/978-3-642-01793-3_24

Silvelo, A. (2019). *Sistema de autenticación biométrica basado en el análisis del comportamiento mediante interacción por pantalla táctil y sensores de movimiento* [Universidad de La Coruña]. http://hdl.handle.net/2183/24560

Soewito, B., Gaol, F. L., Simanjuntak, E., & Gunawan, F. E. (2016). Smart mobile attendance system using voice recognition and fingerprint on smartphone. *2016 International Seminar on Intelligent Technology and Its Applications (ISITIA)*, 175–180. https://doi.org/10.1109/ISITIA.2016.7828654

Sulla, T. (2022). *Sistema biométrico basado en aplicaciones móviles para el control de asistencia de estudiantes del Instituto Superior Tecnológico Americana del Cusco* [Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/30756

Supabase. (2023). *The Open Source Firebase Alternative*. Supabase. https://supabase.com/

Tee, T. X., & Khoo, H. K. (2020). Facial Recognition using Enhanced Facial Features k-Nearest Neighbor (k-NN) for Attendance System. *Proceedings of the 2020 2nd International Conference on Information Technology and Computer Communications*, 14–18. https://doi.org/10.1145/3417473.3417475

Torres, E. (2019). *Implementación De Un Sistema De Control De Asistencia Con Código Qr Para La Institución Educativa Ricardo Palma – Carhuaz; 2019* [Universidad Católica Los Ángeles Chimbote]. http://repositorio.uladech.edu.pe/handle/20.500.13032/13800

Valverde, M. (2018). *Desarrollo de una aplicación móvil android para la Empresa Righttek S.A. como aporte a los controles de localización y registro de ubicación del personal de soporte a usuarios* [Universidad César Vallejo]. https://hdl.handle.net/20.500.12692/87748

Vardakis, G., Tsamis, G., Koutsaki, E., Haridimos, K., & Papadakis, N. (2022). Smart Home: Deep Learning as a Method for Machine Learning in Recognition of Face, Silhouette and Human Activity in the Service of a Safe Home. *Electronics*, *11*(10), 1622. https://doi.org/10.3390/electronics11101622

Wasilewski, K., & Zabierowski, W. (2021). A Comparison of Java, Flutter and Kotlin/Native Technologies

for Sensor Data-Driven Applications. *Sensors*, *21*(10), 3324. https://doi.org/10.3390/s21103324

Zambrano-Vega, C., Oviedo, B., & Moncayo Carreño, O. (2020). *Assessing the Performance of a Biometric Mobile Application for Workdays Registration* (pp. 1004–1015). https://doi.org/10.1007/978-3-030-12385-7_68