but, from its architecture and security focus there are vulnerabilities that might allow false-identity alterations when presenting platform-based activities, where, even if they are saved in the system, the logs with the log-in records that specify IP addresses with which an activity has been made, there is no certainty that the user in the platform is who really has entered the system.

After having made the platform security protocol description and, acknowledging the central role that users have in new technologic resource design and implementation, a survey was held with the participation of 22 University teachers, and 500 University students enrolled in on-site class mode that take virtual optional courses.

The survey inquiries about the perception of safety that working on the platform generates and about the importance users give to these aspects, from obtained results it can be stated that in spite of the identified problems on a technologic level, people that interact within the platform feel safe and do not perceive any threat or identity-theft risk that could affect their academic activities.

78.8% of polled people have a favorable concept of security in the platform and 89.1% feel that their information is safe and consider being cyber-attacks victims a remote possibility. It is important to highlight that for the 84.8% polled, the system vulnerability could affect their performance.

Additionally, questions are made to identify the users' preferences and opposability from the users to face recognition technology and systems and it was found that even though it is not the preferred method as can be observed in Figure 1, 87 from the 522 people that answered the poll selected the aforementioned as the system with the most acceptance. When asked about if they would agree with face recognition as an identity validation method on virtual exams on the academic UMB platform to avoid identity theft, 72,2% of polled people express agreement (Agree or Strongly Agree), whilst people with reluctance to its implementation were represented with 20.9% of people polled (see Figure 2). Results that clearly support the decision of designing and implementing this authentication system on VirtualNet.

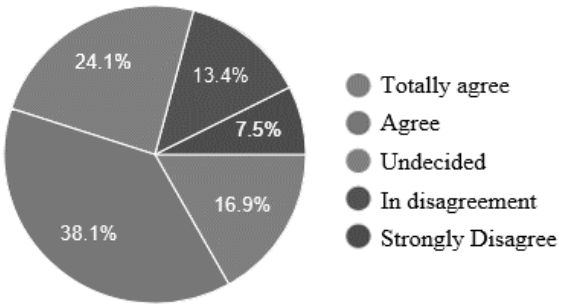

Figure 2. Face recognition acceptance as a validation method

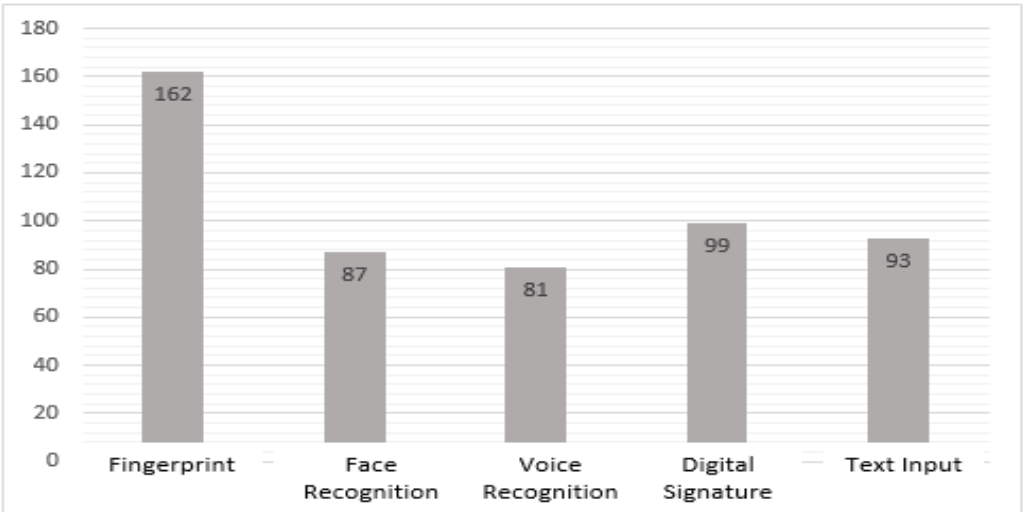

Figure 1. Authentication system preference

3. Project framework

3.1. Project and objectives Presentation

E-learning is being positioned worldwide and locally as a mode of teaching and learning, UMB as a response, not only for its formative processes on a disciplinary level, but given its commitment with a quality education for everyone, draws out virtualization rules for on-site class courses in response to the social demands of current times. Thus, the University offers extensive cross-curricular courses for students enrolled in on-site class, full-time mode, which brings the answer to the following question: How can one assure that students obtaining their certification in any course are the ones that have taken them, given that there does not exist on-site class contact? This situation evidences the vulnerability of the system to guarantee the trustworthiness in the students' authentication.

As a consequence, the project's objective is to design an algorithm to strengthen the authentication mechanisms on VirtualNet users, with the purpose of diminishing the error margin in certificating students that use the platform.

3.2. Project Description

Within the nature of this work, an algorithm is designed to strengthen the authentication mechanisms on VirtualNet users; statement that in the future will be oriented towards the implementation of face recognition services that allow to validate access and presence of the students to this LMS.

This project's approach seeks to offer validation processes in user authentication to favor security aspects, for which it will be based on [4] to propose a system structuring which is more solid and that can lessen identity-theft attacks; usability, with a quality systematic focused on the user; and legally, taking into account the current legislation on cyber safety globally because of the possibilities that the cyber space offers that allows to consider ethic and legal privacy issues, data handling and integrity and respect for people that are involved in teaching and learning on virtual platforms.

Attending to the usability of virtual learning environments and in consideration of the student design-centered, results from the surveys are taken and the required times for tests and implementation of the algorithm to select the face recognition as an authentication system to validate the users' identity on VirtualNet.

The authentication processes will be implemented randomly and during the users' time of presence in the platform. The login register through user and password is kept through the said user information therefore adding the face recognition process after.

3.3. Project Phases

The Project is divided in three phases, the first is oriented to the algorithm's initial design, where the following stages are included:

1. Current system revision in informatics safety.
2. Environment analysis and users' needs.
3. Methodological questioning on informatics security aspects on LMS.
4. Triangulation of the methodological aspects and environment analysis.
5. Establishing solution alternatives to implement methods that allow to enhance the level of trustworthiness of the face recognition implementation as a tool of identity verification.
6. Structural algorithm design for the implementation.

Subsequently, the second phase will take place, where the direct implementation of the algorithm on the LMS VirtualNet will be carried out; on this phase the initial prototype, taking into account the following stages:

1. To integrate the face-recognition structural design within the LMS evaluation module.
2. To do initial validation tests through Black Box Texting

Finally, upon the third stage, the following is expected:

1. To implement an academic program that is specific for the UMB University in Colombia to evaluate in an initial simple that complies with the required characteristics for the data compilation and evaluation.
2. To proceed with the module validation tests and their new integration.

3.4. Environment Description

On the long run, the management learning system LMS VirtualNet, in its second phase, will count with 2 verification tools that will look to improve the user authentication on the platform, with the purpose of increasing the reliability on official certification either from government entities or students.

3.5. Course Description and how are exams like?

The pilot evaluation module from this implementation, in which a great part of the UMB

online courses development is centered, will count with identity verification tools, improving platform safety in terms of identity theft and at the same time, allowing the university to reach its goal of certainty in its academic study certification process.

3.6. Resources

Process summary information statistics were distributed through the same communication modules from VirtualNet, e-mails and other information sources. The strategy planning was made on the documents offered by the facial recognition services from Amazon Web Services and the previous safety study analysis made to VirtualNet.

4. Preliminary results

4.1. Project's first phase

As results of the methodologic inquiry on LMS security information aspects, the following possible vulnerabilities under the identity-theft mode were found:

- The identity robber can use a static image of the account owner and locate it in front of the devices camera.
- The user can be in front of the device's camera, which would give a degree of approved similarity, but could be accompanied by a third party that would be answering the platform activities.
- The user can take unfamiliar objects over their face to make recognition difficult or impossible.
- Based on the aforementioned, it is determined that for this first version of the algorithm's initial design the following characteristics shall be taken into account:
- It is necessary to make different takes of the user on different random moments to obtain the best possible amount of data per try.
- The facial recognition system must show a degree of similarity between the original document's photograph and the ones capture don different times during the exam.
- The system has to offer a face recognition that is in the capacity of identifying the quantity of people on different moments throughout the exam.
- The face recognition service has to supply information on the users' facial patterns, with the intention of evaluating the different moments in session and being able to dismiss the likelihood of the usage of static photography on the camera.
- The compiled data has to generate silent alerts which will be stored for their analysis and later verification on its usefulness and truthfulness for this project.

As a result of this investigation it has been decided to implement the following processes to improve the possibilities of identifying the user that is active to avoid possible frauds. To demarcate this first phase, the specific use on exams proposal will be made on the platform, taking into account:

1) The system has to take the designated time for the exam and calculate the average time for it in similar evaluations. Having this timeframe, 5 to 10 moments must be taken at random for the samples to be taken on each exam for each user. This to allow to create unique simple intervals for each attempt within the exam.

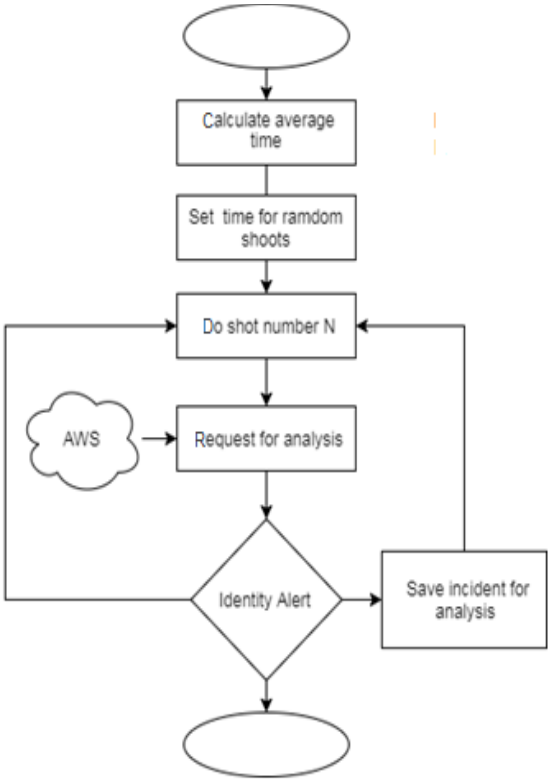

Figure 3. General flow diagram

2) Each one of these samples (images) are analyzed with the face recognition service from ***Amazon Web Service (AWS),*** obtaining as an answer a series of parameters and prospects to be analyzed, taking into account the degree of similarity between comparisons of current photography taken during the exam and pictures from the student's identification documents, amount of people on the pictures taken randomly, unidentified objects in the photography's and facial treats for the person taking the exam. These

parameters must be stored and be perfectly clear in the analysis results. These parameters have to be stored to be able to have proof of the results after the analysis is made.

3) With the analyzed data per try, alarms of possible attempt of identity-theft will be created based on the following statements:

   I. The actual samples have a similarity under 80% in relation to the identity document.

   II. The user of the platform has unidentified objects on their face.

   III. There is more than one person on the scene in more than two takes

   IV. There are two samples that are completely the same in facial expressions which would indicate that there are static photography's in use to avoid the authentication measure.

Taking the proposed analysis into consideration, the initial design of the algorithm is done to strengthen the user authentication mechanisms on VirtualNet (see Figure 3).

4.1. Project's second phase

The construction of the project is developed under the incremental iterative model, in which it can be adjusted according to the academic needs from the UMB, in the first prototype face-recognition structural design will be integrated within the LMS evaluation module, which will later be tested for initial verification under Black Box Testing. The aforementioned process will be developed taking into account the following stages (see Figure 4).

1. Requirement Definition: Specifications and Functionalities needed for the project.
2. Iterative prototype: Development, parameterization and increasing customation.
3. Tests and feedback.

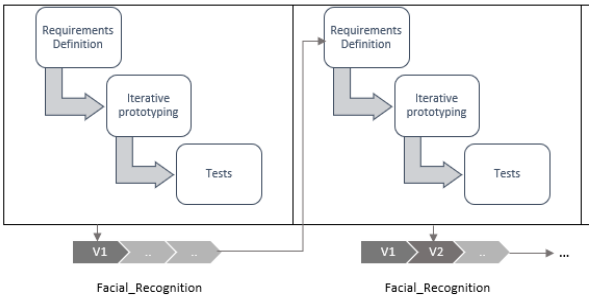

Figure 4. Implemented Iterative Increasing Model

The purpose for each iteration will present a new version of the integration to check its applicability and user friendliness, with the objective to increase the reliability and usefulness to increase student certification. Within this framework, results are then described in the first version.

4.1.1. Facial Recognition V1. For the first testing integration on the platform 'Virtualnet 2.0' and "Facial_Recognition_v1" the steps to relate the SDK offered by AmazonWeb Service which will allow the image acknowledgement and processing (https://aws.amazon.com/es/tools/#sdk) in the constructed version for PHP language for University LMS.

Within this first instance for the process, a problem is detected because the SDK by Amazon for current face-recognition, is supported for PHP 5.5 versions and more updated ones, which presents problems to achieve the incorporation to LMS Virtualnet, because it was built in a 5.3 version of PHP, reason why it is not possible to do a direct implementation of the SDK and the object module as pilot. 'Virtual Exams'. With this in mind, after a thorough analysis it was determined that there are two possible options:

1. To try and use the SDK with an updated and alternative PHP service which is up and running on a different port.
2. Update everything on the LMS Virtualnet to a PHP version which is needed to use a unique version throughout the whole platform.

While evaluating the current alternatives, it was decided for the first option, given that under the iterative increasing model it will be taken as an opportunity that will allow to work in the presentation for the Facial_Recognition first version in a PHP updated and alternative service, which counts with virtualnet's specific characteristics; for the near future, it is expected to proyect the possibility of optimizing the system to improve general security, by updating Virtualnet to PHP 5.6.3.

Under the mentioned scenario, the testing implementation and compatibility of the SDK is initiated, taking into account the following functional requirements (see Table 1).

Table 1. Facial Recognition V1 Initial Requirement Description

Code	Requirement Description
R1	In the evaluation modules, create a main class that establishes the intermediation parameters between its requests and the offered answers for the Amazon web service for image recognition through SDK.

Code	Requirement Description
R2	Create an agreement where the user is informed (students) that a series of photographs will be taken during the exam, with the purpose of validating the identity of the person in front of the computer screen.
R3	Based on the initially stated algorithm, the evaluation module will take the user's identification photo, previously related, to be taken as a comparison to later be prepared to be sent to the face recognition web service.
R4	Using HTML5 technology and JavaScript, the frontal camera activation form the user's computer will be activated.
R5	The module randomly establishes the amount of takes that will be taken and the estimated times for each one, taking into account the exams duration.
R6	Having each one of the previous characteristics, at the beginning of the examination, that counts on the timer that will trigger the captures of images.

Taking into account the previous considerations, the first Facial Recognition V1 through the code:

```
// Service Configuration

$options = [
   'region' => 'us-west-2',
   'version' => '2016-06-27',
   'credentials' => [
      'key' => '',
      'secret' => '',
   ]
];
$rekognition = new RekognitionClient($options); // AWS comparison method is used
$result = $rekognition->compareFaces([
            'SimilarityThreshold' => 0.8,
            'SourceImage' => [ // REQUIRED
                        'Bytes' => $image_base // ID photo
            ],
            'TargetImage' => [ // REQUIRED
                        'Bytes' => $image, // during the exam photo
            ],
]);
```

It allows:

A. To send validation data message
B. To load the timer for taking pictures depending on exam time
C. Give the first photo signal
D. Take the user's first photo
E. Store the captured image in a temporary file.
F. Use SDK to send the first picture test.
G. Given the described conditions, for this first momento the preliminary from the WEB Service is taken, which contains the result of the comparison between the stored photo in the database and the one taken during the exam, as evidenced in Figure 5.

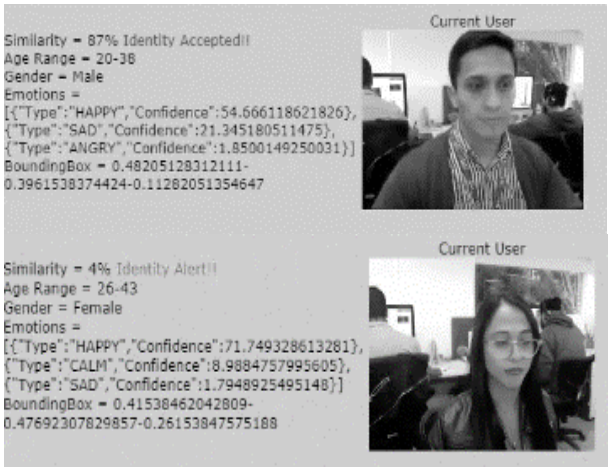

Figure 5. Biometric identity validation results

It is of great importance to highlight that the validation characteristics' information generated will be stored within a table in the database from the LMS , for further analysis, to define and establish the silent alarms proposed for this phase.

At the same time, the timer will still be active waiting to activate the next takes, to do the same actions which were previously defined, until finishing the loop.

Table 2. Similarity for different users when authenticating

	user 1	**user 2**	**user 3**	**user 4**	**user 5**	**user 6**
Frontal Posture	10%	15%	2%	20%	4%	28%
Frontal-side Posture 1	13%	19%	5%	19%	2%	22%
Frontal-side Posture 2	14%	17%	3%	18%	2%	24%
Closed eyes	20%	28%	5%	17%	10%	23%
Glasses	25%	22%	10%	22%	12%	27%

Within the analyzed exercise, it is evidenced that the neeed to establish the measuring tools to validate

the trustworthiness and system failure in acknowledgement, which is why 2 diferrent samples were taken to determine the standard. The first of those is through the photographic intake of the different subjects that have similar aspects to the user authenticated in the platform with several attempts and different light conditions (see Table 2). The second sampling shows the photographic take from the same user authenticated in the platform with different postures, objects and light conditions (see Table 3).

Table 3. Similarity percentage between several attempts for the platform's user

	Test 1	**Test 2**	**Test 3**	**Test 4**
Frontal Posture	87%	90%	77%	92%
Frontal-side Posture 1	84%	89%	75%	90%
Frontal-side Posture 2	85%	91%	76%	91%
Closed eyes	80%	85%	72%	87%
Glasses	76%	80%	75%	82%

The previous information demonstrates that similarity for different users in authentication does not mark over 20% similarity, while for the same registered user marks above 75% (see Figure 6).

The previous verifying process allows to complete the iterative increasing model from the first face recognition process, given that through these tests, the Black Box testing is done, base don the functional requirements defined in Figure 1, which allowed to identify (see Figure 4).

Table 4. Black Box Testing Facial Recognition V1

Code Requirement	**Entry Data**	**Expected Result (output)**	**Does it achieve expectations?**
R1	Images from the identity document and images taken during the exam	Similarity percentage between the 2 images	Pass
R2	User acceptance on the emerging window to take the verifying images	Access to the exam module.	Pass
R3 R5 R6	Trigger action and picture capture in different time intervals.	ID images and taken images during the exam.	Pass
R4	Navigator request for frontal camera use.	Frontal camera activation form the user's computer	Pass

The previous results allow to conclude that the first proyect iteration, giving as a result the initial prototype in the evaluation module, with a PHP updated and alternative service, from Virtualnet, that allows to validate user authentication. In this first version, through picture taking and image

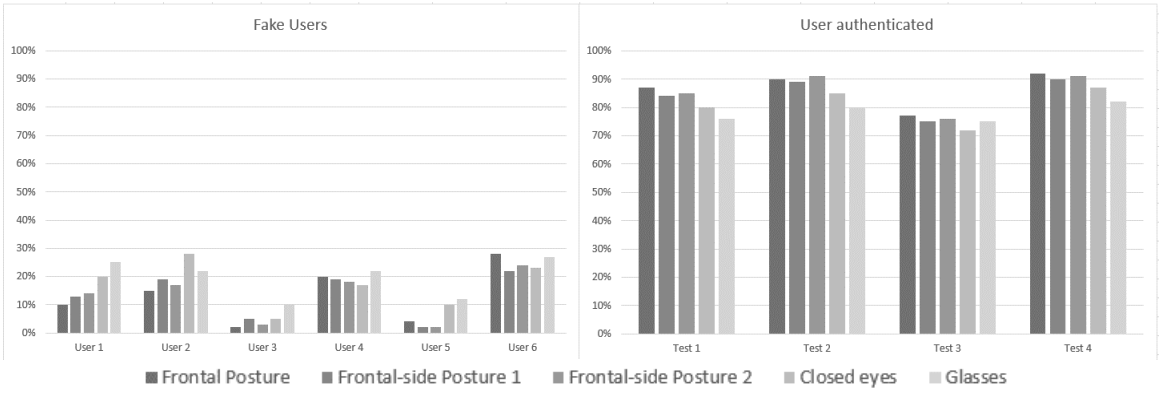

Figure 6. Sample Authentication

comparison, the registered user recognition results are accomplished The Facial Recognition V1, on this initial phase, allow the system to throw silence alerts when the similarity between the photo and the pictures taken throughout the exam be inferior to the minimal obtained value during the facial recognition tests for a valid user.

5. Ongoing Work / Future Work

As work in progress, on the investigation team we are implementing on the VirtualNet development environments the first version of the algorithm herein described. In the future, it is expected that Facial Recognition could count with a main controller, directly on Virtualnet, that is in charge of receiving and processing every petition from and to the Amazon Web Service, where the main controller has to be addressed from the main module's class which will be the pilot module. Under the iterative development model, for version 2, it is estimated that the information from these alarms be directed and analyzed by teachers and managerial positions, contributing to the qualification of the validity of the information, which is basic for the academic process certification in the UMB. As first implementation stage, the functionality of face recognition will be applied on the exams from the course 'Fundamentos de Investigación' which currently counts with 400 students, to be able to compile and analyze the possible cases of identity theft on exam presentation.

6. Conclusions

The work will continue until 2018's second semester, when its complete implementation is fulfilled, therefore only partial results are presented on this work, specifically on the exposed proposal on the initial phase.

It is found that VirtualNet users do not notice safety issues nor feel vulnerable to cyber-attacks, in spite of the limited levels of safety that the platform counts on. Under this fact, it is mandatory to maintain this perception of usefulness strengthening the safety system in place.

The platform users acknowledge and consider some biometric authentication systems as reliable, the one with the most acceptance is the one that is found most frequently on a local context, in this case the fingerprint method.

The majority of VirtualNet users do not consider invasive nor reject face recognition usage as a resource of authentication to work on virtual courses offered by the UMB.

To guarantee the accreditation and certification of the students that are part of the learning community mediated by the LMS, it is necessary to use algorithms and artificial intelligence resources of pattern recognition.

7. References

[1] J. Díaz, A. Schiavoni, A. Osorio, P. Amadeo, y E. Charnelli, "Integración de plataformas virtuales de aprendizaje, redes sociales y sistemas académicos basados en Software Libre. Una experiencia en la Facultad de Informática de la UNLP", Universidad Nacional de la Plata, 2012.

[2] S. Bayat, M. Mozaffari and A Reyhani-Masoleh "Efficient and Concurrent Reliable Realization of the Secure Cryptographic SHA-3 Algorithm", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, n. º 7, pp. 1105-1109, jul. 2014.

[3] Y. Mena, "Algoritmos HASH y vulnerabilidad a ataques", Journal Información, Tecnología y Sociedad, p. 108, 2009.

[4] A. Morales, J. Fierrez, R.Vera-Rodriguez, & J. Orteg "Autenticación Web de Estudiantes Mediante Reconocimiento Biométrico". In III Congreso Internacional sobre Aprendizaje, Innovación y Competitividad. 2016.

