A Gamification Architecture to Enhance Phishing Awareness

Abstract

The development of emerging technologies, namely, the Internet of Things (IoT) and Artificial Intelligence (AI), have provided a spectrum of online and remote solutions in various fields. However, the proliferation of targeted cyberattacks against such technologies has made our assets and data relatively vulnerable to adversaries and hackers. Considering the higher number of victims, it is necessary to consider technical solutions that limit the development of a critical mass of people who can participate in collective resistance to such a phenomenon. Raising awareness is, undoubtedly, a way to prevent as many people as possible from falling prey. Given the changes in the different educational theories, we must seek the best way to sensitize users of cyberspace to their varied profiles and needs. This study develops an educational gamification architecture that can ensure commitment, motivation, and consideration of a learner's profile. Subsequently, the problem of the best didactic means is posed with openness to the integration of artificial intelligence, the choice of the type of gamification, and the technologies that can contribute to ensure that everyone is competent such to enable each person to escape from traps of phishing, regardless of age, level of mastery of digital tools, or education. The proposed approach was evaluated according to the robustness and flexibility of the solution, and didactic and pedagogical innovations to improve the target's experience. The rest of the work consists of integrating the conversational aspect through chatbots.

Keywords: cyberspace, architecture, victimization, competence, gamification.

1 Introduction

COVID-19 has helped to demonstrate the urgency of linking many structures, organizations, and countries to technological and scientific revolutions. It is in this wake that the rush observed towards digitalization is located without a real preparation for this mutation in most cases. Prodigious developments in the Internet of Things (IoT) and innovative technologies such as Artificial Intelligence (AI) are increasingly having an undeniable impact on teaching methods. Access to the common space of communication represented by cyberspace is not without its pitfalls. Said spaces are currently experiencing the proliferation of criminals of another kind. While taking advantage of ignorance or naivety, some users of cyberspace, on the fringes of lawful activities, perform increasingly sophisticated criminal actions by multiplying cyberattacks [1]. The cybercrimes encountered include infiltrations, malicious applications for ransoming systems and networks, theft of sensitive information, system paralysis, and financial embezzlement.

In Cameroon, a study conducted in 2021 by Ntsama et al. [2], revealed that crimes related to embezzlement of money were the most frequent, representing a portion of 70.51%. In addition to the technical detection and control solutions [3-4][5] which have not eradicated yet the phenomenon, it is necessary to use awareness-raising solutions, whose merit reduces victimization and prepares a critical mass for collective resistance to the phenomenon that is taking on a worrying scale. It is not surprising to agree with the report of the National Agency for Information and Communication Technologies (ANTIC) that severe losses are recorded, i.e. 12.2 billion CFA francs [6] loss for the Cameroonian economy in 2019.

Digitization with the race towards increasingly high-performance digital terminals exposes people to risk, but also augurs great prospects in solutions that offer everyone the possibility of learning or raising awareness of the situation without restriction. The problem of the best didactic offer to ensure user awareness remains.

Currently, techno-pedagogy offers scripting as a means of improving the transmission of content [7]. Gamification, on the other hand, introduces playful elements into a non-playful learning environment to increase motivation, create emulation, and captivate learner [8][9]. The use of automatic learning techniques [10] can bring the didactic approach closer to the learner's experience. Emphasis is on the level of awareness and skill development to enable learners to avoid easy prey. Furthermore, as cyberspace is not a domain reserved for a few elite, the gamification tools and architectures available often target specific segments of the population: class craft [11]. cybermuna [12], PAP [13], and cyber awareness/girl scout at home [14]. In addition, these proposals have limits on aspects concerning the target of awareness, functionalities, and the didactic approach that takes into account the level of psychological development [15][16]. At the same time, we observed the failure to take into account the profile and needs of the learner [17], as well as the time taken to show competence through scenarios. Raising awareness using easily accessible tools must begin early. However, the thorny problem of the best didactic means allows awareness to even lead to real learning to escape the increasingly sophisticated traps of cybercriminals.

Through this work, we describe a model of educational gamification architecture integrating the didactic means witch can facilitate awareness for any user. This process enable them to escape increasingly sophisticated traps of criminals who threaten the digital economy. The rest of the document first focuses on the background, with a review of educational theories and existing gamification solutions in cybersecurity. Thereafter, we propose an architecture that evokes the methodology, the global view of the system, the exploited gamification, its structure, its operation, and the evaluation of the score. We propose a prototype and evaluate the described architecture of the system, conclusions, and perspectives.

2 Background

2.1. Educational theories

Many advances have been made in the area of educational theories. We have observed a succession of numerous didactic approaches.
Behaviorism, in which appropriate stimuli lead to possible results as a proof of possible assimilation [18]. Behaviorists will be inclined to use exercisers, quizzes, educational games, and/or animations when designing and carrying out distance training. However, this theory seems too poor to be sustainable [19].

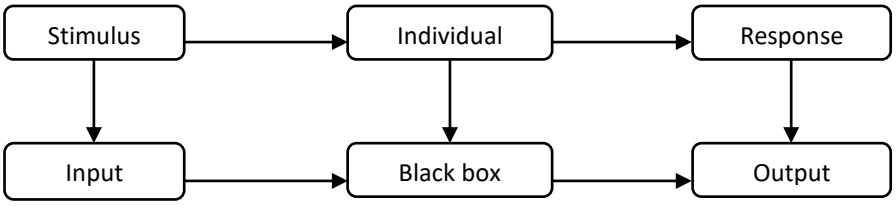

Fig. 1: Functional diagram of behaviorism

Cognitivism, which believes that learning process, cannot be limited to conditioned recording. It is necessary to resort strategies to manage memory [20]. Strategies depend on different types of knowledge to be developed, namely declarative, procedural, and conditional knowledge (Legault, 1992).
Constructivism, which admits that knowledge is acquired through construction. This model promotes not only the introduction of tools that offer great autonomy to students in order to progress at their own pace but also the development of computer-assisted problems [21].
Socio-constructivism, through which knowledge is acquired by construction and social interactions [22]. In addition, while giving to a child a learning environment in which he offers the best of himself, the teacher's choices tend to encourage group work [23].
Connectivism, which, through the development of networks, has favored the proliferation of learning platforms, such as e-learning, distance education, and gamification [24][36].
Many theories have militated in favor of the place of game in the learning process. The said process should remain playful and engaging.
We can thus distinguish:
Serious games, where we have to learn through a game in order to improve the learning experience of the target.
Gamification uses elements taken from the game in a non-gaming context to entertain the teaching/learning process [25][26], as well as the development of interactions, engagement, and motivation [27].

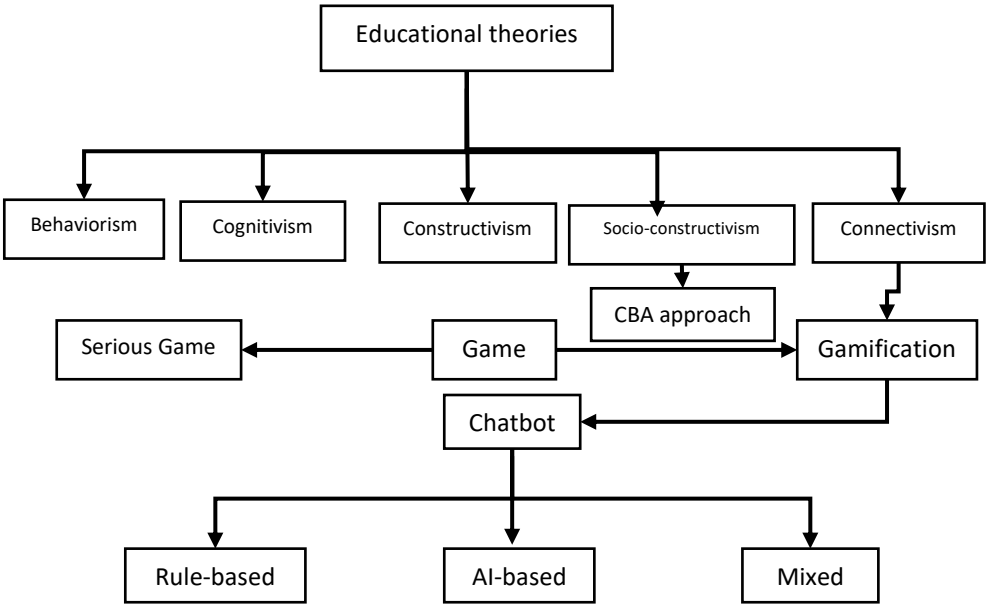

Fig. 2: Diagram of educational theories

Nowadays, apart from the face-to-face learning mode, e-learning, there is also distance education that complements the face-to-face mode through the virtual class. It contribution is to better establish skills developed in face-to-face part-time class with the stigmas of the context of COVID 19, through lessons, exercises, and revisions. However, distance education does not provide the possibility of making the teaching or learning process fun by introducing elements drawn from the context of the game to increase motivation, commitment, and emulation, such as points, progress bars, leadership boards, awards and avatars or images. To be close to the reality of the learner by a method of proximity pedagogy, it is necessary to consider his profile. In addition, the orientation towards digitalization of teaching was further explored. The boom observed in the use of digital terminals is part of the race for digitalization and, at the same time, offers a point of vulnerability. At the same time, these terminals can facilitate access to an awareness solution, regardless of the situation and profile.

2.2. Current Contributions in the fields of gamification and cybersecurity

Many authors have developed gamified systems for one domain or another with a predetermined target. The same have been done in the field of cybersecurity. The aim is to sensitize users of the cyberspace about cybersecurity, and how to escape from attacks.

Through a web application, some have contributed to improvement of learner's knowledge of phishing through the practice of phishing (PAP) approach [13]. This approach is an animated website implementing a structural gamified system, with sound and animation for attractiveness, but also through its menus (basic knowledge, avoid phishing, useful tips, explore more about phishing), screenshots, boards, and games based on MCQs segmented according to the profile associates, game elements such as points and scores. However, this game is not segmented into ages levels of the child's psychological development. There is also a lack of diagnostic assessments to verify prerequisites; the interactive side is very little perceptible outside the game. Lack of a progressive measurement of the evolution of learning and lack of ranking of the best to activate intrinsic motivation.

The Classcraft website not dedicated to cybercrime; however, only secondary education is targeted. There is no extension to other levels of learner's psychological development (mental age). The way of thinking can be dependent of the target psychological age [11].

The Cybermuna website is committed to the protection of young people online through the training of students under 21 year old, teachers, and parents using an interactive web application. This site carries out a diagnostic assessment of knowledge, targeting QUIZ of students: from 8 to 16 years old and under 21 years old. Teachers like parents are targeted by same QUIZ. The user chooses one of the above profiles for learning. Online resources are downloadable, and the score is given at the end of QUIZ [10]. Note that it is not only students, parents, and teachers who require cybersecurity training. There are also uneducated people who also suffer from the effects of cyber criminality with the development of social engineering tricks in cyberspace. In this solution, it is not possible to clearly visualize the step-by-step progress of learners during the learning process. Such a deficiency can result in a lack of intrinsic motivation and emulation. Moreover, this proposal was not sufficiently interactive. However, learner progress cannot be measured as the learning process evolves. The score was given only at the end of QUIZ.

The site girl scout objective is to train young girls in cybersecurity by helping them deal with any attack by ransomware, phishing, passwords, game security, and video call security. It includes a menu of access to PDF resources, video courses of procedures, and the possible registration for a diploma as intrinsic motivation [14]. However, the need for cybersecurity training goes beyond the scope of young girls alone, even if this solution meets the need. Learner's progress is not implement. We are not rewarded for the progress made: extrinsic motivation. Intrinsic motivation was found to be weak. We do not perceive progressive evolution through any passage from one level to another. Absence of diagnostic and formative evaluation to appreciate skills acquired by the target.

Hwang et al. (2021) presented recent research on "Cybersecurity Educational Games: Theoretical Framework," where the development of games for cybersecurity is to help individuals and organizations strengthen their defense against cybercrime [2][28]. The finding is that the effectiveness of the existing games is low. This article aims to guide the design and testing of more effective cybersecurity educational games by developing a theoretical framework with independents variable as follows:

•Game characteristics: What contributes to the usefulness, interactivity, playfulness, or attractiveness of a game;

•Game context: Factors determining how a game is used, target audience, skills involved, history;

•Learning theory used: behaviorism, cognitivism, humanism, socio-constructivism;

•User characteristics: gender, age, computer experience, knowledge, perception.

Dependent variables with five characteristics: information, content, strategic knowledge, desire to learn, time spent, and behavior change.

This proposal does not consider satisfaction, emotion, immersion, and the level of the learner at the beginning of learning, which constitute important aspects of the evaluation of the solution.

In its first version, the PASEA platform (Practices against Social Engineering Attacks), was an implementation of an architecture of an educational gamification platform for cybercrimes through phishing [29]. The acquisition and improvement of learner's performance require the introduction of gamification elements [8][9]. However, the contribution of chatbots would have allowed this platform to adapt to the situation and specificity of a particular user and, therefore, to his profile. Missing Artificial Intelligence (AI) assets would have made it possible to adapt the training offered to users [2][11][22].

All these contributions show that either many online platforms reveal their limits in terms of target audience, functionalities, or didactic theories underlying the

pedagogical approach adopted, which may not integrate the development of real skills. Either the integration of aspects of the subject's level of psychological development or ease of access in the context of the high cost of connections. Align the training offer increasingly with the needs or profile of the user. The time taken to show competency also needs to be considered.

The major objective is to provide an intelligent, adaptive, accessible, and flexible gamification architecture. It offers all guarantees of successful awareness raising and the development of proven and recognized skills. This is how we can prepare a critical population mass capable of accessing cyberspace without the risk of falling prey to cybercriminals. It is important that the architecture of awareness gamification adapts and aligns with the daily situation and non-static needs of cyberspace users. Any awareness strategy should be based on the target profile.

The use of automatic learning techniques can make it possible to bring the didactic approach closer to the learner's experience [10][30][11]. Companies must emphasize the level of awareness and their competence to act in a professional context to avoid being easy prey. Moreover, since cyberspace is not a domain reserved for a few elites, young people would benefit from starting awareness very early with easily accessible tools to protect themselves and thus create a critical mass ready for collective resistance to the phenomenon. However, the thorny problem of the best didactic means and robust architecture in an awareness platform to even lead to real learning to escape the increasingly sophisticated traps of cybercriminals.

3 Architectural proposal

3.1 Methodology

To carry out this work, we followed the diagram of Figure 3 below:

Fig. 3: scheme of the methodology

Existing studies allow us to investigate the existing in order to carry out an analysis of the needs and possible functionalities of the future system [30], to identify the strengths and weaknesses of existing gamification platforms in cybersecurity, and to identify future users and their expectations.

The choice of architecture allows starting from the limits of the existing one to proceed to the choice of the type and relevant elements of gamification.

Architecture modeling to proceed with the development of the system architecture;

Implementation and deployment of a prototype and evaluation, host a prototype online.

3.2 *System overview*

This system aims to raise learner's awareness of cybercrime related to phishing, fake news, existing detection/fighting solutions against phishing, system/network security, and data security (Figure 4).

Each aspect of raising awareness is based on the acquisition of resources, competent actions, and evaluation/remediation. After a lightened learning process, because of the different targets, the evaluation puts the learner in a situation that encourages him to exercise the skill. This approach does not fail to maintain a learner's interest and commitment. This is found in the gamification of the elements drawn from the game, such as points, scores, progress bars, and leaderboards. It is also relevant to add elements of artificial intelligence to this environment to get closer to the learner's profile, simulate scenarios, or adopt a virtual teacher (Figure 4 below).

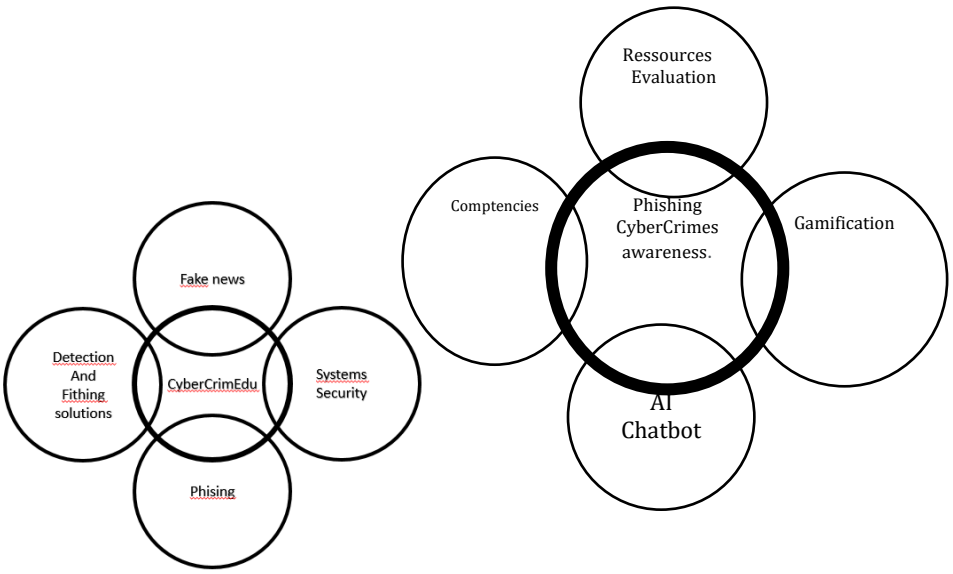

Fig. 4: System overview diagram

3.3 Gamification exploited

In this section, the choices made for the proposed system are presented. This is the general structure of a modeled platform.

For Abdoul Basit et al., gamification has five stages: identifying the target audience and context, defining learning objectives, structuring the experience, identifying resources, and applying gamification elements [28].

According to Kapp (2012), there are two types of gamification. Structural gamification or game elements are chosen to avoid altering the content [31]. Only the structure of the elements around the learning content resembles to a game.

Content-centric and user-centric gamification. The content is adapted to the user and may look like a game, but not completely become one.

However, gamification can be mixed, that is, sometimes structural and sometimes centered on the needs of a user profile.

Our segmentation of users is based on their level of maturity and varied needs. The psychological age of a child can be a brake on rationalism and the representation he has on things and on his environment [32].

The work of Wallon Henri [33] and taking into account Garnier et al. (1991) summarize the stages of psychological development from child to adolescent on logical, cognitive, and language levels. This division fits well with the requirements of school careers. However, potential victims have varied profiles. It would be interesting to break down an awareness model that considers the diversity of profiles.

We will consider this architecture, an educational gamification at three levels (child, adolescent, and adult): under 13, under 21, and over 20. They will be educated or not, parents, and teachers. An evaluation or consideration of the learner's level on the basic notions related to digital technology and cyber security practices to limit victimization through phishing attacks with social engineering technics. The nature of the assessments was MCQ or QUIZ. Intrinsic and extrinsic motivations depend on the level at which the evaluation is carried out. We must measure personal and collective development, and therefore, the evolution of the player or target: formative evaluation. A learner's score should lead to conclusive summative assessment. At the same time, this level was reached in comparison with other players at the end of the game.

In this case, the target was anyone who could access cyberspace. The main objective is to equip any person with competencies to avoid being easy prey faced to sophisticated traps of cybercriminals.

3.4 General structure of the application

The starting point for any user is registration and then logging in as an administrator or user.
As an administrator, you can perform administrative tasks, such as creating courses, levels, recording tutorials, evaluations, answers to prepare remediation, and the scoring guide.
In addition, learners can connect to the course and the level corresponding to the user profile, learn there, or be evaluated. A successful evaluation advances, where as an unsatisfactory evaluation requires remediation before returning to the previous level.
It is important to remember that you can exit at any level and the context is saved for the next connection, or the user is not required to start over at the beginning (Figure 5 above).

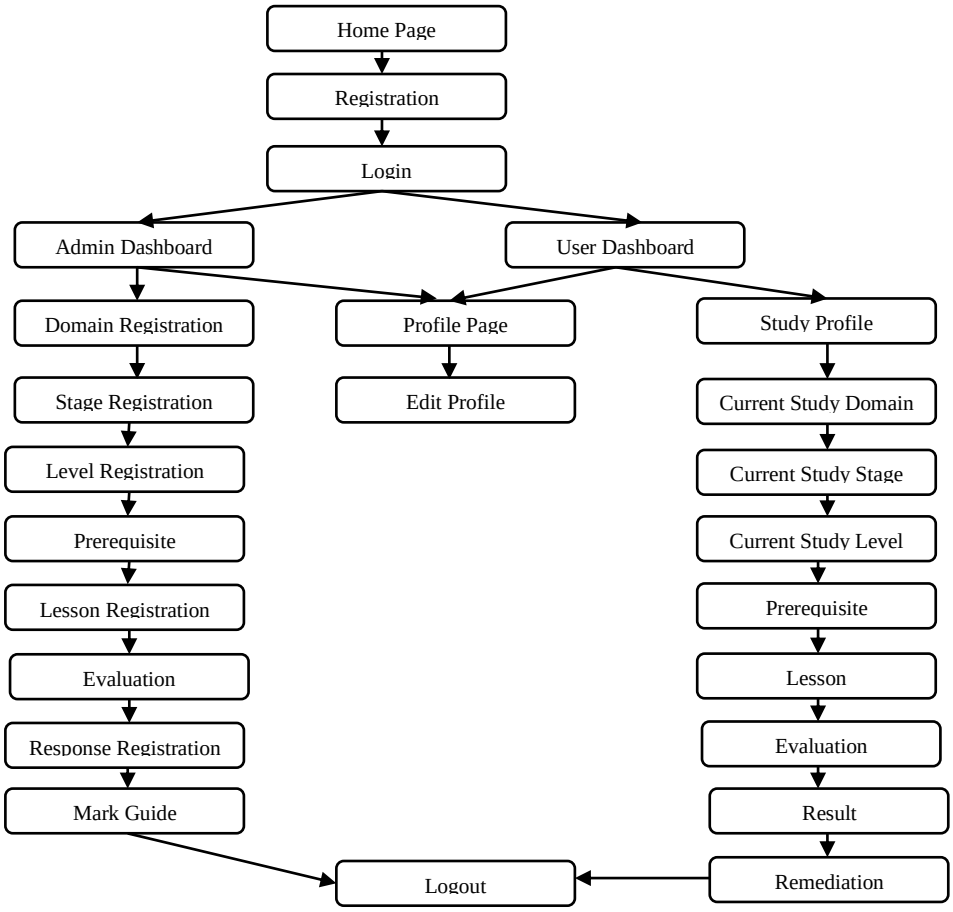

Fig. 5: Application structure

3.5 Navigation scheme

The connection of any user to this platform with login parameters requires prior registration. They can exit the application at the desired time and return to continue or resume to improve their performance. The user can access the awareness tutorial and be assessed, and if the assessment is not favorable, proceed with remediation.

For navigation at this site, the user connects by declaring his level of Digital Tools Mastery (DTM), informs about his age, picture, e-mail, pseudonym (Pseudo), and password. The system verifies that this nickname exists for the same age and returns a Boolean value. If it exists, the context saved in the last connection is retrieved. Otherwise, depending on age, one is redirected to the appropriate stage of application.

Each user creates an account to connect to the system. A profile of a user is informations concerning this particular user (Pseudo, avatar/picture, age, image, password, mastery of Digital Tools). Awarenees is about the same specific theme as cybersecurity. All three stages are based on it, from the lower level to the higher one. Each stage has four levels. Level 1 : Cybersécurité et ingénierie sociale, Level 2 : Les moyens et étapes d'une attaque par ingénierie sociale, Level 3 : Finalité d'une attaque, Level 4 : Types d'attaques et pratiques de sécurité. When a learner stops, his context is saved.

A learner start at a stage related to his profile, psychological development level, and Digital Tools Mastery level. He can also continue where he stopped.

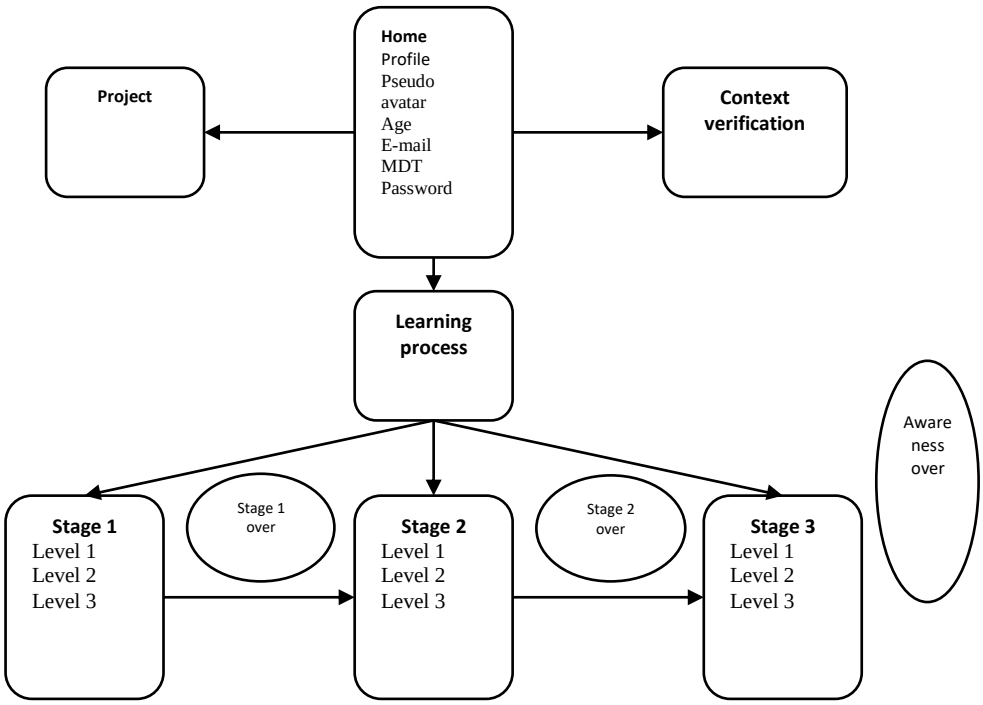

Fig. 6: Navigation scheme

The user is redirected to an appropriate stage depending on the age and level of digital proficiency. There are three stages adaptable according to the secondary school course: the cycle of observation, orientation, and the cycle corresponding to the first and the terminal.

Considering the need to form a critical mass of all sides accessing cyberspace and exposed to the same risk of cybercrime, we distinguish three stages: beginner, mastery, and expert. The same theme was developed with increasing levels of requirements.

The model in connection with the cutting of profiles has three stages, and each stage is divided into four levels or levels.

Each N level deals with a specific theme. This is how we have Level 1 (cybersecurity and social engineering), two level is about means and steps of a social engineering attack, three Level (finality of an attack), and Level 4 (types of attacks and security practices).

There are three levels of Mastery of Digital Tools (MDT): beginner (B), Intermediate (I), and Expert (E).

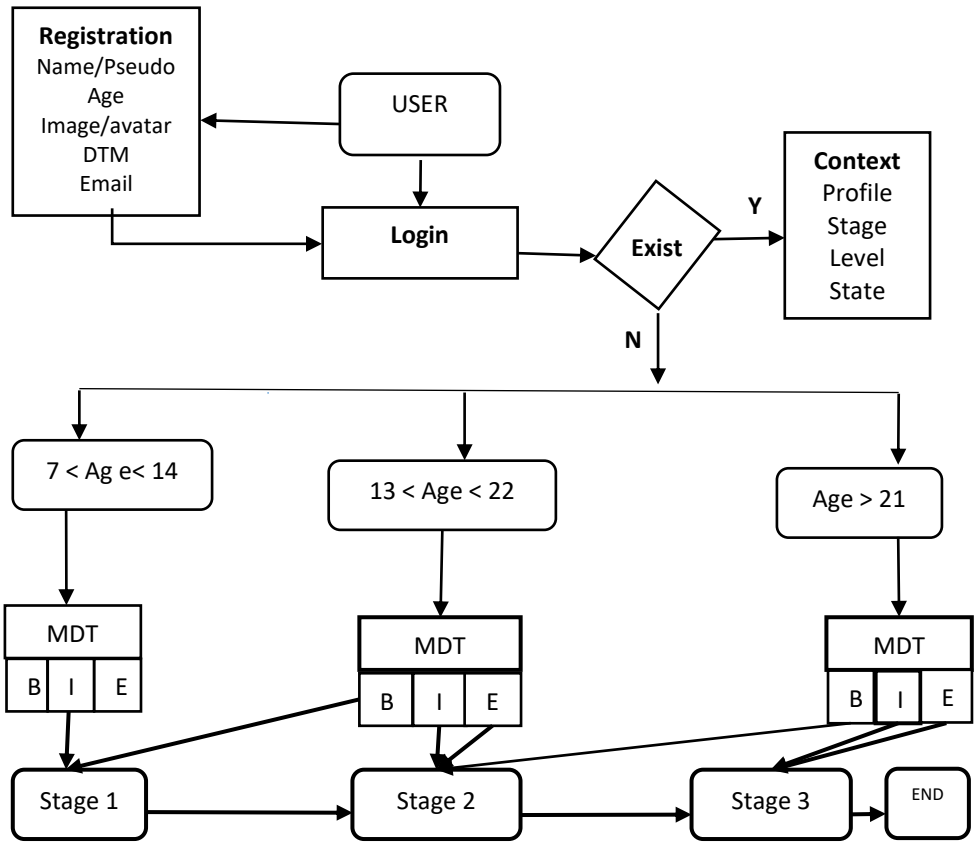

Fig. 7: Detailed navigation scheme

3.6 Modeling of system operation

The system comprises the three stages described above, and each of the stages comprises four levels or levels: Level K, K∈{1,2,3,4}
For any K, Level K verifies the prerequisites, learning, evaluation, and remediation if the evaluation is unfavorable.
To move from one stage to the next, the learner must be competent with a score greater than or equal to 70% at the last level of the previous stage.
The positive evaluation at Level 4 (Eval4>0.7) of stage N, N∈{1,2} makes it possible to move on to the next stage N+1.

```
Var st, LevelK, MDT, pseudo, age, avatar, Email, password,
EvalK
Function profile(pseudo, age, avatar, Email, password):
boolean
Begin
   if (profile=yes)  //exist
   {
      St= StContext; LevelK= Levelcontext; State=
stadecontext; //profileContext
   } else {
      If(age < 14)
         {
            St=1; LevelK=1;
         }
      elseif (Age<22)
         {
            If (MDT=B)
               {
                  St=1;
               }
            else
               {
                  St=2;
               }
         }
      else{
         if (MDT=B)
            {
               St=2
            }
         else
            {
               St=3
            }
      }//orientation of a learner

While (St<=3)
{
   LevelK= 1;

   While (LevelK<=4)
      {
         If (Evalk>0.7)
            {
               LevelK= next (Level K);
               print (Level Over);
            }

         Else
            {
               Remediate LevelK; LevelK= LevelK;
            }
         }
   }

Print (Over stage);

St=St+1;

Endwhile

Print (Game over); Print (score); Print (score board);

End
Print (Game over); Print (score); Print (score board);
End
```

Fig. 8: operation algorithm

3.7 Moving from one level to another

To move from one level of a stage to the next level of the same or another stage, the learner must be competent with a score greater than or equal to 0.7 at the previous level in a reasonable time. If he is not competent, the remediation mechanism brings him back to the previous level. Each stage has four levels (level p with $p \in \{1,2,3,4\}$.
At each level, we assess prerequisites, learning, formative and summative assessment, and remediation can occur at a score of < 0.7.
The transition from Level p, $p \in \{1,2,3\}$ to Level (p+1) is only possible if the score is greater than or equal to 0.7; otherwise, we go through remediation and return to Level p (Figure 9).

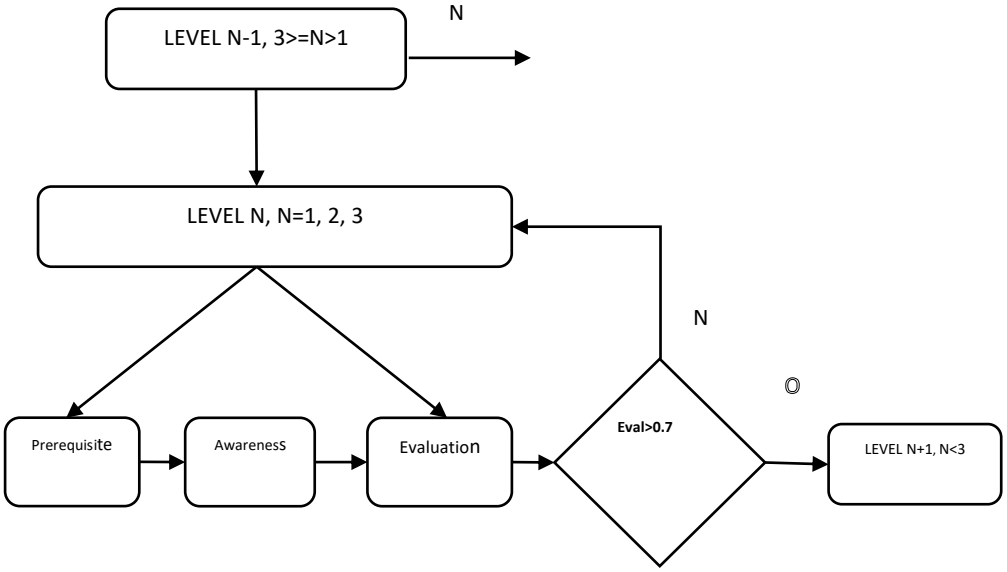

Fig. 9: Detailed level change diagram

3.8 Mathematical modeling of score evaluation

Let Nij be the score of stage i at level j, where i=1, 2,3 and J=1, 2, 3, 4.
We have matrix N(Nij) of scores of the different levels. It is a 3*4 matrix.
Given stage k= 1, 2, 3 the stage score is Sck=¼∑Nkj, j= 1, 2, 3, 4 and K=1, 2, 3.
We obtain matrix S(Scpk) of scores from different stages of a given player p. S is a row matrix (Scpk), k= 1, 2, 3. Let (Scp1, Scp2, Scp3) be for any given player p.
At the end of the game, the player must be evaluated throught his arithmetic mean of scores of his different stages: average (Scpk). However, some players started at Stage 2 or 3 without going through Stage 1.
We define M (75, 75, 0) a constant matrix and a column vector μ, which, for each learner, associates three default scores of a given player p in the three stages ScpD=M*$(\mu p)^t$ with μp= (μi), i=1, 2, 3:
-Si μi=1, Scpi=0 i=1, 2 for player p;
- In the conditions of age and digital proficiency allowing starting at stage 2, $(\mu)^t$=(1, 0, 0) ;
- In the conditions of age and digital proficiency allowing starting at stage 3, $(\mu)^t$=(1, 1, 0) ;
-In the rest of the cases, $(\mu)^t$=(0, 0, 0).
Given Sp(Spi) i=1, 2,3 the matrix of final scores by the stage of player p with Spi=ScpDi+Scpi
Final score: F= Average (Spi, i=1, 2, 3) or F= ⅓∑Spi, i=1, 2, 3

4 System prototype and evaluation

The described architecture made it possible to implement an online awareness platform cyberssecurityawareness.com.

4.1 Use tools

For our databases, we chose the MONGO DB. In this application, NoSQL is favored over SQL. This method is suitable for high-speed parallel activities. The number of accesses is unlimited. The SQL-pending trap has been avoided.
JavaScript, as opposed to other languages, uses fewer hardware resources to execute the tasks. A computational load occurs on the server side. Most browsers support said language, and there is an adaptation of the display. A script was provided to switch to another language.
We used cacoo.com to represent the Logical Data Model and WinDesign for UML diagrams.
Front-end server, we use ReackJS, and NodeJS for the back end to insure adaptability.

4.2 Conceptual Data Model (CDM

To provide an abstract representation of the reality of the application, we propose the Conceptual Data Model below (Figure 10). It presents entities involves in collection of data and their properties, such as user model, study profile model, domain model (awareness domain), evaluation profile model, user privilege model, rang model, stage model, level model, question model. Each learning (tutorial model) is linked to a level and a level is that of a stage. The evaluation of learning consisted of questions and answers to ensure remediation.

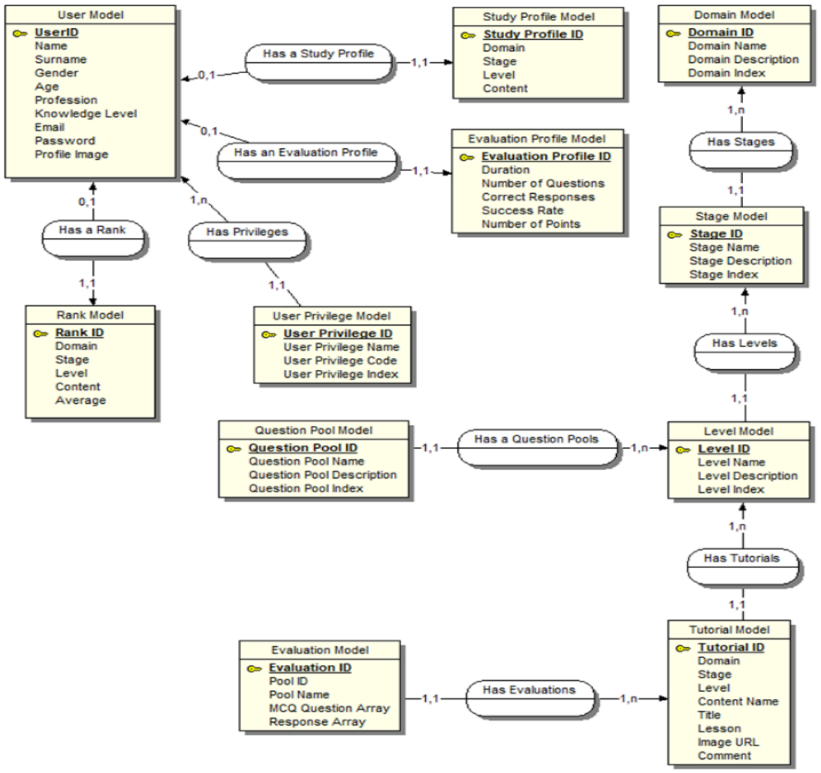

Fig. 10: Conceptual Data Model (CDM)

4.3 Use case diagram

The diagram in Figure 11 made it possible to highlights the possible actions of the administrator or the user in the system.
The administrator can create an awareness domain, learning stages, and stage levels. For a given stage, he is called upon to create tutorials with their prerequisites as well as evaluations by recording the questions and answers.
The user is called upon to register, connect, start/continue learning the prerequisites for the assessment, and simply choose to self-assess.

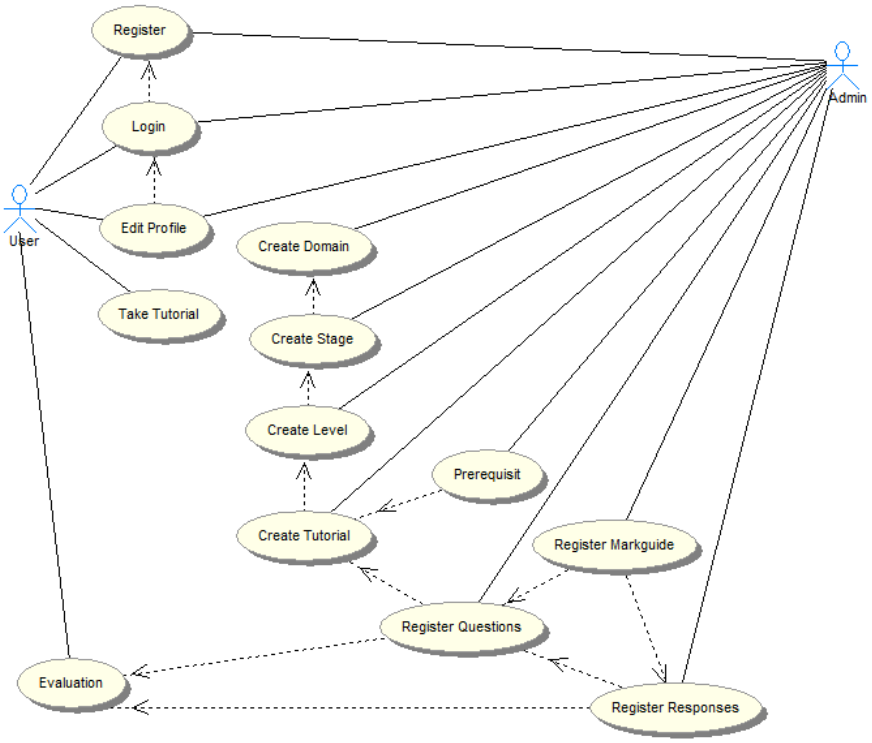

Fig.11: Use case diagram

4.4 User activity diagram

Figure 12 presents the interactions between the system and the user. The question presents the responses of the system to the user, the expectations of the system, and the actions to be carried out.

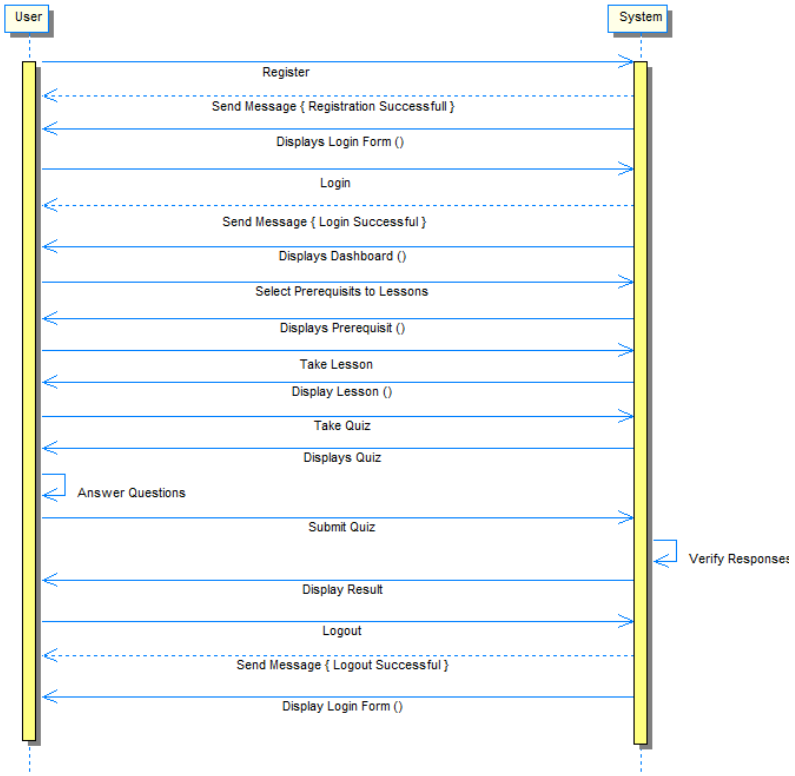

Fig. 12: User activity diagram

4.5 User state diagram

Figure 13 shows the different states of the proposed application. Users visiting the platform must complete a registration form. After registration, he was able to connect and see his profile. In this profile, he begins or continues the awareness process.

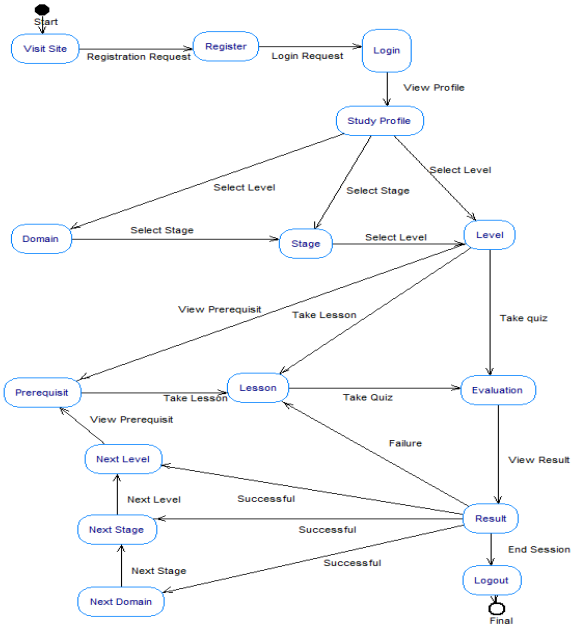

Fig.13: User activity diagram.

4.6 Presentation of interfaces

Those interfaces allow one to choose whether to register or log as an user or an administrator.

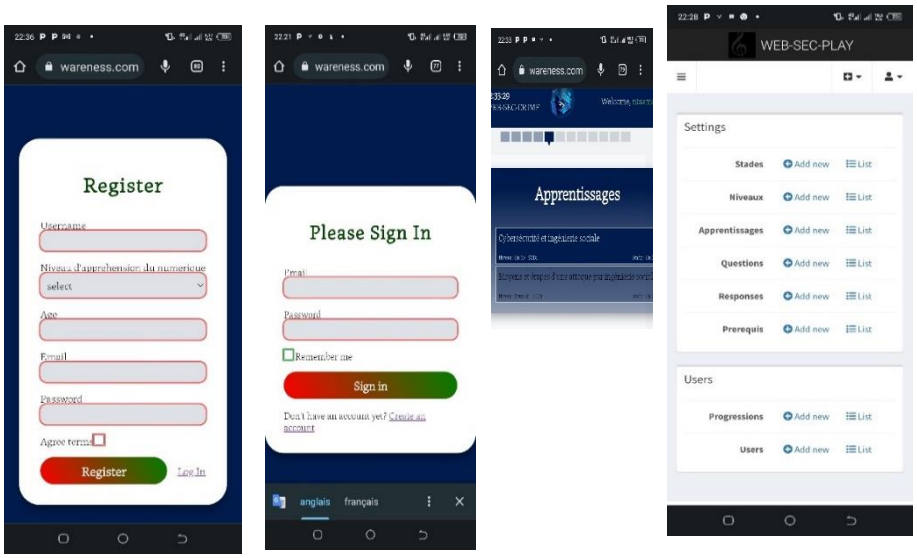

Fig.14: prototype Interfaces

4.7 Evaluation of the solution and discussion

In this section, we highlight the benefits of the proposed architecture through evaluation. The prototype exists online through the link www.cyberssecurityawareness.com.

The assessment was based on the objective criteria. We based our study on the following criteria: the robustness and flexibility of the solution, and didactic and pedagogical innovation in improving the target's experience. Robustness refers to the capacity of the system to remain operational and resilient to possible limitations and pedagogical innovation refers to question old pedagogic pratices versus those proposed in this architecture and check if they can be generalize or give better results in a long term perspective.

The robustness and flexibility of the architecture

The adopted architecture makes a clear distinction between the front and back ends, which guarantees flexibility. Therefore, the same data can be used in several applications. In addition, the platform is scalable with reusable modules, the possible addition of sub-applications, and functionalities without taking the application offline or "hot update." Portability is ensured by deploying the platform on desktops, laptops, tablets, and smartphones. In the development process, the aforementioned separation allows a better division of labor between the front-end developer and the back-end developer. The choice that the front-end and the back-end are all developed in JavaScript is to take advantage of the speed of this language. In addition, unlike other languages, JavaScript uses fewer hardware resources to perform tasks. A computational load occurs on the server side. Most browsers support said language, and there is an adaptation of the display. A script was provided to switch to another language (translation). DB was used for the MONGO database. In this study, we favored NoSQL over SQL because it is suitable for high-speed parallel activities. The number of accesses was unlimited. The pitfall of SQL waiting for any update of any resource in use is avoided.

Didactic and pedagogical innovation in improving the target's experience.
Didactics considers two essential questions: the content taught and the way of teaching; it is at this stage that educational theories come into play. The gamification immerses the learner in a virtual environment. It integrates elements of motivation, emulation, commitment, evaluation, remediation, and self-evaluation through the introduction of game elements such as points, score bars (individual or team), leader boards, and avatars, among others. Evaluation is very important in the teaching/learning process, and it is necessary to be aware of the initial state at all times, the progress made during the learning process, and the efforts to enhance the learning process. Our gamification is mixed, and considers both content and users. It is adaptive, according to the learner's profile. The principle of the Flipped Classroom pedagogy was applied. The user can first learn the subject before tackling it. We were flexible in remediating the questions that the learner did not find, and for a score below 70 percent. Simultaneously, both individual and collective work must be valued. Pedagogical approaches are accessible to all, with the aim of enabling real learning to develop competence. At the same time, effective consideration of the psychological development levels, profiles, and needs of users is needed in order to improve their experience. The provision in this model of the best didactic means allows an awareness capable of leading to real learning to escape the increasingly sophisticated traps of cybercriminals and to create a critical mass for collective resistance to the phenomenon. The educational community has a flexible tool that can be adapted to the curricula, languages, and disciplines. In distance education, which is in progress at the Ministry of Secondary Education, this platform, in addition to content and exercises, provides evaluation, which is an important part of any teaching-learning activity. Moreover, making learning fun brings commitment, motivation, and emulation without which we observe a disinterest in the target. However, this work should, to reach the majority of children under 13, rely a little more on staging audio animations, and this approach should have more facilities to reach them.

5 Conclusion and perspectives

The choice of an appropriate gamification architecture and the use of automatic learning techniques [11] can make it possible to bring the didactic approach closer to the learner and his experience. Companies must emphasize their level of awareness and competence to act in a professional context to avoid being easy prey. Moreover, since cyberspace is not a domain reserved for a few elite, young people would benefit from starting awareness very early with easily accessible tools to protect themselves and thus create a critical mass ready for collective resistance to the phenomenon. However, there is a thorny problem with the best didactic means allowing awareness, which leads to real learning to escape the increasingly sophisticated traps of cybercriminals. The perspective of this work is to integrate the conversational model of artificial intelligence through Chabots to make our gamification more adaptive, as in [28][34], and to carry out tests on a sample of hundreds of individuals simultaneously. The architecture describes here do not consider emotions of the learner.

References

1. Datta P. December. The promise and challenges of the fourth industrial revolution (4IR). *Journal of Information Technology Teaching Cases* (2022). doi:10.1177/20438869211056938
2. Ntsama, J.E., Tchakounte, F., Tchakounte Tchuimi, D., Faissal, A., Fotso Kuate, F. A., Effa, J. Y., Udagepola, K. P. & Atemkeng, M. In: Saeed, R.A., Bakari, A.D., Sheikh, Y.H. (eds) Towards new e-Infrastructure and e-Services for Developing Countries. AFRICOMM 2022. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 499. Springer, Cham. https://doi.org/10.1007/978-3-031-34896-9_19
3. Benavides, E., Fuertes, W., Sanchez, S., & Sanchez, M. (2020). Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. In Developments and advances in defense and security (pp. 51 64). Springer.
4. Shie, E. W. S. (2020). Critical analysis of current research aimed at improving detection of phishing attacks. Selected computing research papers, p. 45.
5. Ho, H.T.N., Luong, H.T. Research trends in cybercrime victimization during 2010–2020: a bibliometric analysis. SN Soc Sci 2, 4 (2022). https://doi.org/10.1007/s43545-021-00305-4
6. Andzongo, S. Au Cameroun, la cybercriminalité fait perdre 12,2 milliards de FCFA à l'éco- nomie en 2021 (Antic). https://www.investiraucameroun.com/gestion-publique/0703- 17600-au-cameroun-la-cybercriminalite-fait-perdre-12-2-milliards-de-fcfa-a-l-economie- en-2021-antic, last accessed 2022/08/19.
7. Piaget, J. et al., la formation du symbole chez l'enfant : initiation, jeu et rêve, image et représentation, Harmattan, 1978, 310p
8. Schell, J. (2008). The Art of Game Design : a Book of Lenses. CRC Press. Seaborn, K., & Fels, D. I. (2015). Gamification in Theory and Action: A Survey. International Journal of Human-Computer Studies, 74, 14–31. https://doi.org/10.1016/J.IJHCS.2014.09.006
9. N. Yue, "Computer multimedia assisted English vocabulary teaching courseware," Int. J. Emerg. Technol. Learn., vol. 12, no. 12, pp. 67–78, 2017. https://doi.org/10.3991/ijet.v12i12.7955
10. Arakpogun, E.O., Elsahn, Z., Olan, F., Elsahn, F. Artificial Intelligence in Africa: Challeng-es and Opportunities. In: Hamdan, A., Hassanien, A.E., Razzaque, A., Alareeni, B. (eds) The Fourth Industrial Revolution: Implementation of Artificial Intelligence for Growing Business Success. Studies in Computational Intelligence, vol 935. Springer, Cham (2021).
11. Eric Sanchez, Shawn Young, Caroline Jouneau-Sion (2019), Classcraft : de la gamification à la ludicisation
12. Cybermuna (2019), www.cybermuna.com.
13. Kanmogne Wabo, L. Increasing user knowledge on email phishing scams in cyberspaces : a gamified system, Master thesis, Department of Mathematics and computer science, University of Ngaoundere, 2019.
14. Cyberawareness/girlscout at home (2019), www.girlscouts.org
15. Piaget, J. et al., Psychologie de l'enfant, PUF, 1976, 310p
16. Constantin Xyspas, les stades du développement affectif selon Piaget, Harmattan, 2001, 169p
17. Monterrat Baptiste et Al., Modèle de joueur pour la ludification adaptative d'une plateforme d'apprentissage, Jun 2015, Agadir, Maroc. pp. 348-359
18. Raynal, F., Rieunier, A. & Postic, M. (1997). Pédagogie : Dictionnaire des concepts clés : Apprentissages, formation, psychologie cognitive. ESF.
19. El Bouhdidi, J. (2013). Une Architecture Intelligente Orientée objectifs basée sur les Ontologies et les Systèmes Multi-agents pour la Génération des Parcours d'Apprentissage Personnalisés (Doctorat, Université abdelamalek essaadi).
20. Da Costa, J. (2014). BPMN 2.0 pour la modélisation et l'implémentation de dispositifs pédagogiques orientés processus (Doctoral dissertation, University of Geneva)
21. Zamzami Zainuddin et Al., The impact of gamification on learning and instruction: a systematic review of empirical evidence, Faculty of Education, The University of Hong Kong, Pokfulam Road, Hong Kong, 2020
22. Doise, W. & Mugny, G. (1981). Le développement social de l'intelligence (Vol. 1). Paris : InterEditions.
23. Mohammed Chekour, Mohammed Laafou, Rachid Janati-Idrissi (2019), L'évolution des théories de l'apprentissage à l'ère du numérique, École Normale Supérieure de Tétouan, Maroc, researchgate, 8, 1-6

24. Duplàa, E., & Talaat, N. (2012). Connectivisme et formation en ligne. Distances et savoirs, 9(4), 541-564.
25. Krause, M., Mogalle, M., Pohl, H. , et Williams, J. J. (2015). A playful game changer: Fostering student retention in online education with social gamification. Dans Proceedings ofthe Second (2015) ACMConference on Learning@ Scale (p. 95-102). ACM.
26. Dichev, C., & Dicheva, D. (2017). Gamifying education: what is known, what is believed and what remains uncertain: A critical review. International journal of educational technology in higher education, 14(9), 1–36. https://doi.org/10.1186/s41239-017-0042-5.
27. Jayalath, J., & Esichaikul, V. (2020). Gamification to enhance motivation and engagement in blended eLearning for technical and vocational education and training. Technology Knowledge and Learning. https://doi.org/10.1007/s10758-020-09466-2.
28. Hwang, Susan Helser, Jeux éducatifs sur la cybersécurité: cadre théorique (2021)
29. Ntsama, J. E. approche de Gamification educative pour la cyber-arnaque (2021), memoire de Master, faculte de sciences, Universite de Ngaoundere.
30. Martin Böckle, isabel Micheel, Marcus Bick, Jasminko Novak (2018), A design framework for adaptative gamification application, Proceeding of the 51th Hawaii International conference on system sciences
31. Kapp, K. M. (2012). The gamification oflearning and instruction: game-based methods and strategies for training and education. John Wiley & Sons.
32. Piaget, J. Le langage et la pensée chez l'enfant : Etudes sur la logique de l'enfant. Neuvième édition, D E L A C H A U X ET N I E S T L É, Neuchâtel – Paris (1923)
33. Wallon (H.). L'évolution Psychologique de l'enfant, Libraire Armand Colin, Paris, 1947.
34. S. Bezzina et Al., leveraging gamification in education through artificial intelligence, University of Malta (MALTA), 2022, orcid:0000-0002-8689-3318
35. Duplàa, E., & Talaat, N. (2012). Connectivisme et formation en ligne. Distances et savoirs, 9(4), 541-564