applied sciences

MDPI

Article

A Cloud Game-Based Educative Platform Architecture: The CyberScratch Project[†]

Llanos Tobarra *, Alejandro Utrilla, Antonio Robles-Gómez, Rafael Pastor-Vargas and Roberto Hernández

Department of Control and Communication Systems, Computer Science Engineering Faculty, Spanish National University for Distance Education (UNED), 28040 Madrid, Spain; autrilla14@alumno.uned.es (A.U.); arobles@scc.uned.es (A.R.-G); rpastor@scc.uned.es (R.P.V.); roberto@scc.uned.es (R.H.)

* Correspondence: llanos@scc.uned.es

[†] This paper is an exhaustively extended version of a paper published in Learning Analytics Summer Institute (LASI) Valladolid, Spain, 15–16 June 2019.

Abstract: The employment of modern technologies is widespread in our society, so the inclusion of practical activities for education has become essential and useful at the same time. These activities are more noticeable in Engineering, in areas such as cybersecurity, data science, artificial intelligence, etc. Additionally, these activities acquire even more relevance with a distance education methodology, as our case is. The inclusion of these practical activities has clear advantages , such as (1) promoting critical thinking and (2) improving students' abilities and skills for their professional careers. There are several options, such as the use of remote and virtual laboratories, virtual reality and game-based platforms, among others. This work addresses the development of a new cloud game-based educational platform, which defines a modular and flexible architecture (using light containers). This architecture provides interactive and monitoring services and data storage in a transparent way. The platform uses gamification to integrate the game as part of the instructional process. The CyberScratch project is a particular implementation of this architecture focused on cybersecurity game-based activities. The data privacy management is a critical issue for these kinds of platforms, so the architecture is designed with this feature integrated in the platform components. To achieve this goal, we first focus on all the privacy aspects for the data generated by our cloud game-based platform, by considering the European legal context for data privacy following GDPR and ISO/IEC TR 20748-1:2016 recommendations for Learning Analytics (LA). Our second objective is to provide implementation guidelines for efficient data privacy management for our cloud game-based educative platform. All these contributions are not found in current related works. The CyberScratch project, which was approved by UNED for the year 2020, considers using the xAPI standard for data handling and services for the game editor, game engine and game monitor modules of CyberScratch. Therefore, apart from considering GDPR privacy and LA recommendations, our cloud game-based architecture covers all phases from game creation to the final users' interactions with the game.

Keywords: cloud learning environments; gamification; Learning Analytics (LA); data privacy management; standards; game-based education; cybersecurity

check for updates

Citation: Tobarra, Ll.; Utrilla, A.; Robles-Gómez, A.; Pastor-Vargas, R.; Hernández, R. A Cloud Game-Based Educative Platform Architecture: The CyberScratch Project. *Appl. Sci.* **2021**, *1*, 1. https://doi.org/

Received: 23 December 2020
Accepted: 12 January 2021
Published:

1. Introduction

The increasing employment of new technologies can help people in plenty of fields of our daily life. In Engineering education, practical learning scenarios become essential to achieve applied skills by spreading critical thinking knowledge. There is a need for trained professionals in Engineering to meet the challenges of today's society [1], such as cybersecurity, data science, and artificial intelligence, among others. For instance, the educative system must provide cybersecurity capacities to their population [2]. Our future Engineers must be able to prevent cyber-threats from Internet in a practical way. Some examples for education in cybersecurity are [3–5], as detailed in the next Section.

However, learning certain cybersecurity concepts (especially protocols and procedures) can be tedious or complicated. This especially true if lecturers use traditional techniques based on only material written in digital format. Several actions can be taken to increase the students' motivation within a learning environment [6]:

- Performing practical experimentation or learning by doing.
- Increasing interactivity with the online platform and providing feedback.
- Allowing the process of making mistakes.
- Enabling the students to have the perception of control over their learning progress.

These practical activities acquire even more relevance with a distance education methodology, as our case is. There are several options, such as the use of remote and virtual laboratories, virtual reality, and game-based platforms, among others. In this sense, the teaching and learning process with games improves the students' motivation, reduces dropouts, and their fear of failure. Educational games satisfy the premises mentioned above: experimentation, interaction and feedback, trial and error and control.

According to [6], the students' learning/teaching with games can be seen like three independent or complementary approaches to improve motivation: teaching tools, learning objects and/or gamification [7–9]. In the case of the CyberScratch project [10], the developed cloud game-based educative platform is a teaching tool to learn contents and acquire skills and abilities about cybersecurity subjects. It can be viewed as a learning resource integrated into the instructional design of these subjects. Additionally, the learning process of students in our case considers gamification, since the principles of a game are applied to this process with our game-based platform, as well as the employment of game mechanisms and elements (stories, challenges, scores, hints, and so on). This way, students will be engaged and motivated. The employment of games and competitions keeps participants engaged and motivated with their learning [11].

The main contribution of this work is the design of a cloud game-based educative architecture to innovate in the design of mechanisms for the inclusion of gamification techniques in practical activities aimed in the context of cybersecurity, as well as their integration into the field of education. The deployed cloud architecture will provide a set of flexible interaction consoles, monitoring and data storage, and data privacy management according to European standards. Our previous experience with customized containers for the dynamic generation of platforms [12,13] can be adapted to the requirements of the project.

Therefore, this work first considers all the privacy aspects for the data generated by our games-based platform, by adapting the European legal context for data privacy following GDPR [14] and ISO/IEC TR 20748-1:2016 [15,16] recommendations for Learning Analytics (LA). We also provide implementation guidelines for the efficient management of data privacy for our game-based educative cloud platform. These both contributions are not found in current related works. The CyberScratch project, which was approved by UNED for the year 2020, considers using the Experience API (xAPI) [17] standard for data handling and services for the modules that compose our developed platform. These modules are the game editor, game engine and game monitor. Some efforts have previously performed to standardize the phases of LA [18] for serious games.

The most relevant related works on gamification are presented in the Section 2, some of them are specific in the cybersecurity domain. Section 3 presents our research methodology. Section 4 introduces a set of definitions for the learning and teaching activity with gamification in the CyberScratch project. The cloud platform architecture and structure is also presented. The cloud game monitor implemented for data privacy is detailed in Section 5. The conclusions and future works are detailed in Section 6.

2. Background and Discussion

2.1. Gamification in Education

The past success of traditional video-games has led the scientific community to adapt visual simulation, virtual reality and games to other contexts of application, such as health, education, law, and so on [19–22]. One approach currently on the rise is gamification [7], as a part of the Engineering curricula for education. Gamification can bring significant advantages to the teaching/learning process in terms of practical experimentation, collaborative learning, and an increment of motivation by including challenges or game competitions.

A puzzle-based learning for cybersecurity education is presented in [3]. Its main objective is to help students to analyze attacks, which exploit hardware/software vulnerabilities, and establish the corresponding countermeasures. Some of them are fraud, cybercrime, and Advanced Persistent Threats (APTs). Additionally, a virtual network environment among students with a set of a services is provided in [4]. Authors proved these tools are suitable to acquire cybersecurity skills. The employment of practical activities for training will develop the students' critical thinking skills [5].

Within the gamification topic, a very popular approximation is the use of Capture-The-Flag (CTF) platforms, by providing students with a set of practical challenges and competitions [23]. CTFs are very rich since they have several key elements, among others: quizzes and flags. Quizzes are questions to be answered by users. In contrast, flags are practical challenges to be solved by users, and these are the most interesting. Some of them become available after solving prior challenges. In our particular case, they are about key topics of cybersecurity.

Competitions imply a set of punctuation, depending on the number of clues used during a concrete challenge and, consequently, a dynamic user-ranking. This fact increments the motivation and engagements of students. The collaborative work can also be considered [24]. Once the competition has finished, solutions can be published for review [25]. In [26], an experience in 2015 about a massive competition, was described and discussed. The platform was able to detect flag-plagiarism and generate challenges in an automatic way. Other works [27,28] also includes anti-plagiarism techniques to secure the proposed challenges by encryption. Highlighting the relevance of the inclusion of storytelling as motivation feature in these competitions is also described in [29].

On the other hand, a competition was established in 2017 [30]. Gamification was deployed in a public cloud infrastructure and managed by a controller node. To our knowledge, this is one of the pioneer work using both the cloud and games paradigms. This cloud infrastructure provides a set of Virtual Machines (VMs) and associated web services. The management of VMs by cloud architectures is becoming obsolete, since it is better to employ flexible lighter web-services, which is based on container, as performed in this work.

Additionally, the Git-based competition proposed in [31] is based on defense and attack flags, encouraging users to be more interactive, since they belong to a red or blue team. Challenges can be configured and monitored. This concept is also incorporated to our cloud architecture.

From the point of view of description language definition, several efforts have also been made. In [32], a formal definition language is used for the verification and validation of the configured scenarios. A generation environment of restricted cyber-ranges is presented in [33]. They employ an Artificial Intelligence (AI) engine and a repository of VMs with vulnerabilities to generate a sequence of exploits depending of the user preferences. As detailed in the next Sections, our cloud game-based architecture will also cover this edition phase for faculty with the use of standardized data communication services.

All these features are very valuable within educative contexts. Some initial works can be found in the field of distance education [34,35]. These works state that competitions are very relevant to increasing students' motivation and satisfaction when performing cybersecurity practices. Related to this, a generator of scenarios with traditional VMs is proposed in [36] in the field of security education. The scenario language is defined with XML scripts. Additionally, some efforts have previously performed to standardize the phases of LA [18] for serious games with the use of xAPI [17] for standardization. This xAPI is the standard to be employed in the current work. Engagement and motivation in Massive Open Online Courses (MOOCs) by using gamification is also a topic of interest [9].

2.2. Motivation and Privacy Challenges

The inclusion of games to our learning methodology offers significant advantages, but it is not easy, as introduced in the previous Section. The design of a suitable level of complexity for a security context is complicated [37]. It is essential to track the students' performance during their interactions with the platform, which support practical activities. Helping students to learn in an effective and efficient way becomes a challenge. Data privacy considerations must be also considered.

In the case of difficult competitions, the participants might get frustrated. In easy competitions, its challenging decreases and participants will lose interest. A carefully designed game-based platform should offer various challenges so that all participants with different cybersecurity skill levels would be engaged and motivated by success. A set of useful cybersecurity approaches to increase the students' motivation are [20,38,39] , which have used gamification for cybersecurity in a satisfactory way, from the points of view of law students and remote laboratories. Gamification is a part of the instructional design in the course.

The use of gamification in educational settings must be validated through evaluation metrics that allow us to know if they are effective or not. To achieve the above goal, it is necessary to add mechanisms on how to obtain information and data on that platform's interaction. That is to say, we must use learning analytics (LA) techniques based on such data. In the specific case of cloud platforms, such data management becomes very relevant since mechanisms of privacy and ethical use of such data must be provided. There is a lack of proposals which consider standards to manage an LA process and privacy regulations at the same time, as our cloud game-based educative platform incorporates.

According to this, some initial efforts have been performed. Within the field of LA, addressing issues for ethics and privacy is a topic of interest that is being addressed, since it is a problem that must be solved [40]. A process must be carried out that consider ethics and data privacy in all phases of the process. In 2015, a code of good practices at an institutional level for LA was proposed by [41] and updated in 2018. JIST is a non-profit organization that supports educational and research technologies, being supported by various European projects, such as the LA Community Exchange (LACE) project [42]. It was deployed in the Open University of the United Kingdom. Another relevant project is the SHEILA project [43], for developing a privacy data framework for educative institutions.

Both the new General Data Protection Regulation (GDPR) [14], and the ISO/IEC TR 20748-1:2016 standard [16] have been adapted to our purposes. This way, great transparency and suitable privacy of data must be achieved at an institutional level. An initial approach has been deployed in the CyberScratch project, as presented in the next Sections.

3. Research Method

The research methodology of this work is framed within the CyberScratch innovation project [10,37], approved by the UNED for the year 2020. The main objective of this project is to use gamification to improve the learning process of students within cybersecurity subjects. In our case, with the UNED's own distance methodology. Therefore, the use of cutting-edge technologies becomes more relevant, so that practical activities are attractive to the student. When using distance methodology, it is more complex to have an instructional design process that motivates students.

The main specific objectives of the CyberScratch project:

- Development of challenging competitions with games.
- Customizing the context of the game depending on the profile of participants.
- Creation of motivating and engagement games with complex stories and sequential and concurrent challenges.
- Monitoring of the students' actions and data privacy management in the developed gamed-based cloud platform.

To fulfill these objectives, a first step is the definition of a description language for scenarios and an editor for helping lecturers to create games. A game definition is composed by the game history diagram, several resources that are needed for the game development and a template in order to personalize the gamer experience. The result of the creation of a game is game package. Once the game is imported into a cloud platform. The game XML definition is used to create the game dynamics for each player. Further details about the CyberScratch framework are given in the next Section.

One of the most relevant aspects of this teaching innovation project to maintain the privacy of the data and manage it in an appropriate way, in accordance with the existing standards of data privacy and information communication through lightweight web services. The whole life cycle of LA have also followed with the guidelines of ISO/IEC TR 20748-1:2016 [15] (Information technology for learning, education and training—Learning analytics interoperability—Part 1: Reference model), as it will be seen in next Sections. Additionally, our developments have been hosted in the cloud.

The ISO/IEC TR 20748-1:2016 is a model focused on dealing with aspects related to the interoperability required by the technological systems when analysing the learning/teaching process of students. In our case, the use of game architecture in the cloud for distance education in cybersecurity, in which LA techniques are used to improve the quality of courses.

This fact includes the definition of various key concepts, user requirements, work-flow and information transfer, as well as aspects related to how a technological architecture is developed with the guidelines offered by the ISO/IEC TR 20748-1:2016. In particular, in the 6th clause, the phases of a LA cycle-file is specified. In addition to this, GDPR [14] will be used to establish the protocols of handling data in a legal and ethical way. This regulation is the general data protection law approved by the European Union in April 2016. The GDPR rights have been correlated with the LA phases to establish privacy of educative data and its efficient management.

Figure 1 shows all the phases of a whole LA process: Learning and Teaching, Data Collection, Data Processing and Storing, Data Analyzing, Data Visualization, and Feedback and Recommendation.

- Learning and Teaching. This phase corresponds to the game definition and all elements involved in the learning and teaching process when gamification is employed.
- Data Collection. A set of generated data during the interactions of participants with the game-based cloud platform must be collected. As we will see later, data privacy considerations have to be studied.
- Data Processing and Storing. Data is processed to select the most relevant information and is stored. In our case, several communications and record elements are used for this purpose in the cloud.
- Data Analyzing. Once we have all data, this data is analyzed employing several techniques, in order to take decisions and help students with the game. It is an internal mechanism to provide hints in the game, with bot characters conversations, and so on.
- Data Visualization. Students are provided with progress visualizations about all game participants in order to keep motivation among them. Data visualization also helps faculty the take these decisions about the students' learning.
- Feedback and Recommendation. Some reports are generated about the state of the activities, students' progress, and other relevant information, as well as a set of recommendations. Two types of reports are generated, one for the student and another for faculty. During the game, the platform will provide alert messages to report about students at risk or unusual situations.

This work will focus on the learning and teaching activity, data collection, and data processing and storing, as detailed in the next Sections.

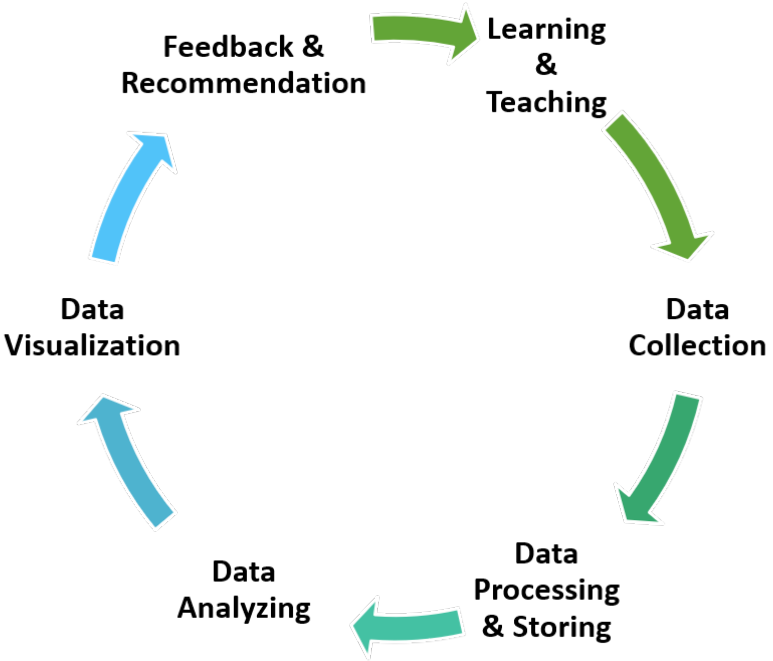


Figure 1. LA cycle following the guidelines of ISO/IEC TR 20748-1:2016.

4. Learning and Teaching Activity

From the perspective of our CyberScratch project, the learning process of students takes place by means of a game. For this reason, the introduction of a set of definitions about the game and its elements becomes essential, as well as the proposed CyberScratch framework for the instructional design of a course in a cloud environment. The cloud game-based educative platform is also presented.

4.1. Game Design

4.1.1. Pedagogical Model

The cloud game-based platform supporting the CyberScratch project is not a game itself, it is a platform oriented to host games; a game editor module has been build to be detailed later, by taking into account some guidelines for integrating gamified learning in online courses. This platform will be named CyberScratch for simplicity.

The game design process is mainly guided by educational competences associated with the learning context. The term educational competences describes a set of capabilities and knowledge that students must achieve. From these competences, a group of learning objectives are derived, that express the learning outcomes. In our context, a general common objective is acquaint students with practical cybersecurity concepts and techniques, but, this global objective can be refined in each game into more detailed objectives. These objectives must be adapted to the intended audience in terms of complexity inside the game. Finally, selected activities related to fine-grain objectives are selected as content to teach. All this process is supported by the game editor, that register existing activities as basic blocks for game creation.

Additionally, the CyberScratch platform has been designed according to gamification patterns described in [44], where gamification can be defined as "the use of gamification design or gamification elements and play to nonentertainment purposes". The gamification main instruments are adapted in our proposal as follows:

- Achievements. As many missions are completed by a player more progress he/she achieves in the game. Missions are grouped into cases. A game is a set of cases, but, in order to avoid frustration, hints are provided. And some missions are key missions that ends other auxiliary missions.

- Rewards. Recognition for effort and skills developed are recognized by the experience. There are several rankings based on points through the game: general game ranking and each case ranking. When a team solves a mission they receive an amount of points which depends on the particular game design. Additionally, at the end of each case, students can report their solution as a write-up. Students can vote other write-ups so authors get recognition.
- Story. The designer of a game must create a story that unfolds throughout the various cases and missions that make up the game.
- Customization. Teams can personalize a set of features, such as avatar, name, and so on.

These instruments in combination with the game mechanics are oriented to achieve the proposed learning outcomes while students are engaged and motivated.

Effectiveness of this approach is going to be evaluated with the combination of a qualitative statistical analysis of the registered data in the platform by means of xAPI standard and TAM (Technological Acceptance Model), as it is described in Section 4.4.

4.1.2. Game Mechanics

The mechanics of a game hosted in CyberScratch, that implements previous instruments, are based on CTF competitions combined with traditional platforms games. On one hand, each game is composed by several levels (cases), where players must complete several missions. Each mission is a practical challenge to be solved by finding a passphrase called flag. Some of these game patterns are identified following the description of [45] and analyze using Machinations tool [46] (see Figure 2).

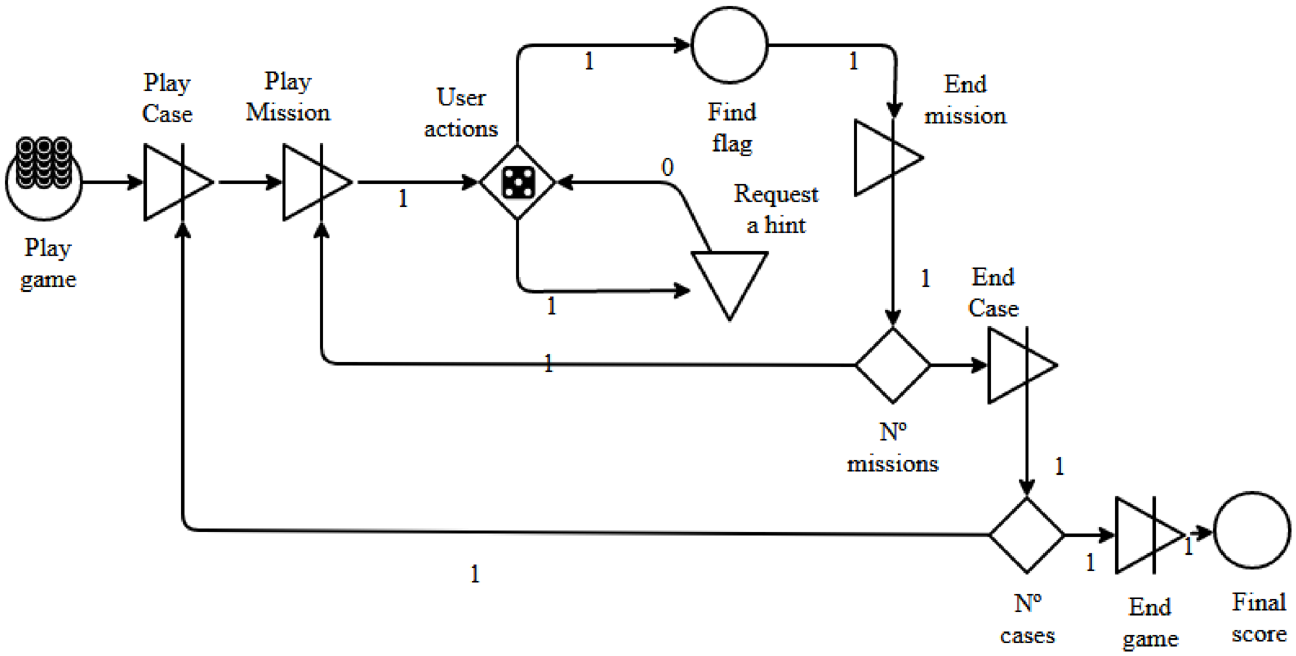


Figure 2. Game pattern diagram using Machinations [46].

Figure 3 shows the whole conceptual structure of the game definition. In the context of the project, a game will conceptually be made up of a set of cases. At least, one case must be defined. Several characters interact among them and with the cases of the game. In this case, it does not make sense having only one character.

A case consists of a concrete context and a story, and one or several missions. The development of the missions can be sequential or concurrent. Some parts of the case can be sequential, whereas other parts are concurrent since a mission is available after solving some previous events. As for missions, some of them are key for solving the case. Once they are solved, the rest of the active missions are closed. The mission order is determined using two attributes, both the previous mission and the cancel events.

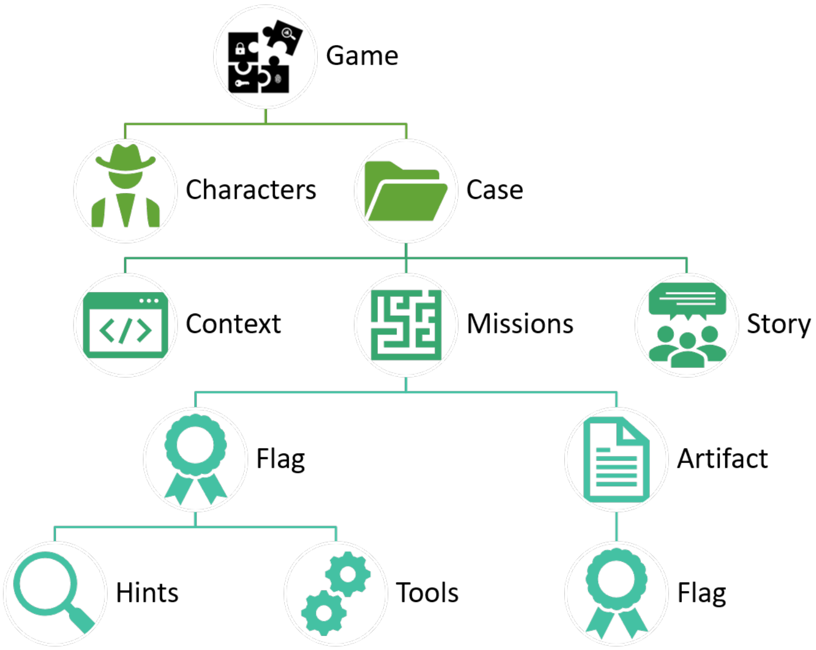
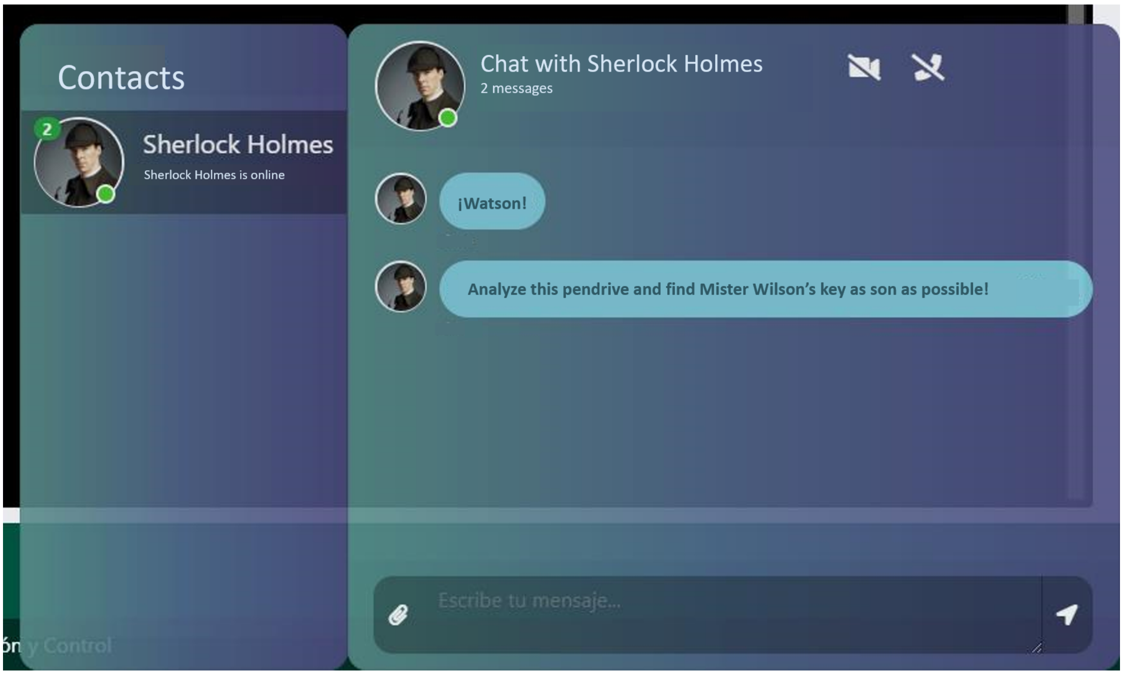


Figure 3. Conceptual structure of the game definition in CyberScratch.

Each mission is guided by some artifacts and a story, although it may be guided by several stories, making a crossover of cases. The story element contains several messages, such as a video, an audio file, an HTML fragment or a PDF file with the story's narration. These messages can be used to train a character bot. This last option allows players to chat with bot characters. An example of chatbot for our cloud game-based educative platform can be observed in Figure 4.



¡Watson!

Analyze this pendrive and find Mister Wilson's key as son as possible!

Figure 4. Chat-bot for the cloud game-based educative platform [37].

According to this, a mission is solved when the player finds a flag. From the point of view of the game, each case can have associated one or more artifacts. These artifacts can have associated a file (a image, a document, a memory image, a system, etc.) and some hidden information, the flag. When the artifact is a file, artifact can be updated to inject a randomized flag. Hidden data is generated by the execution of a command with a set of parameters. Other artifacts can be generated on the in run-time. Another interesting parameter about artifacts is the score, which is used with a concrete value if a mission is solved. A mission must be defined at least, including the mission's flags. A schematic representation of the game flow is given in Figure 5.

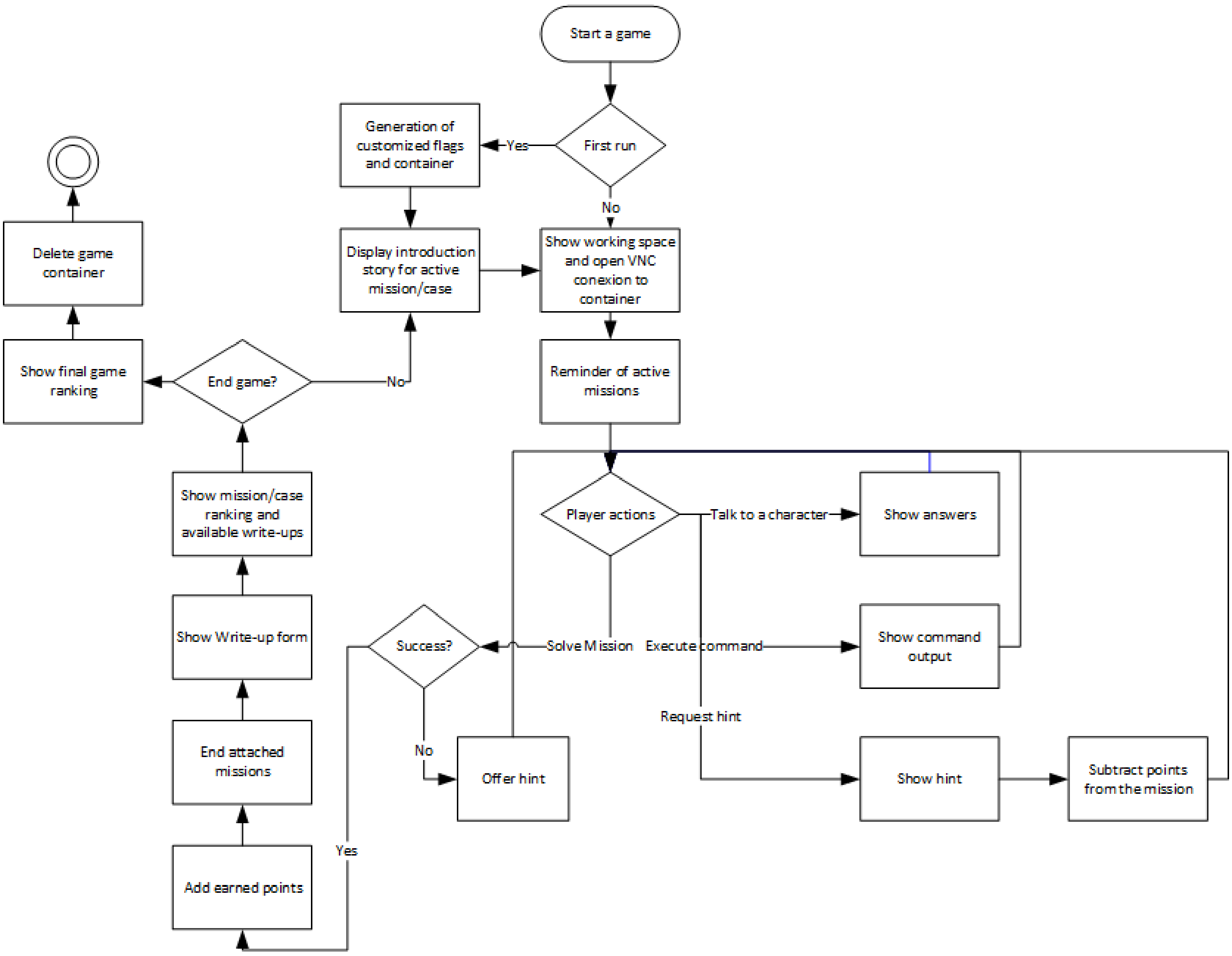


Figure 5. Schematic representation of the game flow. ◯ is the start of the game. ⊚ is the end of the game.

The CyberScratch framework is described in the next section with the following modules: game editor, game engine and game monitor. The last one is the core of data privacy considerations.

4.2. The CyberScratch Framework

In this section, the proposed framework for the CyberScratch project is described, as observed in Figure 6. This is composed by next components:

- *Game Editor*. This module helps faculty to create and edit a new game package by means of a graphical editor. A game package is composed by a game definition document (with a JSON/XML format), several multimedia resources (videos, audios, images, and so on) and a docker-file for the deployment of virtualized containers [47]. The XML/JSON definition of the game is used to create the game dynamics for each player. Game packages can also be imported and exported thanks to this module.

- *Game Engine*. The component handles the game dynamics so that players can start a new game. It also allows players to interact with characters, retrieve hints to get help and check the solutions of the different game challenges.
- *Game Monitor*. It manages the user profiles, records the different activities as xAPI statements, offers visualizations of the participants' progress, and handles the user's consents for data privacy. This module is the core for LA purposes and the principal objectives of this work. For this reason, it will be exhaustively detailed in the next Section.

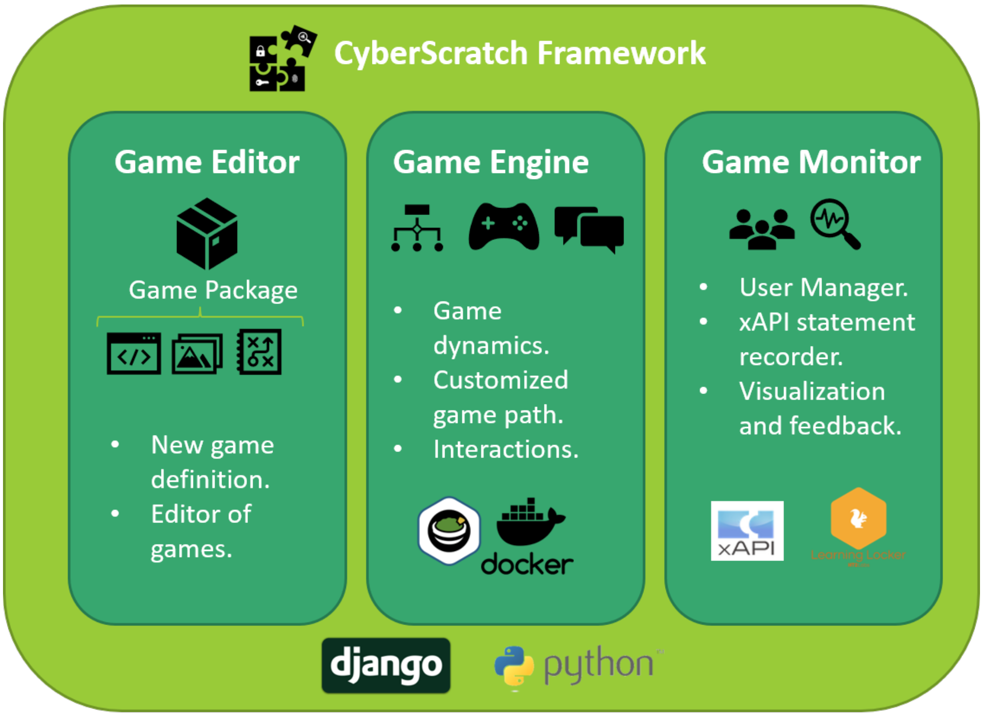


Figure 6. Proposed game architecture for the CyberScratch framework.

4.3. The Cloud Game-Based Educative Platform

Once detailed the main components of the game-based platform, we must define their functional dependence with the corresponding modules deployed in the cloud. It is important to emphasize here that a primary objective of the Cyberscratch project is to provide the gamification environment and define a flexible architecture in the cloud that allows the deployment of similar solutions. These gamification solutions can be based on other different technologies and areas, but the generated architecture aims to provide the essential services: interaction consoles, monitoring, data storage, and data privacy management according to European standards for data privacy management. With this architecture, it would be possible to generate new solutions for gamification in the cloud, adapting other solutions [48].

In this case, our principal interest is to propose a cloud gamification learning environment for cybersecurity courses. Additionally, we will get a full prototype to demonstrate the cloud environment's viability and architecture for gamification. For this reason, it is necessary to detail the cloud-based educational services and infrastructure, which support this platform from the point of view of technical detail, to manage data with cloud computing educational approaches.

Figure 7 shows the structure of the proposed architecture for our cloud game-based educative platform. This is composed of several layers: (1) the CyberScratch framework; (2) a control plane, in order to automatically manage the load-balancing for and support hardware failures at a network level, with Kubernetes [49]; and (3) a cloud provider, such as Amazon AWS [50] or Microsoft Azure [51].

Layers 2 and 3 are game agnostics/independent so, we can transparently reuse these layers. The CyberScratch framework components are specific for the created game but can be easily adapted to new games and connected to layer 2. Additionally, the game monitor component is designed to be compliant with data privacy management guidelines. This component gets the interaction data from the game engine and stored it on layer 2 (xAPI sentences database, Learning Locker). The game editor manages all the accesses to this information, so it makes a secure architecture. The game monitor must be only configured for the particular scenario, and there is no need for rebuilding this component. The game engine and game editor components are specific for the game objectives so in other projects must be built/developed/integrated and adapted to the architecture. This way, to reuse the architecture, game developers only have to provide the game engine and editor components.

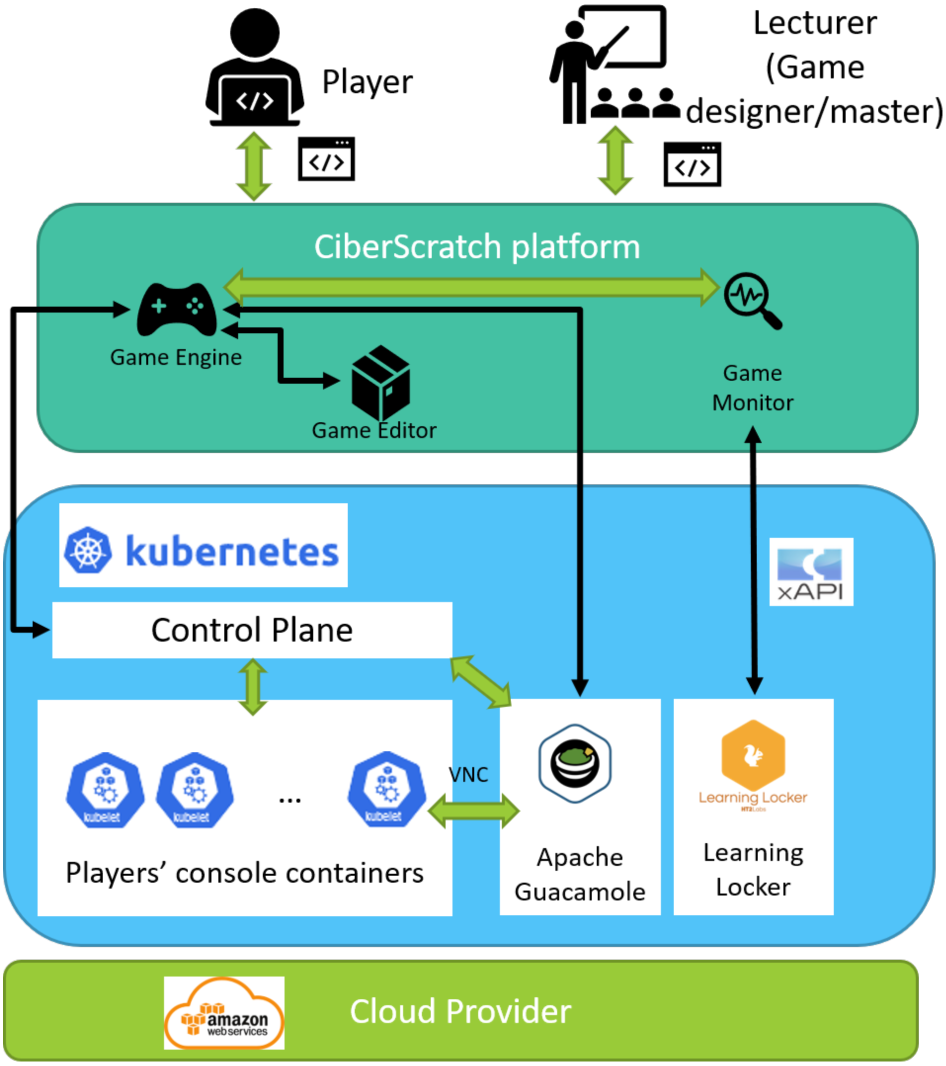


Figure 7. Architecture of our proposed cloud game-based educative platform.

The game editor allows to instructors the inclusion of game resources which be combined with container templates in order to create specific Docker container for the player console. Docker-containers are deployed as required by players using Kubernetes (with provides high availability), instead of employing traditional VMs. This technology is more flexible and with a higher migration. Each container is remotely accessed utilizing the Apache Guacamole project [52] for the cloud game-based educative platform. The proposed game platform have been developed using the Django web framework [53], but it can be easily deployed as other Kubernetes container.

The employment of Docker containers in our educative platform has several benefits. The main advantages of using virtualization through Docket-containers are the following:

- Independence in the file system in each container.
- Independence of resources allocated to each container.
- Each node in a virtual container network operates autonomously, just as if it were a physical network.
- Change management capacity.
- Interactive interfaces in real time.

One of the main current standards that allows the collection of information about the activity produced in an educational environment is xAPI [17]. This standard provides a way to record the activity through sentences with a predefined format and a secure mechanism to access them from a Learning Record Store (LRS). The xAPI standard can be seen as the next generation of SCORM. The LRS is a repository, which stores the data generated from a learning experience.

In addition to this, we have selected Learning Locker [54] as LRS, and adapted it for our purposes. One of the main advantages of this software is that can be easily deployed in several famous cloud providers. In our case, Amazon AWS was chosen. Our institution has several agreements with this and other providers Additionally, scalability and availability of our development will be higher. The migration to the cloud and continuous development is very intuitive, since the technology is based on Docker containers. The sentence transmission from client-side, from the CyberScratch platform towards the cloud LRS, has been secured in order to prevent the exposition of sensitive data to malicious users.

4.4. User Satisfaction

When creating a new learning scenario, faculty can build and customize learning scenarios and incorporate to a virtual course. These scenarios will be available for students in order to acquire a competence of the course. In order to evaluate our cloud game-based educative platform, an opinion survey will be filled out.

From this information, a Structural equation Model (SEM) will be proposed and analyzed by using the TAM methodology [55]. This model can be used to measure users' attitudes over a new technology, so determining their intention to use it in a particular context [56]. This way, a set of acceptance constructs/factors will be studied, in order to check the perceived usefulness, perceived ease of use, users' attitude towards the platform, and their intention to use in the future for other purposes. All statements for each of them are detailed in Appendix A.

These constructs/factors are:

- *Perceived usefulness*. It is the usefulness perceived by the user when using the cloud game-base educative platform.
- *Perceived ease of use*. It is the effort perceived by the user when using the cloud game-base educative platform.
- *Attitude*. It is the users' resistance of using the cloud game-base educative platform, and its benefits of usage for practical activities.
- *Intention To Use*. It is the possibility of using this type of technology for other experiences in the future.

The educative context will be focused in the subject "Cibersecurity" with a distance learning methodology. It covers network security principles from a practical approach. For this reason, our cloud game-based educative platform meets the necessities of this subject.

5. Cloud Game Monitor

The cloud game monitor in the CyberScratch project is the key, where data is being managed. This module must take into account data privacy implications. Apart from data privacy, it is also essential for LA purposes in order to establish procedures to collect, process and store data in an efficient way. The management of the LA process will be transparent for the user of the cloud platform. For both cases, several data privacy and communication standards are established and adapted to our project.

5.1. Data Management

xAPI has been used with great success as an activity record mechanism in various educational tools in recent years [18,57,58], as well as incorporated from multiple Learning Management Systems (LMSs). Therefore, this standard is used as a tool to manage the recording of the activity of the participants. This way, it is possible to reuse existing LA techniques and integrating them to our CyberScratch project. Our LRS will be hosted in the cloud.

Each xAPI statement represents an event that has taken place within our educational application. An xAPI statement is composed of three main elements:

- *An actor*. An actor must have an associated account in the educational platform. From our perspective, there are three main actors available in our environment: the teachers, the players (the students) and the students' groups.
- *A verb*. Verbs are actions that are represented by URIs, such as access, init, ends, among others.
- *An object*. Within the definition of xAPI, it is the element of the framework on which falls the action (a game, a mission, a case, a flag, a reward . . .).

It is also possible to add more information about the context of the events through an element called *Context*. If desired, we can add a specific element to add information about the result of the action.

The process of designing sentences is performed with the next steps:

1. Listing the relevant events to be recorded for the monitoring of the games. These events must allow lecturers to produce learning reports and, also adapt them and improve the experience of our players. The main registered events in CyberScratch are:
    - Start and ends of each session at the platform. It allows lecturers to determinate the time elapsed. It also allows detecting those students at risk.
    - Start and ends of a game, each case and each mission at the platform. It allows lecturer to determinate the performance of the player and determinate the difficulty level of each challenge.
    - Visualization of a story inside the platform. Lecturers can determine the appealing of the designed stories and the player comprehension of the story.
    - Request of a clue. This event can allow to determine the complexity of the challenge for a player and the need of further support from the lecturer in order to succeed in the game.
    - Artifact download by a player. This event and the next one are correlated with the resolution path of the challenge.
    - Command issued by a player inside her/his console.
    - Try of mission resolution and its corresponding result (failure or success).
    - Creation/joined to a group at the game.
2. Creating a statement template for each event registered, which is detailed in the previous step. For each statement template the following guidelines have to be followed:
    - As defined above, each actor is correlated with an account.
    - Verbs and objects are selected from xAPI Registry [59] and Serious Game xAPI Profile, as stated in [18]. They provide enough verbs and objects definitions that easily fit in our framework.
    - Each statement contains a timestamp with the correct time zone.

- The statement context should contain minimal information. This element is more focused on debugging information rather than educational information.

3. Correlating the existing variables in each template with existing variables in the application.

Once xAPI templates are designed, the point where each statement is built, transmitted and identified. xAPI statements are constructed with the TinCanPython library [60] within the created Python framework. The statements are transmitted towards our cloud LRS.

Once data management has been described, data privacy about our developments is performed next.

5.2. Data Privacy

Accompanying the need to follow the activity of students, we must include in any development project, even more, if it is educational, mechanisms to protect the privacy of data. Democratization for the use of social networks has made society increasingly aware of the growing exposure of personal data in an increasingly global context. In 2018, a survey conducted by the United Nations Conference on Trade and Development [61], 107 countries (58%) had developed data protection legislation, and the 10% were in the process of doing so. In Spain, this is regulated by the Organic Law 3/2018 of 5 December on the Protection of Personal Data and the Guarantee of Digital Rights (LOPDGDD) and GDPR [14]. This privacy of data must also be regulated in the field of education, in which personal data is being managed.

Automation of LA processes are increasingly being integrated into educational institutions and platforms oriented to Lifelong Learning, such as the case of our CyberScratch project. Addressing issues for ethics and privacy becomes essential in all LA phases [40]. In 2015, a code of good practices at an institutional level for LA was proposed by [41] and updated in 2018. JIST is a non-profit organization that supports educational and research technologies, being supported by various European projects, such as the LACE project [42] for the Open University in UK. In the LACE project, the question of the impact of privacy on the area of the development of LA was raised. Another relevant project is the SHEILA project [43], for providing a privacy data framework to educative institutions.

Therefore, there is an increasing development for data protection regulation. It is necessary to follow modern standards that help us to do so, as we propose in this work. Following this spirit of the regulation, the ISO/IEC TR 20748-1:2016 standard [16] have been adapted to our purposes. This way, it will be possible to provide with mechanisms to avoid students' monitoring and manage data control and user identification. This way, great transparency and suitable privacy of data must be achieved at an institutional level. An initial approach is being deployed in the CyberScratch project.

According to this work, each phase must fulfill the following privacy requirements, as shown in Figure 8. Our framework start from these recommendations, as well as the rights that must be guaranteed according to the GDPR standard to include mechanisms that allow us to guarantee them through the different phases of our LA process. As a result, Table 1 represents these relationships, in which each GDPR right is associated to each LA phase. The collected data is basically the recommended by the ISO/IEC TR 20748-1:2016 standard. Our main objective here is to establish a correlation about the LA phases and the GDPR rights.

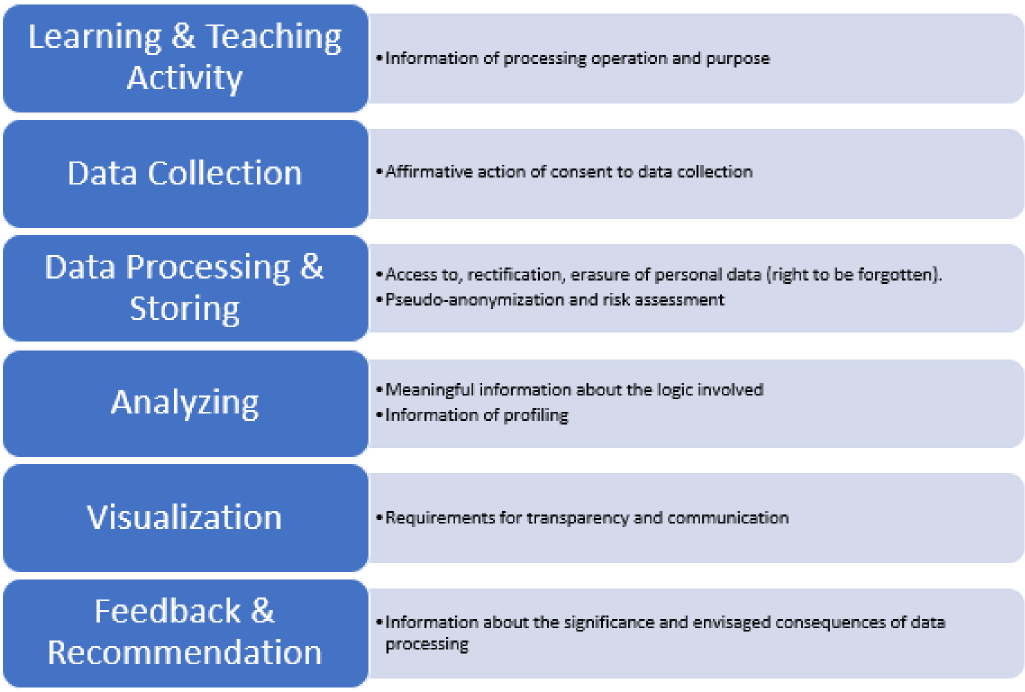

Learning & Teaching Activity
•Information of processing operation and purpose
Data Collection
•Affirmative action of consent to data collection
Data Processing & Storing
•Access to, rectification, erasure of personal data (right to be forgotten).
•Pseudo-anonymization and risk assessment
Analyzing
•Meaningful information about the logic involved
•Information of profiling
Visualization
•Requirements for transparency and communication
Feedback & Recommendation
•Information about the significance and envisaged consequences of data processing

Figure 8. Correspondence among ISO/IEC TR 20748-1:2016 phases and their corresponding privacy requirements [16].

Table 1. Correlation among GDPR rights implementations and the affected LA phases in our CyberScratch project.

GDPR Rights	**Learning & Teaching**	**Data Collection**	**Data Processing & Storing**	**Data Analyzing**	**Data Visualization**	**Feedback & Recomm.**
Right to be informed	✓	✓	✓	✓	✓	✓
Right of access	✓	✓	✓	✓	✓	✓
Right to rectification	✓	✓	✓	×	×	×
Right to erasure	✓	✓	✓	×	×	×
Right to restrict processing	×	×	✓	×	×	×
Right to data portability	×	×	✓	×	×	×
Right to object	✓	✓	✓	✓	✓	✓
Right in relation to automated decision making and profiling	×	×	×	✓	✓	✓

Thus, we have adapted these GDPR recommendations to our CyberScratch framework, which is summarized as follows:

- *The right to be informed*. Our framework does not collect many sensitive mandatory information further than an email account and the actions of the user inside the platform. Users are informed when they first register on the platform by means of a form. This form allows them to consent which treatments of the information they accept. More detailed information is provided through a document that is posted on the project's website and linked to the acceptance form.
- *The right of access*. Users *"shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data"*, cited from [14]. Users can access to the following collected data:

    - Personal information (username, password, name and surname) from the profile section at user menu.
    - Activity data though session reports, showed at "Progress" section. These reports are available to lecturers that evaluate the user's performance of the activity. Thus this fact is also reported to users.
    - Data used for analysis from their personal profile section (as a set of JSON documents), downloadable from "My Data" section.
    - Stored results of analysis from personal performance as visualization from "Progress" section. Some of these visualizations are available to lecturers that evaluate the output of the activity. Thus this fact is also reported to users.

  Apart from the data itself, users are reported about each process objective and the categories of data involved by a privacy report, as it is described in the previous right. Data is not transferred to third parties, being only managed by UNED.
- *The right to rectification*. Users can update their data at the profile area of the framework. They can exercise this right at any time during any phase of the learning analytics process as long as their account is active.
- *The right to erasure* ('right to be forgotten'). Users can request the deletion of their data and their user account from the profile section, but, as LA is an integral part of the course, data can not be deleted until the course is finished. Thus, users will be reported that data will be preserved as long as it is needed for evaluation purposes. After that, it can be deleted.
- *The right to restrict processing*. As it is described in the previous right, data is employed by evaluation purposes. Thus, users can restrict those process which are not fundamental for the framework (mostly research oriented).
- *The right to data portability*. This right states that users *"have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format"*, cited in [14]. As described before, students can download its data as a zipped file ciphered with the same password of user profile from "My Data" section (see Figure 9). From the point of view of faculty, some user interactions can be analyzed as a proof of concept for this characteristic. First, the most popular verbs in statements can be examined. In our example, the logging and logout are the most used. Secondly, the evolution of the activity in terms of statements can be observed along the time, Thirdly, the most active users could be checked. Fourthly, the most popular activities can be visualized. The visualizations can be downloaded from the "Progress" section with PNG format. They can exercise this right at any time during any phase of the LA process as long as their account is active.
- *The right to object*. Users *"shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point"*, cited in [14]. As described, before users are requested explicit consent to each data procedure. The consent received for any procedure can be changed at any time by using the "My Data" section of the user profile. Every changed in this sense is registered in the framework. Some data process are needed in order to the framework work. Thus, if a user do not provide consent, the user account could be disable as a consequence. This fact is reported to the user in conjunction with the process description.
- *Rights in relation to automated decision making and profiling*. None automated decision making is performed inside CyberScratch platform at this stage. Some profiling mechanisms are implemented in order to detect students at risk during the activity. In that case, lecturers are told about this circumstances. This fact does not carry any decision which can significantly affects users. Anyways, there is an email account to retrieve students' opinions in the agreement form about this aspect.

In addition to these mechanisms, security procedures are designed in order to guarantee the accountability and data governance. Thanks to the features of Learning Locke platform, role-based control access and authentication mechanism are configured. Log registry options are also enabled. Periodic audits every six months are also scheduled so the security posture is reviewed. A key procedure is also a breach notification protocol. Our framework follows the protocol designed by UNED, communicating it through the responsible for data protection of the university that will raise the breach to the national data protection agency.

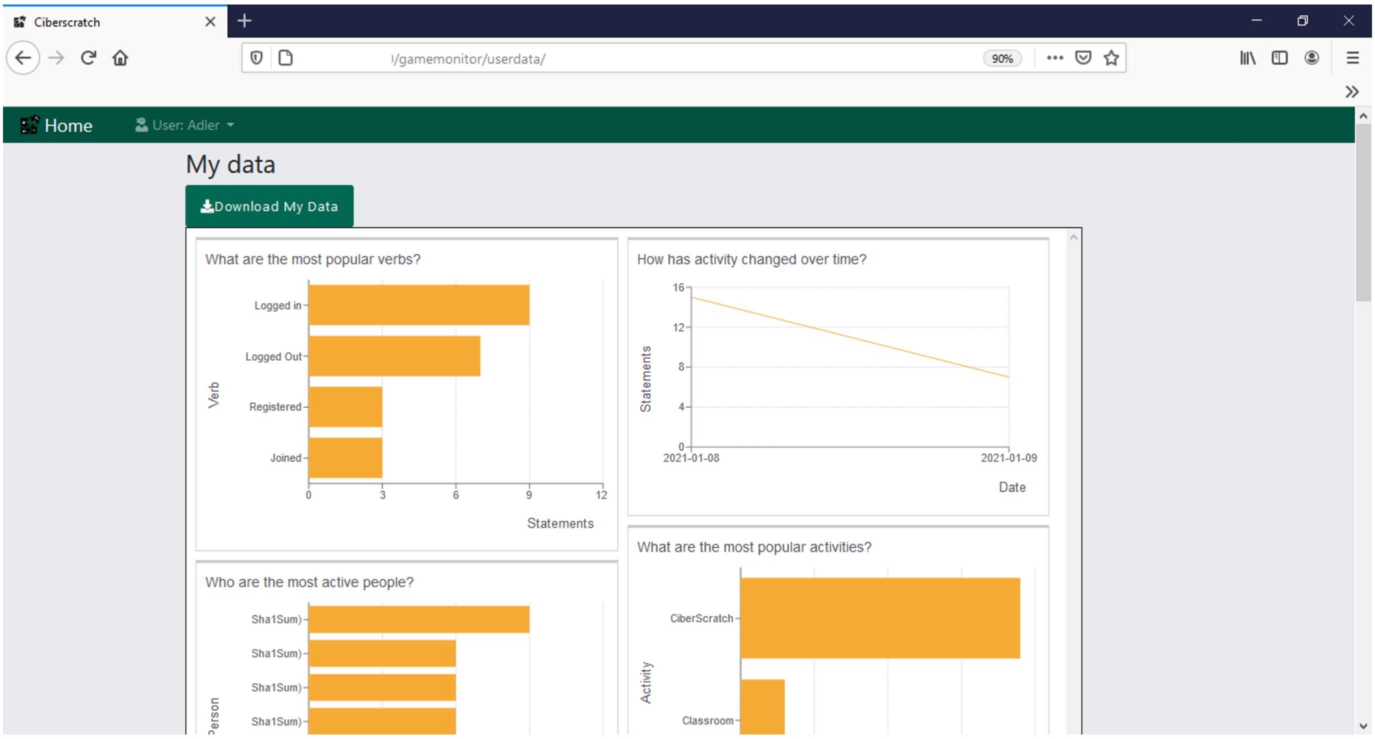


Figure 9. "My data" section in the CyberScratch platform.

6. Conclusions and Further Works

The inclusion of practical engineering subjects is highly demanded nowadays, such as cybersecurity or data science topics. Their main objective is to promote critical thinking and improve a student's abilities and skills, from the point of view of their professional career. The option studied in this work is the employment of a game for educative courses in cybersecurity with a distance methodology. Gamification seems to help students to increase their motivation and engagement in practical activities since this paradigm is based on challenges, hints, and scores [11].

To get the advantages of gamification, we need adequate technological infrastructures to apply these gamification techniques. These infrastructures must be scalable and flexible. The flexibility feature allows instructors to use the infrastructure in different engineering domains. This paper has shown an architecture with these features, which can be deployed as a cloud environment. A particular case, the CyberScratch project, shows how this cloud game-based environment is defined and structured in several components: game editor, game engine, and game monitor. These components are supported by several layers which can be reused for other serious games.

The generated cloud architecture provides interaction consoles, monitoring and data storage, and data privacy management according to European standards. This design characteristic is critical in Learning Analytics (LA) projects, which involves the treatment and use of private data, so the platform is built with the objective of data privacy management. The LA phases are implemented in this work by adapting the ISO/IEC TR 20748-1:2016 recommendations for the LA process. The LA cycle-life is composed of learning and teaching, data collection, data processing and storing, data analyzing, data visualization, feedback and recommendation. We have primarily focused on the first three steps for data management. This way, it is possible to monitor the actions of participants in online courses. The collected data are basically those recommended by the ISO/IEC TR 20748-1:2016 standard. Our main insight with respect to data privacy management is to establish a correlation about the LA phases and the GDPR. Our cloud game-based platform is able to manage data in an autonomous way, without the intervention of the game editor, faculty, and so on.

Students are currently using the platform, and analytical data will be available at the end of the course. This data could be used to verify if this technology enables a concrete way to increase motivation and engagement, as expected. For this purpose, a TAM model will also be used based on the survey presented in Table A1 of the Appendix A. This survey will be carried out after the course by students and instructors. It is intended to improve and standardize the game editor and game engine components concerning the architecture. Right now, these two components are specific-only components implemented for the CyberScratch project. Still, the aim is to define a standard that allows different scenarios based on cases and missions (Figure 3 of the paper). We will also improve the game engine to incorporate popular game frameworks engines (unity, unreal, etc.) to add new capabilities of the component. These new features will enable the instructors to have a general editor to build their games and take advantage of the proposed architecture.

Author Contributions: All authors were involved in the foundation items.

Funding: This work is a part of the CiberScratch PID project for the year 2020, and it is funded by the Universidad Nacional de Educación a Distancia (UNED).

Institutional Review Board Statement: The study did not require ethical approval. No personal information was used in this study. All data was anonymized and aggregated.

Informed Consent Statement: According to the GDPR all the users using the CyberScratch platform have been informed and given consent to the treatment of their data.

Data Availability Statement: Not applicable. The data are not publicly available due to compliance with GDPR.

Acknowledgments: Authors would like to acknowledge the support of the eNMoLabs research project for the period 2019–2021, the CiberGID UNED innovation group with the CiberScratch project, the G-eLios UNED research group, as well as the E-Madrid-CM Network of Excellence (S2018/TCS-4307). The authors also acknowledge the support of SNOLA, officially recognized Thematic Network of Excellence (RED2018-102725-T) by the Spanish Ministry of Science, Innovation and Universities.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

APT	Advanced Persistent Threat
AI	Artificial Intelligence
AT	Attitude
AWS	Amazon Web Services
CTF	Capture The Flag
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITU	Intention To Use
JSON	JavaScript Object Notation
LA	Learning Analytics
LACE	Learning Analytics Community Exchange
LMS	Learning Management System
LOPDGDD	Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales
LRS	Learning Record Store

MOOC	Massive Open Online Course
PEU	Perceived Ease of Use
PNG	Portable Network Graphics
PU	Perceived Usefulness
SCORM	Shareable Content Object Reference Model
SEM	Structural equation Model
SNOLA	Spanish Network Of Learning Analytics
TAM	Technological Acceptance Model
UNED	Universidad Nacional de Educación a Distancia
URI	Uniform Resource Identifier
VM	Virtual Machine
VNC	Virtual Network Computing
xAPI	Experience API
XML	eXtensible Markup Language

Appendix A. Statements for Constructs/Factors of the TAM Model

This appendix shows the statements of the opinion survey, which will be presented to users (faculty and students). Table A1 shows this survey, based on the proposed one in [13]. On the first column the construct/factor identifier for each statement is detailed. The specific statement is specified on the second column. TAM constructs/factors are Perceived Usefulness (PU), Perceived Ease of Use (PEU), Attitude (AT), and Intention To Use (ITU). Each factor is made up of 3 or 4 statements. Users must grade each statement using a five-point liker-type scale. Ranges are from (1) strongly disagree to (5) strongly agree.

Table A1. Survey for the TAM model.

Identifier	Question
PU 1	I find the cloud game-based educative platform very useful for teaching and learning.
PU 2	Using the cloud game-based educative platform allows to do the gamification activities in a more efficient way.
PU 3	Using the cloud game-based educative platform increases the productivity of learning.
PU 4	If I use the cloud game-based educative platform, I think the opportunities of passing the subject are increased.
PEU 1	My interaction with the cloud game-based educative platform has been clear and understandable.
PEU 2	I think it is easy to learn how to use the cloud game-based educative platform.
PEU 3	I find the cloud game-based educative platform easy to use.
AT 1	I think using the cloud game-based educative platform is a good idea.
AT 2	The cloud game-based educative platform increases the interest in the proposed contents.
AT 3	Using the cloud game-based educative platform is enjoyable.
AT 4	I like using the cloud game-based educative platform.
ITU 1	I would like to reuse the cloud game-based educative platform in other activities for distance education.
ITU 2	I would like to access the cloud game-based educative platform to reinforce the learning in a freeway, even if the activity has not an associated score.
ITU 3	I would like to reuse the cloud game-based educative platform in other subjects.

References

1. (ISC)^2. Strategies for Building and Growing Strong Cybersecurity Teams. Cybersecurity Workforce Study. 2019. Available online: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482 (accessed on 23 December 2020).
2. Catota, F.E.; Morgan, M.G.; Sicker, D.C. Cybersecurity education in a developing nation: the Ecuadorian environment. *J. Cybersecur.* **2019**, *5*, 1–19 doi:10.1093/cybsec/tyz001.
3. Dasgupta, D.; Ferebee, D.M.; Michalewicz, Z. Applying Puzzle-Based Learning to Cyber-Security Education. In Proceedings of the 2013 on InfoSecCD '13: Information Security Curriculum Development Conference, Kennesaw, GA, USA, 12 October 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 20–26. doi:10.1145/2528908.2528910.
4. Martini, B.; Choo, K.K.R. Building the next generation of cyber security professionals. In Proceedings of the ECIS 2014 Proceedings—22nd European Conference on Information Systems, Tel Aviv, Israel, 9–11 June 2014.
5. Willingham, D. Critical Thinking Why Is It So Hard to Teach? *Arts Educ. Policy Rev.* **2010**, *109*, 21–32. doi:10.3200/AEPR.109.4.21-32.
6. Molina-Carmona, R.; Llorens-Largo, F. Gamification and Advanced Technology to Enhance Motivation in Education. *Informatics* **2020**, *7*, 20. doi:10.3390/informatics7020020.
7. Nacke, L.E.; Deterding, S. The maturing of gamification research. *Comput. Hum. Behav.* **2017**, *71*, 450–454. doi:10.1016/j.chb.2016.11.062.

8. Santos-Villalba, M.J.; Leiva Olivencia, J.J.; Navas-Parejo, M.R.; Benítez-Márquez, M.D. Higher Education Students' Assessments towards Gamification and Sustainability: A Case Study. *Sustainability* **2020**, *12*, 8513. doi:10.3390/su12208513.
9. Borrás-Gené, O.; Martínez-Núñez, M.; Martín-Fernández, L. Enhancing Fun through Gamification to Improve Engagement in MOOC. *Informatics* **2019**, *6*, 28. doi:10.3390/informatics6030028.
10. CiberGID. CiberScratch (in English, CyberScratch). 2020. Available online: https://blogs.uned.es/cibergid/ciberscratch/ (accessed on 23 December 2020).
11. Jayalath, J.; Esichaikul, V. Gamification to Enhance Motivation and Engagement in Blended eLearning for Technical and Vocational Education and Training. *Technol. Knowl. Learn.* **2020**. doi:10.1007/s10758-020-09466-2.
12. Robles-Gómez, A.; Tobarra, L.; Pastor, R.; Hernández, R.; Duque, A.; Cano, J. Analyzing the Students' Learning within a Container-Based Virtual Laboratory for Cybersecurity. In Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality, TEEM'19, Leon, Spain, 16–18 October 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 275–283. doi:10.1145/3362789.3362840.
13. Tobarra, L.; Robles-Gómez, A.; Pastor, R.; Hernández, R.; Duque, A.; Cano, J. Students' Acceptance and Tracking of a New Container-Based Virtual Laboratory. *Appl. Sci.* **2020**, *10*, 1091. doi:10.3390/app10031091.
14. EP and the CEU: Regulation (EU) 2016/679 GDPR. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679. (accessed on 23 December 2020).
15. ISO/IEC JTC 1.Information Technology SC 36. Information Technology for Learning Education and Training.. Information Technology for Learning, Education and Training— Learning Analytics Interoperability—Part 1:Reference Model. 2016. Available online: https://www.iso.org/standard/68976.html (accessed on 23 December 2020).
16. Hoel, T.; Griffiths, D.; Chen, W. The Influence of Data Protection and Privacy Frameworks on the Design of Learning Analytics Systems. In Proceedings of the Seventh International Learning Analytics & Knowledge Conference, Vancouver, BC, Canada, 13–17 March 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 243–252. doi:10.1145/3027385.3027414.
17. xAPI Specification. 2016. Available online: https://github.com/adlnet/xAPI-Spec/ (accessed on 23 December 2020).
18. Serrano-Laguna, A.; Martínez-Ortiz, I.; Haag, J.; Regan, D.; Johnson, A.; Fernández-Manjón, B. Applying standards to systematize learning analytics in serious games. *Comput. Stand. Interfaces* **2017**, *50*, 116 – 123. doi:10.1016/j.csi.2016.09.014.
19. Zyda, M. From visual simulation to virtual reality to games. *Computer* **2005**, *38*, 25–32.
20. Cano, J.; Hernández, R.; Ros, S. Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation. *IEEE Commun. Mag.* **2014**, *52*, 101–107.
21. Maskeliunas, R.; Damasevicius, R.; Lethin, C.; Paulauskas, A.; Esposito, A.; Catena, M.; Aschettino, V. Serious Game iDO: Towards Better Education in Dementia Care. *Information* **2019**, *10*, 355. doi:10.3390/info10110355.
22. Maskeliunas, R.; Kulikajevas, A.; Blazauskas, T.; Damasevicius, R.; Swacha, J. An Interactive Serious Mobile Game for Supporting the Learning of Programming in JavaScript in the Context of Eco-Friendly City Management. *Computers* **2020**, *9*, 102. doi:10.3390/computers9040102.
23. Zhang, X.; Liu, B.; Gong, X.; Song, Z. State-of-the-Art: Security Competition in Talent Education. In *Information Security and Cryptology*; Chen, X., Lin, D., Yung, M., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 461–481.
24. Jariwala, S.; Champion, M.; Rajivan, P.; Cooke, N. Influence of Team Communication and Coordination on the Performance of Teams at the iCTF Competition. *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* **2012**, *56*, 458–462. doi:10.1177/1071181312561044.
25. Childers, N.; Boe, B.; Cavallaro, L.; Cavedon, L.; Cova, M.; Egele, M.; Vigna, G. Organizing Large Scale Hacking Competitions. In *Detection of Intrusions and Malware, and Vulnerability Assessment*; Kreibich, C.; Jahnke, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 132–152.
26. Burket, J.; Chapman, P.; Becker, T.; Ganas, C.; Brumley, D. Automatic Problem Generation for Capture-the-Flag Competitions. In Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), Washington, DC, USA, 11 August 2015; USENIX Association: Washington, DC, USA, 2015.
27. Chothia, T.; Novakovic, C. An Offline Capture The Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education. In Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), Washington, DC, USA, 11 August 2015; USENIX Association: Washington, DC, USA, 2015.
28. Chang Feng, W. A Scaffolded, Metamorphic CTF for Reverse Engineering. In Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15), Washington, DC, USA, 11 August 2015 ; USENIX Association: Washington, DC, USA, 2015.
29. Chothia, T.; Novakovic, C.; Radu, A.I.; Thomas, R.J. Choose Your Pwn Adventure: Adding Competition and Storytelling to an Introductory Cybersecurity Course. In *Transactions on Edutainment XV*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 141–172.
30. Trickel, E.; Disperati, F.; Gustafson, E.; Kalantari, F.; Mabey, M.; Tiwari, N.; Safaei, Y.; Doupé, A.; Vigna, G. Shell We Play A Game? CTF-as-a-service for Security Education. In Proceedings of the 2017 USENIX Workshop on Advances in Security Education (ASE 17), Vancouver, BC, Canada, 8 June 2017; USENIX Association: Vancouver, BC, Canada, 2017.
31. Wi, S.; Choi, J.; Cha, S.K. Git-based CTF: A Simple and Effective Approach to Organizing In-Course Attack-and-Defense Security Competition. In Proceedings of the 2018 USENIX Workshop on Advances in Security Education (ASE 18), Baltimore, MD, USA, 13 August 2018; USENIX Association: Baltimore, MD, USA, 2018.

32. Russo, E.; Costa, G.; Armando, A. Scenario Design and Validation for Next Generation Cyber Ranges. In Proceedings of the 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 1–3 November 2018, pp. 1–4.
33. Eckroth, J.; Chen, K.; Gatewood, H.; Belna, B. Alpaca: Building Dynamic Cyber Ranges with Procedurally-Generated Vulnerability Lattices. In Proceedings of the 2019 ACM Southeast Conference, Kennesaw, GA, USA, 18–20 April 2019; Association for Computing Machinery: New York, NY, USA, 2019; pp. 78–85. doi:10.1145/3299815.3314438.
34. Martin, S.; Diaz, G.; Castro, M.; Rodriguez-Artacho, M. Increasing Engagement in a Network Security Management Course through Gamification. In Proceedings of the 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, UAE, 8–11 April 2019; pp. 1380–1383.
35. Trapero, A.; Tobarra, L.; Pastor, R.; Robles-Gómez, A.; Hernández, R.; Duque, A.; Cano, J. Game-based learning approach to cybersecurity. In Proceedings of the 2020 IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 27–30 April 2020; pp. 1125–1132.
36. Schreuders, Z.C.; Shaw, T.; Shan-A-Khuda, M.; Ravichandran, G.; Keighley, J.; Ordean, M. Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events. In Proceedings of the 2017 USENIX Workshop on Advances in Security Education (ASE 17), Vancouver, BC, Canada, 15 August 2017; USENIX Association: Vancouver, BC, Canada, 2017.
37. Uzal, A.; Tobarra, L.; Utrilla, A.; Robles-Gómez, A.; Pastor-Vargas, R.; Hernández, R. Tracking the Students' Learning Behavior for Cybersecurity Scenarios. In Proceedings of the Learning Analytics Summer Institute Spain 2020. online, 15–16 June 2020; Volume 2671, pp. 143–155.
38. Hamari, J.; Koivisto, J.; Sarsa, H. Does Gamification Work?—A Literature Review of Empirical Studies on Gamification. In Proceedings of the 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA, 6–9 January 2014; pp. 3025–3034. doi:10.1109/HICSS.2014.377.
39. Cano, J.; Hernández, R.; Ros, S.; Tobarra, L. A distributed laboratory architecture for game based learning in cybersecurity and critical infrastructures. In Proceedings of the 2016 13th International Conference on Remote Engineering and Virtual Instrumentation (REV), Madrid, Spain, 24–26 February 2016; pp. 183–185.
40. Drachsler, H.; Hoel, T.; Cooper, A.; Kismihók, G.; Berg, A.; Scheffel, M.; Chen, W.; Ferguson, R. Ethical and Privacy Issues in the Design of Learning Analytics Applications. In Proceedings of the Sixth International Conference on Learning Analytics & Knowledge, LAK '16, Edinburgh, UK, 25–29 April 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 492–493. doi:10.1145/2883851.2883933.
41. Sclater, N.; Bailey, P. Code of Practice for Learning Analytics. JISC. 2015. Available online: https://www.jisc.ac.uk/guides/code-of-practice-for-learning-analytics (accessed on 23 December 2020).
42. Griffiths, D.; Drachsler, H.; Kickmeier-Rust, M.; Steiner, C.; Hoel, T.; W.Greller. *Is Privacy a Show-stopper for Learning Analytics? A Review of Current Issues and Solutions*; public project report available at project site 2016. Available online: https://www.estandard.no/files/LACE-review-6_privacy-show-stopper.pdf.
43. SHEILA Project. Using Data Wisely for Education Futures. 2020. Available online: https://sheilaproject.eu/ (accessed on 23 December 2020).
44. Deterding, S.; Dixon, D.; Khaled, R.; Nacke, L. From Game Design Elements to Gamefulness: Defining "Gamification". In Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, MindTrek '11, Tampere, Finland, 29–30 September 2011; ACM: New York, NY, USA, 2011; pp. 9–15. doi:10.1145/2181037.2181040.
45. Ašeriškis, D.; Damaševičius, R. Gamification Patterns for Gamification Applications. *Procedia Comput. Sci.* **2014**, *39*, 83–90. doi:10.1016/j.procs.2014.11.013.
46. Dormans, J. The Effectiveness and Efficiency of Model Driven Game Design. In *Entertainment Computing —ICEC 2012*; Herrlich, M., Malaka, R., Masuch, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 542–548.
47. Docker. Debug Your App, not Your Environment. 2020. Available online: https://www.docker.com/ (accessed on 23 December 2020).
48. Darejeh, A.; Salim, S.S. Gamification Solutions to Enhance Software User Engagement—A Systematic Review. *Int. J. Human–Computer Interact.* **2016**, *32*, 613–642, doi:10.1080/10447318.2016.1183330.
49. Kubernetes. Kubernetes Website Available online: (accessed on 23 December 2020).
50. Amazon Elastic Compute Cloud. Available online: https://aws.amazon.com/es/ec2/ (accessed on 23 December 2020).
51. Microsoft Azure. Available online: https://azure.microsoft.com/ (accessed on 23 December 2020).
52. Foundation, T.A.S. Apache Guacamole. 2020. Available online: https://guacamole.apache.org/ (accessed on 23 December 2020).
53. Django. The Web Framework for Perfectionists with Deadlines. 2020. Available online: https://www.djangoproject.com/ (accessed on 23 December 2020).
54. Learning Locker. Available online: https://docs.learninglocker.net/welcome/ (accessed on 23 December 2020).
55. Liu, I.F.; Chen, M.C.; Sun, Y.S.; Wible, D.; Kuo, C.H. Extending the TAM model to explore the factors that affect Intention to Use an Online Learning Community. *Comput. Educ.* **2010**, *54*, 600–610. doi:10.1016/j.compedu.2009.09.009.
56. Davis, F.D. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Q.* **1989**, *13*, 319–340.

57. Berg, A.; Scheffel, M.; Drachsler, H.; Ternier, S.; Specht, M. The Dutch XAPI Experience. In Proceedings of the Sixth International Conference on Learning Analytics & Knowledge, Edinburgh, UK, 25–29 April 2016; Association for Computing Machinery: New York, NY, USA, 2016; LAK '16, p. 544–545.
58. Manso-Vázquez, M.; Caeiro-Rodríguez, M.; Llamas-Nistal, M. An xAPI Application Profile to Monitor Self-Regulated Learning Strategies. *IEEE Access* **2018**, *6*, 42467–42481.
59. Experience API Registry. 2020. Available online: https://registry.tincanapi.com/#home/verbs (accessed on 23 December 2020).
60. RusticiSoftware. TinCanPython Library. 2020. Available online: https://github.com/RusticiSoftware/TinCanPython (accessed on 23 December 2020).
61. United Nations conference on Trade and Development. Data Protection and Privacy Legislation Worldwide. 2018. Available online: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx (accessed on 23 December 2020).