Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 6, Special Issue, 2022

"Current Issues, Trends, and New Ideas in Education"

Utilizing a Restricted Access e-Learning Platform for Reform, Equity, and Self-development in Correctional Facilities

Yannis C. Stamatiou [1], Constantinos Halkiopoulos [2*], Athanasios Giannoulis [2], Hera Antonopoulou [2]

[1] *Department of Business Administration, University of Patras, Greece and Computer Technology Institute and Press (CTI) – "Diophantus", Patras, Greece.*

[2] *Entrepreneurship and Digital Innovation Laboratory (EDILAB), Department of Management Science and Technology, University of Patras, Greece.*

Abstract

Objectives: The goal of this paper is to address the issues that arose because of the exclusion of law offenders in the Greek Correctional Institutions from second chance education during the COVID-19 pandemic. During this period, the offenders were deprived of their right to equal access to second-chance education since the pandemics blocked mobility and close contact with teaching personnel. *Methods/Analysis:* In this paper, we propose a framework based on the Technology Acceptance Model (TAM) that will be deployed to evaluate the acceptance of the CILMS by the learners in Correctional Institutions. We describe a methodology and a set of hypotheses that can reveal the intention of learners to use the system based on several factors, such as trust, perception of privacy, perception of usefulness, and perception of self-efficacy. *Findings*: We suggest that eLearning and limited Internet access should be added to the list of fundamental human rights for CI detainees as well, in order to counteract their separation from physical society. Inmates are still individuals. In fact, they should be placed in solitary confinement as prescribed by the law. *Novelty/Improvement:* This viewpoint has been demonstrated with the development and evaluation of acceptance by inmates through the TAM technology acceptance methodology, as well as the proposal of a generic privacy-preserving Web information and services access model for CIs that can, at the same time, provide sufficient information access freedom while respecting the restrictions that should be imposed on such an access for CI inmates.

Keywords:

Technology Acceptance Model;
ICT Skills;
e-learning;
LMS;
Correctional Facilities;
Limited Network Access.

Article History:

Received:	30	August	2022
Revised:	17	October	2022
Accepted:	07	November	2022
Published:	28	December	2022

1- Introduction

It is well known that the adoption of eLearning, or Learning Management Systems (LMS), systems can achieve an improved learning level and experience either in conjunction with or independently of the traditional teaching and learning process [1, 2]. Thus, numerous educational institutions, from schools to universities [3], have adopted this viewpoint and have developed several online courses [4] targeting normal courses, postgraduate programs, continuous education [5], and lifelong learning, as well as seminars offering some type of skills certification [6, 7]. The importance of eLearning in improving digital literacy is emphasized by UNESCO, which reports that Massive Open Online Courses (MOOCs) are among the top educational priorities of many countries worldwide [8, 9]. We characterize as MOOCs the open eLearning platforms that offer online courses with minimal requirements of previous ICT knowledge or experience except simple use of the Internet and online applications [10-12]. MOOCs support online classes and offer video (also offline) lectures, self-assessment tests, online assignments, as well as electronic course material. Some of them also provide online forums and chat rooms that lead to increased engagement and socializing among learners and teaching personnel [13].

* **CONTACT**: halkion@upatras.gr

DOI: http://dx.doi.org/10.28991/ESJ-2022-SIED-017

However, although the usefulness and widespread adoption of LMS are unquestionable, especially in the COVID-19 pandemic era, there are still some members of our society excluded from e-education and web information access, the people confined in Correctional Institutions [14]. This exclusion leads to a deprivation of opportunities for self-improvement and self-development, as well as equal access to the fundamental right to education and global developments in general. Access to the right to education is a complex issue that necessitates the supply of both the necessary human resources and technical infrastructure. Nonetheless, its unrestricted and complete exercise is contingent upon the general conditions of the correctional facility and the extent to which other rights are respected and protected. For instance, overcrowding in a prison complex inevitably leads to the exclusion of prisoners from the education process when the available study places are filled, whereas the insecurity that an inmate may feel due to ill-treatment and violence within the correctional facility can be a deterrent to his participation in programs of meaningful use of his time, such as educational ones.

In order to address this inequality situation, in this paper we address the sensitive application area of digital learning and digital information access in the penitentiary system and the possibility of providing availability, under restrictions, of digital learning and information retrieval services to inmates. In addition, the correctional system offers few educational options and chances for adult and adolescent detainees, making education and lifelong learning an urgent concern. Moreover, innovative learning and teaching methods in prisons, using techniques such as gamification, promote cognitive and emotional parameters of the learners' personalities, such as the improvement of their perception, attention, memory, and executive functions in general, as well as their emotional and neurocognitive development. Inmates have a larger requirement than any other educational group to engage in an educational policy targeted at growing and refining their cognitive and psycho-emotional functionality for ultimate social reintegration, as well as strengthening the motivation for behavioral change in general.

One of our contributions is the proposal of a Technology Acceptance Model (TAM) for investigating the acceptance tendency of LMS in Correctional Institutions by inmates as a vehicle for participation in skill enhancement and knowledge acquisition within the confinement conditions of inmates. The model addresses several issues related to the perceived usefulness of an LMS as well as the intention to use such a system for eLearning purposes. We propose a set of hypotheses as well as a model that relates the hypotheses to the viewpoint of inmates about LMS and eLearning. The model includes aspects of trust towards the system as well as potential risks (e.g., in privacy) in its use.

Our other contribution is a proposal for a framework that allows partially anonymous, but controlled, access to Web information resources from within Cis [15, 16]. This framework is based on a special type of digital credentials, called Privacy Attribute Based Credentials or Privacy-ABCs [17, 18].

This type of credentials allows users to provide to Web services only the information required for accessing them and nothing beyond it. This functionality enables partial anonymity since the real identity of users is not revealed but they remain pseudonymous while accessing Web resources. Naturally, since CIs have strict rules, anonymity can be removed, by a special inspector entity, if the inmate using the credentials misuses them towards accessing Web resources, he/she is not allowed to access. This partial anonymity will help inmates have a feeling of independence while they will know that any wrongdoing can be uncovered by the inspector. Accessing Web information will provide inmates with equal rights to information acquisition towards self-development and learning purposes. The generic platform architecture we propose is flexible and allows for a variety of partial anonymity, Web access, depending on the level.

2- Literature Review

Education has always been in conflict between two roles: ensuring continuity and stimulating innovation and change. Within these, technology presents educational institutions with a new set of difficulties and demands. The rate of technological advancement has been remarkable. Today, educators in many nations work with "digital natives", who have grown up with modern technology as a normal part of life. Technology enables us to (co-)create, acquire, store, and utilize knowledge and information; it enables us to connect with people and resources from across the globe, to participate in the development of knowledge, and to share and benefit from knowledge products. The subject of how educators use technology in teaching and learning activities persists. According to research, integrating technology into education is a complicated process, and the scope of technological uses in schools is still quite diverse. Clearly, the utilization of developing educational technologies in (instructor) education has expanded over the past several years, yet technological acceptability and utilization remain troublesome for educational institutions. In the literature, the subject of what factors influence technology integration in education is constantly raised. Measuring user adoption of technology is a method for identifying whether or not an educator intends to use new technologies in their educational practice.

In recent decades, several models have been developed to describe the mechanism behind and factors influencing technology adoption such as the Unified Theory of Acceptance and Use of Technology (UTAUT) and the Technology Acceptance Model. Also, so far, we find a varied range of earlier research on learners' acceptance of technology (e-

learning). Those studies fit popular models and theories including the TAM [19], Technology Acceptance Model 2 (TAM2) [20] and Technology Acceptance Model 3 (TAM3) [21]. The Theory of Reasoned Action (TRA) [22], Theory of Planned Behavior (TPB) [23], Unified Theory of Technology Acceptance and Use (UTAUT) [24] and demonstrate the user's stance on technology use in the face of diverse agents. These agents, such as trainee characteristics or system characteristics, influence the acceptance of technology [25, 26]. In this perspective, several models have been developed further by using outside factors [27, 28]. These models have been shown to influence users' acceptance of e-learning stated as "computer self-efficacy", "computer anxiety", "prior experience", "enjoyment", "learning motivation", "perceived learning ability", "hedonic motivation", "personal innovativeness" and "learner engagement" [29, 30].

As shown by the related literature, the original TAM is suitable for investigating LMS acceptance in Cis. Our basis relies on its fundamental elements which are the following: Perceived Usefulness, Perceived Ease of Use, Intention to Use and Actual Use. We have also, included as a new element the Perceived Self Efficacy (PSE), which is the level of confidence in the capacity to accomplish an educational task. Numerous studies have shown that increased self-efficacy improves productivity with the help of an (educational, in our case) information system [31, 32]. Therefore, the content of the additional factor of Perceived Learnability (PL) would be how one perceives, learns, and remembers the operation of an application. As stated by Hu and Hui [33], the person who has higher perceived learnability assumes that utilizing an information system helps to improve his/her efficiency [34-36]. Lastly, Fun and Reward (FUN) measures the satisfaction of the use of information systems or educational games [37-39] and we have included it in the proposed model.

With respect to the Privacy-ABCs, there are only two applications areas in which they have been applied in the educational system: a secondary school in Sweden and a university in Patras (see https://abc4trust.eu/index.php/pub for the relevant deliverables). No application exists, to the best of our knowledge, to education within the penitentiary system, such as the one we propose.

3- The target LMS platform for CIs

Given the relevance and importance of eLearning education for Greek law offenders, in combination with the stringent Internet access rules in Cis, it was a challenge to propose and implement an eLearning platform that will reconciliate these two opposing goals: preservation of CI rules and eLearning and individuals who are socially isolated, this research attempts to describe the method using a flowchart presentation (Figure 1). As a result of what has been reported thus far and in light of the present literature, the research questions to be addressed can be described as follows:

- [RQ1] Prisoners of second chance schools in Greece were excluded from education?
- [RQ2] Access to education and knowledge is a fundamental right of all people and prisoners?
- [RQ3] Is it possible for Greek prisoners to obtain their right to education via innovative secure tools?
- [RQ4] Is it possible to avoid third-party monitoring and transfer to particular structures/distance learning centres?

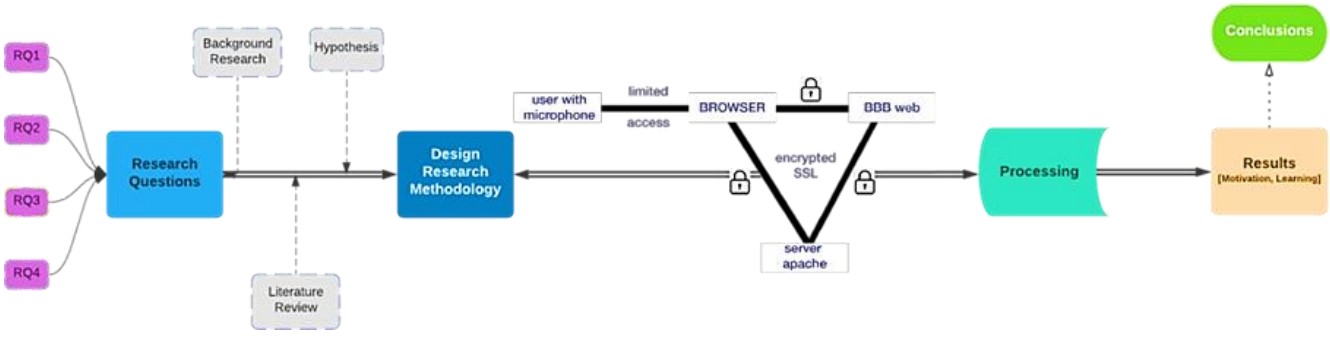

Figure 1. The overall design and implementation approach

All applications that appear in the “triangle” (Figure 2) reside on the same server which is secured by the firewall configuration discussed above. Due to the simplicity of our application, no virtual machines were created since only two applications run at each time (served by the Apache Server connection functionalities), a local (to the server) Web Browser and the BBB (BigBlueButton – see *https://bigbluebutton.org/*) virtual classroom platform. Also, no cloud architecture and services were created (locally) due to the absence of such a requirement for our application. Finally, no outside cloud services were used for the same reason and, furthermore, due to the string security requirements (mainly no or restricted communication with the Internet and the Web beyond the secured prison’s local network).

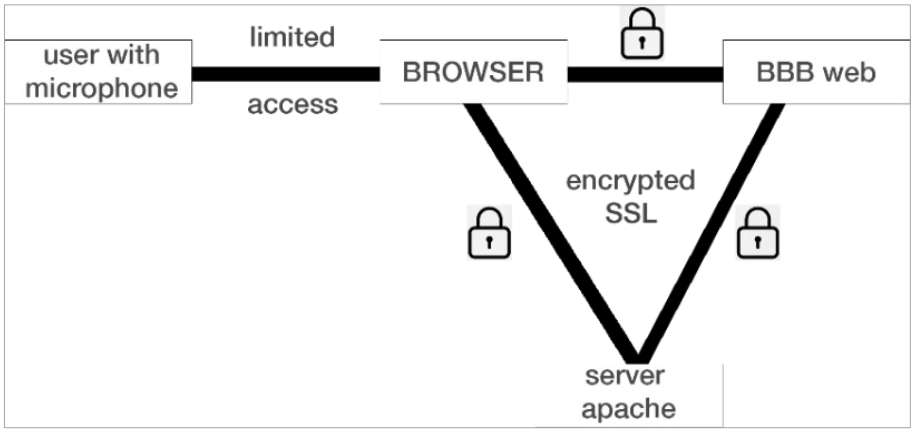

Figure 2. Interconnectivity between subsystems

With respect to security, the installed Apache Server's enabled mod_ssl module provides an interface to the OpenSSL library for strong encryption based on the Secure Sockets Layer and Transport Layer Security (i.e., SSL and, its successor, TLS) protocols.

The learners are connected through Ethernet ports in the establishment's classroom and the installed, in the classroom, computers for increased security. No WiFi connections are allowed to the local WiFi router (the router is configured to block any request for connection beyond specific devices, if necessary, with specific MAC addresses).

The Ethernet ports support only the already connected computers (through whitelisting) and no other computer can be connected to them.

4- The target LMS platform for CIs

In this section, we propose a model based on technology acceptance factors according to TAM along with the involved hypotheses to be tested. The model is shown in Figure 3. Our goal is to assess the "Intention to participate in the CILMS", using the platform we described earlier. Each rectangle represents a TAM factor linked by the correlation hypotheses described below.

The hypotheses should be considered in conjunction with the correlation graph in Figure 3.

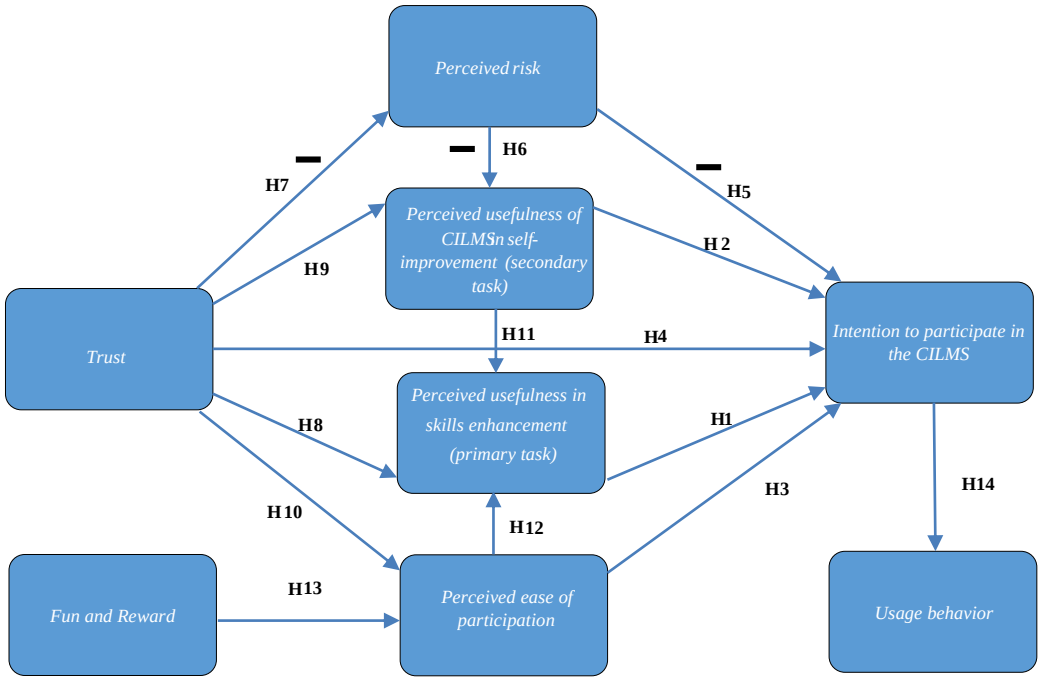

Figure 3. The proposed TAM model (negative correlation is denoted by "-", otherwise it is positive)

Table 1. Hypotheses

H1	The perceived usefulness of CILMS in skill enhancement and preparation for life after CI period ends is positively related to the intention to participate.
H2	The perceived usefulness of CILMS in self-improvement with respect to knowledge and interaction with other people (for, both, CILMS instructors and students).
H3	The perceived ease of participation in the CILMS is positively related to the intention to participate in the system.
H4	Trust in the CILMS is positively related to the intention to participate in it.
H5	The perceived risk in participation in the CILMS is negatively related to the intention to participate in the CILMS system.
H6	The perceived risk is negatively related to the perceived usefulness of the CILMS in self-improvement of the participants.
H7	Trust in the CILMS is negatively related to the perceived risk in using the CILMS.
H8	Trust in the CILMS is positively related to the perceived usefulness of the CILMS.
H9	Trust in the CILMS is positively related is positively related to the perceived usefulness of the CILMS system.
H10	Trust in the CILMS system is positively related to the perceived ease of participation in it.
H11	The perceived usefulness of CILMS in self-improvement is positively related to perceived usefulness of the CILMS system.
H12	The perceived ease of participation is positively related to perceived usefulness of the CILMS.
H13	Fun and Reward, in participating in the CILMS, is positively related to the perceived ease of participation in this system.
H14	The intention to use the CILMS is positively related to the Usage behaviour.

The proposed model is based on the model deployed in Stamatiou et al. [40] for assessing the effectiveness of privacy-preserving authentication technologies and, Privacy-ABCs in particular, in course evaluation systems in higher education.

The standard TAM factors, included in Figure 3, are defined as follows (see, also, [40]):

- *Perceived Ease of Use* is the degree to which a person believes that using a particular system would be free of effort or with small effort.
- *Perceived Usefulness* is the degree to which a user believes that using the target system would enhance his or her skills and performance.
- *Intention to Use*, also called Behavioural Intention in the related literature, refers to the degree to which a user has formulated "conscious plans" to use or refrain from using the target technology.
- *Usage Behaviour* is the actually observed and measured usage, for instance frequency and duration of the usage of the target system.

TAM-based studies may, also, include *external* variables that possibly influence Perceived Usefulness and Perceived Ease of Use. Such external variables may depend on characteristics of the target system (e.g., relation of the system towards the intended user's tasks and perceived quality of the system's effectiveness), the differences among users (e.g., age, gender, previous ICT experience, and computer competency) or even characteristics of the user's environment (e.g., appropriate technical support, influence from other users). However, the actual usage of the system is, frequently, not considered in the studies reported in literature. This is due to the fact that actual usage data is, usually, not available or can be obtained over a prohibitively long time period. Thus, TAM studies usually focus on the Intention to Use only, which is considered to be, also, a reliable predictor of the actual usage of the system, although less accurate quantitatively. However, we have included this factor in order to be able to assess not only the intention to use, but whether this intention is transformed into actual use of the CILMS. Actual system use can be obtained with suitable applications that record the time periods over which users are connected to the CILMS and use the eLearning material.

We, finally, remark that our study includes, in contrast to all other TAM studies except the one in Stamatiou et al. [40] (to the best of our knowledge) several trust-related (i.e., trust towards the CILMS) factors (see Table 1). We believe that trust towards ICT system may lead to increased intention to participate as well as usage behaviour (i.e., frequency of use) as it was demonstrated in Stamatiou et al. [40]. Trust, in the case of our target CILMS, is based on privacy-preserving technologies which authenticate users (over some selected identity fields) retaining their anonymity. Our viewpoint is that inmates confined in CIs will feel more at ease knowing that they preserve some privacy when using information technologies in the CI premises. Actually, as we will explain in the next section, privacy-preserving technologies provides more freedom to inmates retaining, however, the constraints in site access imposed by CI regulations. We, thus, have included the trust and privacy factors in our TAM model in order to capture this fact and investigate the extent to which privacy-preserving technologies affect intention to use of a target system (in our case the CILMS).

5- Privacy-Preserving Authentication for Controlled Web Access in CIs

The deprivation of freedom, i.e., imprisonment, has always been a resonant but still civilized method of punishment for delinquent or law-offending behavior. However, notwithstanding the significance of punishment, achieving the convict's discipline and rehabilitation in society is (or should be) an additional goal of imprisonment following our civilization's humanitarian values. This is especially so for juvenile or misdemeanor law offenders who are expected to lead an everyday personal and professional life after discharge from a CI.

Although integration with the physical society may not be possible due to the confinement in the CI, integration with the digital society is achievable without discarding or downplaying the role of the penitentiary system, which relies on imprisonment as a means of punishment. The eLearning platform we described above is one step forward in this direction. However, the goal should be to keep offenders abreast with world developments and infuse them with a feeling of "limited freedom", suppressing the emergence of the "imprisonment stigma", that will ease their anxiety and stress (especially for young people).

The EU has taken some steps towards this direction. For instance, much like in several other EU countries, prisoners at the prison in Gera, in the eastern German state of Thuringia, are allowed to browse selected online content *. As Thuringia's ministry of justice states, pages that are not blocked, such as employment agencies and probation assistance services, can help with inmate's rehabilitation. Moreover, some young prisoners are, even, allowed to produce a podcast about prison life which may act as a deterrent to crime for young people. Notably, a communications company in Hamburg that specializes in the justice domain has, even, created a new technology to support Internet access in prisons. Its mission statement is that "the human right to communicate and the right to information are fundamental humanitarian necessities and must not be regarded as a luxury by law enforcers". To serve this purpose, the firm has developed the "Multio" system, which is a computer system with restricted access to the Internet. It is capable of receiving radio and television broadcasts, as well as making telephone calls. However, the online behavior of inmates is closely monitored by CI personnel. However, the use of new technologies and services by inmates should not create suspicions of surveillance and privacy violation otherwise the goal to provide access to the opportunities of new technologies to inmates and respect their privacy, at an elementary level at least, will fail. Access to the Web and visit to services and websites should not evoke a feeling of a Panopticon, i.e., a "digital prison" within the physical prison itself. The Panopticon (meaning "all-seeing"), originally conceived by the eighteenth-century utilitarian philosopher Jeremy Bentham as an architectural design for circular prisons, has nowadays, in the digital era, a connotation for "constant online observation" as a means of control mechanism and discipline, marking the transition to a disciplinary power where even the slightest movement is supervised, and all events are recorded. Unseen by the prisoners, the structure of Panopticon would allow warders to observe the tiered ranks of cells and survey them from the center of the circle building up a subtle still powerful internalized oppression among the isolated inmates. This consciousness of constant surveillance allowed later on Foucault and other scholars to employ Panopticon as a metaphor to explore the relationship between systems of social control in a disciplinary situation, point out the individuals' deprivation of freedom and subjection to discipline and focus on the power/knowledge concept.

In what follows, we propose a Web access model for CIs (beyond the eLearning LMS described above) that can ease the feelings of exclusion, inequality, and neglect of offenders concerning the digital (at least) society while, at the same time, respects the penitentiary system's goal of confinement and deprivation of some aspects of freedom. This Web access model relies on a new type of digital certificate called Attribute Based Credentials, or ABCs, for short. The critical characteristic of ABCs is that they allow a partial identification of a user towards a service by enabling the user to disclose only those aspects of his/her identity necessary to access the service. In contrast, commonly used user authentication methods (e.g., based on Public Key Infrastructures, or PKIs) that are employed today for controlling access to Web services most often fall short of balancing users' privacy as well as services' access restrictions, such as the ones that Cis should impose on Web access by inmates.

This partial authentication state occurs in Web services in that only a (usually small) subtotal of a user's complete identity profile would be required to permit access. These types of services vary from access to online libraries, where a complete identity profile need not be provided to access e-books, but simply a verification that one is a subscriber to the library, to online movie watching, where it may be necessary to show that one is of the proper age (e.g., over 18) to be able to view certain movies. In such apps, there is an apparent necessity for partial rather than full disclosure of the user's identity. Privacy Attribute-Based Credentials, or Privacy-ABCs in brief, is a privacy-preserving, partial authentication technology for users. Privacy ABCs are being issued like regular electronic credentials (e.g., PKI-based) employing a secret signing key that belongs to the credential holder. The issuer can be, for example, the administration of the CA or the Department of Justice (DOJ). Nevertheless, the user can convert the authentication credentials into a new format, named presentation token, which exposes the information necessary to access a service. This new credential can be authenticated with the issuing party's public key.

* *https://www.dw.com/en/internet-access-for-germanys-prisoners/a-16967584*

The use of Privacy-ABCs can create a vast range of new use cases for CI information systems based on three credential properties. First, Privacy-ABCs allow for secure and trustworthy verification of individual attributes out of a larger credential without giving away the whole set of personal data. The attribute types are not limited to the small set that can be vouched for by a public issuer. Rather any type of attribute value can be described. Therefore, a broad deployment of Privacy-ABCs allows for a radical rethinking about the necessity of processing of personal data in particular for authentication and verification of attributes.

A second privacy challenge that is being faced with the privacy-enhancing properties of privacy-enhancing ABKs is the necessity to collect personal data only in the more or less likely case that the verifier will need the information at a later stage. This might happen in the case of a client not paying or in other cases of breach of contract. The verification mechanism provided by Privacy-ABCs allows for identity disclosure under present circumstances given that encrypted attribute values have been provided and stored as part of the presentation token. The party that only needs the personal data under special conditions then does not have access to the encrypted personal data unless the conditions for an inspection are met. With Privacy-ABCs it is nevertheless possible for the trusting party to verify that the encrypted content really consists of the requested attributes. Thus, inspection allows to abstain from collecting personal data in business cases, which only require contacting the User under certain special conditions. Finally, unlikability is a third key benefit of Privacy-ABCs. Transactions done with Privacy-ABCs cannot be linked to the User or to each other unless attribute values allow for linking or it has been explicitly specified otherwise. This prevents tracking and profiling of the Users by Verifiers. Unlikability is a prerequisite for data minimization and purpose binding. The principle of purpose binding stems from the standard requiring that personal data should be "collected for stated, explicit and lawful purposes and should not be processed further in a manner inconsistent with these purposes", Art. 6 sec. 1 (b) of Directive 95/46/EC. Privacy-ABCs support this principle in several ways. Processing personal data separately for each purpose or transaction allows a clearer connection with the respective purpose and eases the later deletion of personal data related to a transaction, e.g., for deletion after the regular storage period. With presentation tokens being unlikable by default, this idea is supported and can be enforced. Further, the presentation policy of the Verifier stipulates the categories of personal data that are necessary for the particular transaction. This results in the effect that storing the presentation tokens means that only the personal data necessary for the respective transaction is retained.

With these properties, Privacy-ABCs allow for a radical rethinking of the concept and understanding of necessary processing of personal data and the need-to-know principle. Privacy-ABCs may even help to enforce the rethinking process if the technology must be taken into consideration for the evaluation of what is necessary processing. This should be the case once the technology of Privacy-ABCs has been tested and is broadly available – maybe even as part of a unified European eID. However, as to which data controller are forced to deploy Privacy-ABCs and other privacy enhancing technologies is an open question. Art. 17 sec. 1 of Directive 95/46/EC refers insofar to the state of the art and the costs of implementation. Therefore, such technologies must be sufficiently mature and considered state of the. Clarifying this question and enforcing the deployment of privacy-preserving technologies by data controllers is a task for future legislative actions. In Figure 4 we see the entities involved in a Privacy-ABCs system:

- The *User* is at the center of the picture, collecting credentials from various Issuers (i.e., eServices from the eGov domain) and controlling which information from which credentials she presents to which verifiers (other eServices that she is allowed to access).
- An *Issuer* issues digital credentials to users, thus certifying the accuracy of the information included in a credential in relation to the user to whom the credential was issued. Before issuing credentials, the Issuer should authenticate the User, preferably in person, in the CI. Thus, in our context, the issuer should be the CI itself since the authorities can verify an inmate's personal information. In the identity management terminology, the Issuer is, sometimes, termed *identity provider* or *attribute authority*.
- A Verifier secures access to a resource or service it offers by restricting the credentials that people must hold and information about these credentials that people must provide in to gain access to the service. The verifier's restrictions are outlined in the presentation policy. The user produces from their credentials a presentation token containing the required information and support cryptographic evidence. In the identity management literature, the Verifier is at times referenced as the relying party, server, or service provider.
- A Revocation Authority oversees withdrawing credentials that have been issued so that those credentials can no longer be used to create a presentation token in services. The use of a specific revocation authority may be enforced by the issuer, in which case the revoked credentials are not usable with any auditor for any purpose, or by the auditor, in which case the effect of the revocation is local to the auditor and does not affect presentations with other auditors. Both the user and the verifier need to retrieve the latest revocation information from the revocation authority to produce presentation certificates, appropriately.
- An Inspector is a trusted principle that can de-identify presentation tokens under certain conditions. In our case, this should be the Ministry of Justice (MoJ). To exercise this capability, the verifier should specify in the presentation policy which inspector should be able to retrieve which attribute(s) under which circumstances. Therefore, the operator is aware, always, of the de-identification options when creating the token and is actively involved in order to facilitate this. Thus, the user can make an informed decision based on his or her trust in the Inspector. Also, users avoid wrongdoing, while online, since there is a possibility that their actions will be uncovered by the Inspector.

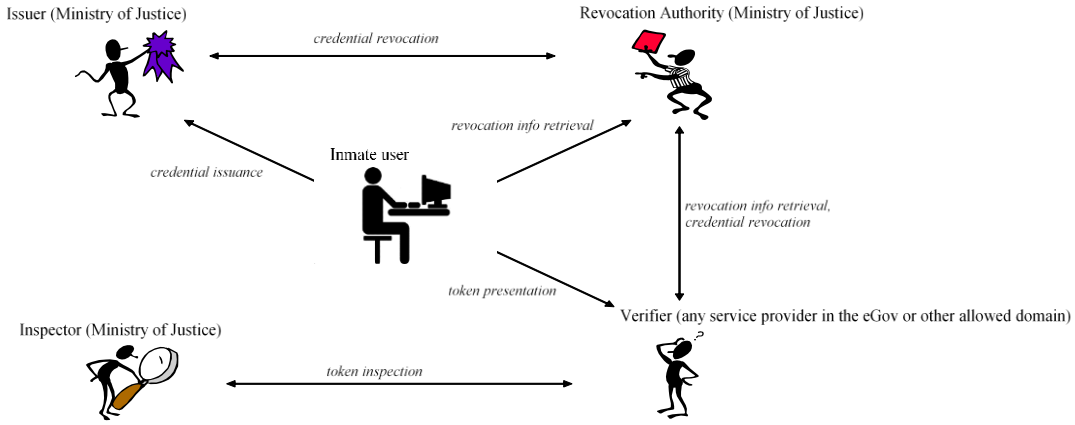

Figure 4. The Privacy-ABCs entities

In an actual deployment, some of the above roles may be fulfilled by the same entity, e.g., Ministry of Justice, or split among many independent authorities, for enhanced trust. For instance, an Issuer may simultaneously play the role of the Revocation Authority and/or the Inspector, or an Issuer could later be the Verifier of tokens derived from credentials it has issued. Figure 5 shows all these entities in the proposed architecture as well as their interactions.

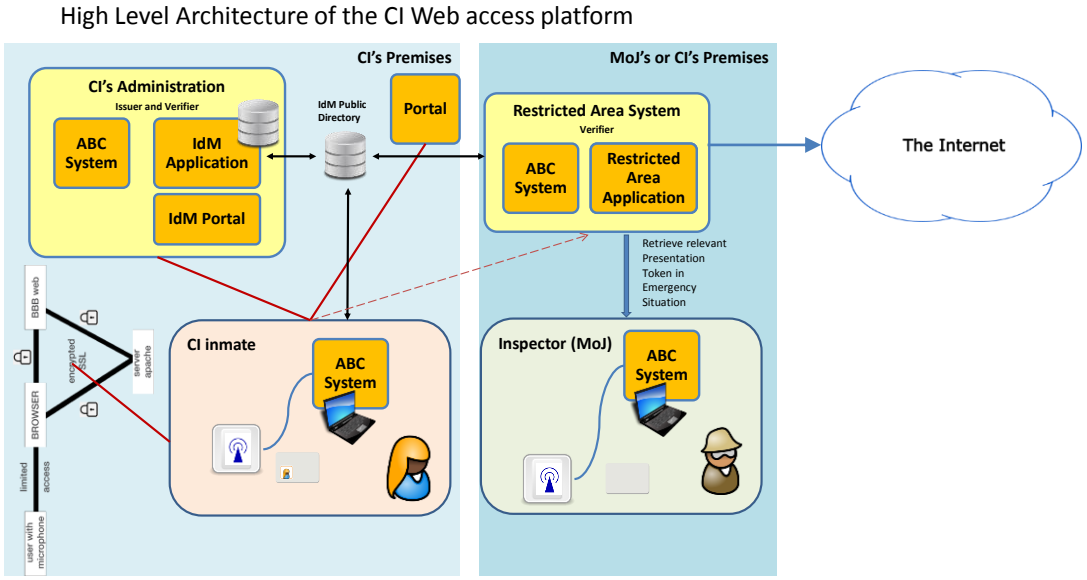

Figure 5. The proposed Privacy-ABCs architecture

We, now, describe the main usage scenario:

- The CI, acting as an Issuer (see Figure 5, left-hand side), issues Privacy-ABCs credentials on a smart card for each inmate, containing his/her personal information according to the credentials format in Figure 6.

Inmate's personal attributes
Name:
Surname:
Date of birth:
Picture:
Inmate's ID (identification number):
PIN stored in secure memory of hardware token
CI's Name:
CI' sector Name:
Date of imprisonment:
Expected date of discharge:
Committed law violation:
Remarks:
Special restrictions or permissions on Web access:

Figure 6. The proposed Privacy-ABCs credentials set

- The Restricted Area System redirects the inmate to the Web information source the inmate requested, if approved by the regulations. Such Web information sources may include, for instance, educational material, electronic news web pages, job related information etc.

The inmate accesses the Restricted Area System situated in the Ministry of Justice and authenticates himself/herself *partially anonymously* by providing only a subset of the information in his/her credential in Figure 6. For instance, he/she proves that he is an inmate in a CI and no special restrictions exist for Web access. He/she does not need to provide his/her name or other identifying information.

At this point, it is interesting to compare our present study framework with the one deployed by Stamatiou et al. [40] to evaluate how privacy-preserving authentication technologies enhance users' trust in educational services. The study by Stamatiou et al. [40] implemented Privacy-ABCs in course evaluation systems in higher education (e.g., Universities) so that users could be partially identified as students at the university who have attended sufficiently many times the courses under evaluation. However, no PID information was disclosed during this partial authentication process. Our present study, although it also targets educational services, differs significantly from the study of Stamatiou et al. [40]. The main difference is the contexts of the studies. To the best of our knowledge, our study is the first to investigate the effect of using Privacy-ABCs for authentication, which implies a form of freedom in a context where users are deprived of their (at least) *physical* freedom, i.e., a CI. Thus, we expect that the results of our study, when it is feasible to conduct it, will demonstrate whether (and how) privacy-preserving technologies can contribute to easing inmate's feelings of privacy deprivation and help them become acquainted with and use new technologies towards self-improvement. Furthermore, our study, in contrast with the study in Stamatiou et al. [40], will focus on whether privacy-preserving technologies can contribute to the enhancement of users' skills and knowledge in contrast with the study in Stamatiou et al. [40] which focused on using course evaluation systems, which are not related the educational and learning processes, and not eLearning ones.

6- Conclusions

In a rapidly evolving world and with the emergence of the Digital Society and Digital Democracy, digital technologies are constantly growing, which has a significant impact on the digital economy, productivity, innovation, and social life [41], as well as equality to information and education access. Thus, digital technologies have modified the value and role of education, training, and access to Web information towards self-development.

Our civilization's values and culture consider equality of opportunities and non-discrimination as fundamental pillars of society. Thus, our viewpoint, expressed in this paper, is that Correctional Institutions can serve a more important, for these pillars, role apart from the punishment of law violation by offering inmate's equal rights to education as well as Web knowledge and information, respecting the CI's main role and regulations.

On the one hand, e-learning-based education demands, besides other requirements, a wide variation, and flexible learning modes and processes offered by ICT, as they can be adjusted to the personal and cognitive needs of each individual (Both the European Commission's Action Plan (January 2018) and Greece's National Strategy aim, moreover, at the digital preparedness of educational institutions, the improvement of digital skills and the development of training in data analysis, emphasis on creating eLearning courses on LMS platforms [42]. The proposed eLearning platform and TAM evaluation model fit precisely within this framework and serve its goals.

On the other hand, eLearning is not the only digital good that enhances people's horizons and opportunities, which is more critical for CI inmates who are physically isolated from the world. In addition, the wealth of Web information and knowledge can offer new routes to inmates for rehabilitation and self-development after the CI term is over.

Our viewpoint is that eLearning and controlled Web access should also be included among the fundamental human rights for CI inmates to counterbalance the isolation from physical society. Inmates are still human beings. Indeed, they should receive the confinement punishment dictated by law. However, our civilization's democratic values do not have a place for revenge, only for lawful punishment. The goal should be rehabilitating inmates into society, but this cannot be accomplished if they are not provided with equal self-improvement opportunities while in the CI. Thus, our society's goal should be to help inmates acquire knowledge and digital skills in order to enhance their competencies and upgrade their qualifications when they return to physical society.

This viewpoint has been demonstrated with the development and evaluation of acceptance by inmates through the TAM technology acceptance methodology, as well as the proposal of a generic privacy-preserving, Web information and services access model for CIs which can, at the same time, provide sufficient information access freedom while respecting the restrictions which should be imposed on such access for CI inmates.

On the other hand, we recognize that our study has certain limitations. Two significant difficulties pose obstacles to the proper implementation of our TAM framework. The first difficulty is that during the (still ongoing) COVID-19 epidemic, we were not even considered for a permit to enter a CI and conduct our study based on the proposed TAM

research framework. The second difficulty is inherent in the way Cis operates in most countries. Access to conducting various studies is restricted and is approved only after several procedures, which take a significant amount of time and effort to conclude. Often, inmates are suspicious of the outsiders' aims and goals and refrain from participating in such studies. Even the CI's personnel may feel awkward or reluctant to assist. Our findings during the development of the TAM framework have shown that the stringent rules of Cis, at least in our country, do not provide a relaxed context to conduct a TAM-based eLearning platform acceptance survey with questionnaires. In addition, the planned TAM-oriented questionnaire should ideally be completed by those who have completed at least one of the online courses offered in a CI. Unfortunately, CI confinement and rules may hinder a massive course completion by CI inmates.

As future work, we believe that privacy-preserving authentication techniques and Privacy-ABCs, in particular, can be deployed in other information systems already used or planned to be introduced in CIs. For instance, Privacy-ABCs can support the development of online psychological support or online discussion with experts system for inmates. They could authenticate themselves, partly to this system revealing, for instance, their inmate status, sex, and age (or range in which age belongs) and receive anonymous support for problems they may face in the CI. Finally, Inmates can use Privacy-ABCs for anonymous questionnaire completion by inmates, with respect to the acceptance of the eLearning and skill development courses they attend and for conducting anonymous (but partially authenticated) surveys concerning daily life and conditions in the CI. The generic credential format shown in Figure 6 is entirely reconfigurable. It can be enhanced and augmented with new fields of any type, which can be verified anonymously by the Privacy-ABCs engine.

However, due to the subtle issues that beset the operation and rules of traditional CIs, our study has revealed that the success of the introduction of new technologies and digital services, such as eLearning, in CIs requires collective action from several sources. First, politicians should reform the CI operation legal framework in order to introduce more information technologies and more freedom to inmates in using them, of course with appropriate restrictions. As we saw, a step in this direction was taken, among other countries, by the German state of Thuringia, where inmates are allowed to browse selected online content from CIs. Then, technology experts should configure properly devices and applications installed in CIs to provide suitable isolation between the CIs internal network and the outside Internet world. Also, privacy-preserving technologies can help enhance the feeling of freedom and self-control in inmates and provide a relaxed environment in which inmates can improve and enhance their knowledge and skills. Finally, there is a necessity for the development of several technology evaluation frameworks, such as the TAM framework we described in this paper, which, however, will embrace not only technological aspects of new technologies in CIs but, also, legal and psychological factors that appear to affect inmates' intention to use the technologies.

In conclusion, we feel that Privacy-ABCs can relieve the effects of the deprivation of freedom in CIs and help inmates develop their skills and interests. At the same time, CI has less anxiety and more self-confidence since they empower them to handle their privacy and freedom to reveal, about themselves, only the necessary personal information necessary to use a service such as the eLearning platform we described in this paper.

7- Declarations

7-1- Author Contributions

Y.C., C.H., A.G. and H.A., contributed to the design and implementation of the research, to the analysis of the results and to the writing of the manuscript. All authors have read and agreed to the published version of the manuscript.

7-2- Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7-3- Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7-4- Institutional Review Board Statement

Not applicable.

7-5- Informed Consent Statement

Participants gave their written consent to use their anonymous data for statistical purposes. All of them were over 18 years old and voluntarily collaborated without receiving any financial compensation.

7-6- Conflicts of Interest

The authors declare that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

8- References

[1] Fokides, E. (2017). Pre-service teachers' intention to use MUVES as practitioners - A structural equation modeling approach. Journal of Information Technology Education: Research, 16(1), 47–68. doi:10.28945/3645.

[2] Serdyukov, P. (2017). Innovation in education: what works, what doesn't, and what to do about it? Journal of Research in Innovative Teaching & Learning, 10(1), 4–33. doi:10.1108/jrit-10-2016-0007.

[3] Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2020). Leadership types and digital leadership in higher education: Behavioural data analysis from University of Patras in Greece. International Journal of Learning, Teaching and Educational Research, 19(4), 110–129. doi:10.26803/ijlter.19.4.8.

[4] Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2021). Transformational leadership and digital skills in higher education institutes: During the covid-19 pandemic. Emerging Science Journal, 5(1), 1–15. doi:10.28991/esj-2021-01252.

[5] Rajabalee, B. Y., Santally, M. I., & Rennie, F. (2020). A study of the relationship between students' engagement and their academic performances in an eLearning environment. E-Learning and Digital Media, 17(1), 1–20. doi:10.1177/2042753019882567.

[6] Antonopoulou, H., Halkiopoulos, C., Barlou, O., & Beligiannis, G. N. (2021). Associations between traditional and digital leadership in academic environment: During the COVID-19 pandemic. Emerging Science Journal, 5(4), 405–428. doi:10.28991/esj-2021-01286.

[7] Antonopoulou, H., Mamalougou, V., & Theodorakopoulos, L. (2022). The Role of Economic Policy Uncertainty in Predicting Stock Return Volatility in the Banking Industry: A Big Data Analysis. Emerging Science Journal, 6(3), 569–577. doi:10.28991/ESJ-2022-06-03-011.

[8] Nikolaidis, S., Nath, S., Procaccia, A. D., & Srinivasa, S. (2017). Game-Theoretic Modeling of Human Adaptation in Human-Robot Collaboration. Proceedings of the 2017 ACM/IEEE International Conference on Human-Robot Interaction. doi:10.1145/2909824.3020253.

[9] UNESCO (2017). Working Group on Education: digital skills for life and work. Broadband Commission for Sustainable Development, UNESCO, Paris, France.

[10] Al-Shabandar, R., Hussain, A. J., Liatsis, P., & Keight, R. (2018). Analyzing Learners Behavior in MOOCs: An Examination of Performance and Motivation Using a Data-Driven Approach. IEEE Access, 6, 73669–73685. doi:10.1109/ACCESS.2018.2876755.

[11] Al-Rahmi, W., Aldraiweesh, A., Yahaya, N., Bin Kamin, Y., & Zeki, A. M. (2019). Massive Open Online Courses (MOOCs): Data on higher education. Data in Brief, 22, 118–125. doi:10.1016/j.dib.2018.11.139.

[12] Castaño-Muñoz, J., Kalz, M., Kreijns, K., & Punie, Y. (2018). Who is taking MOOCs for teachers' professional development on the use of ICT? A cross-sectional study from Spain. Technology, Pedagogy and Education, 27(5), 607–624. doi:10.1080/1475939X.2018.1528997.

[13] Bogdanova, D., & Snoeck, M. (2018). Using MOOC technology and formative assessment in a conceptual modelling course. Proceedings of the 21st ACM/IEEE International Conference on Model Driven Engineering Languages and Systems: Companion Proceedings. doi:10.1145/3270112.3270120.

[14] Giannoulis, A., Theodorakopoulos, L., & Antonopoulou, H. (2022). Learning in second-chance schools during COVID-19 Case study: Legal framework and distance learning platforms in Greek prisons. (2022). European Journal of Training and Development Studies, 9(1), 13–19. doi:10.37745/ejtds.14/vol9no1pp.13-19.

[15] Brands, S. (2000). Rethinking public key infrastructures and digital certificates: building in privacy. Mit Press, Cambridge, Massachusetts, United States. doi:10.7551/mitpress/5931.001.0001.

[16] Camenisch, J., Lysyanskaya, A. (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. Advances in Cryptology — EUROCRYPT 2001. EUROCRYPT 2001, Lecture Notes in Computer Science, 2045, Springer, Berlin, Germany. doi:10.1007/3-540-44987-6_7.

[17] Camenisch, J., & Groß, T. (2012). Efficient Attributes for Anonymous Credentials. ACM Transactions on Information and System Security, 15(1), 1–30. doi:10.1145/2133375.2133379.

[18] Rannenberg, K., Camenisch, J., & Sabouri, A. (Eds.). (2015). Attribute-based Credentials for Trust. Springer, Cham, Switzerland. doi:10.1007/978-3-319-14439-9.

[19] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly: Management Information Systems, 13(3), 319–339. doi:10.2307/249008.

[20] Venkatesh, V., & Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. Management Science, 46(2), 186–204. doi:10.1287/mnsc.46.2.186.11926.

[21] Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. Decision Sciences, 39(2), 273–315. doi:10.1111/j.1540-5915.2008.00192.x.

[22] Ajzen, I., & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Prentice-Hall, Hoboken, United States.

[23] Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. Action Control, 11–39, Springer, New York, united States. 10.1007/978-3-642-69746-3_2.

[24] Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly: Management Information Systems, 27(3), 425–478. doi:10.2307/30036540.

[25] Esteban-Millat, I., Martínez-López, F. J., Pujol-Jover, M., Gázquez-Abad, J. C., & Alegret, A. (2018). An extension of the technology acceptance model for online learning environments. Interactive Learning Environments, 26(7), 895–910. doi:10.1080/10494820.2017.1421560.

[26] Gkintoni, E., Meintani, P. M., & Dimakos, I. (2021). Neurocognitive And Emotional Parameters In Learning And Educational Process. ICERI Proceedings. doi:10.21125/iceri.2021.0659.

[27] Tan, P. J. B., & Hsu, M.-H. (2018). Designing a System for English Evaluation and Teaching Devices: A PZB and TAM Model Analysis. EURASIA Journal of Mathematics, Science and Technology Education, 14(6). doi:10.29333/ejmste/86467.

[28] Tarhini, A., Hone, K., & Liu, X. (2013). Factors Affecting Students' Acceptance of e-Learning Environments in Developing Countries:A Structural Equation Modeling Approach. International Journal of Information and Education Technology, 3, 54–59. doi:10.7763/ijiet.2013.v3.233.

[29] Gkintoni, E., Halkiopoulos, C., & Antonopoulou, H. (2022). Neuroleadership as an Asset in Educational Settings: An Overview. Emerging Science Journal, 6(4), 893–904. doi:10.28991/ESJ-2022-06-04-016.

[30] Wu, B., & Chen, X. (2017). Continuance intention to use MOOCs: Integrating the technology acceptance model (TAM) and task technology fit (TTF) model. Computers in Human Behavior, 67, 221–232. doi:10.1016/j.chb.2016.10.028.

[31] Chao, C.-M. (2019). Factors Determining the Behavioral Intention to Use Mobile Learning: An Application and Extension of the UTAUT Model. Frontiers in Psychology, 10. doi:10.3389/fpsyg.2019.01652.

[32] Fathema, N., Shannon, D., & Ross, M. (2015). Expanding The Technology Acceptance Model (TAM) to Examine Faculty Use of Learning Management Systems (LMSs) In Higher Education Institutions. Journal of Online Learning and Teaching , 11(2), 210–233.

[33] Hu, P.Jh., Hui, W. (2011). Is Technology-Mediated Learning Made Equal for All? Examining the Influences of Gender and Learning Style. Technology Acceptance in Education. SensePublishers, Rotterdam, Netherlands. doi:10.1007/978-94-6091-487-4_6.

[34] Moghavvemi, S. (2015). Impact of Perceived Self-Efficacy and Capability to Use IT Innovation on Individual Use Behaviour. SSRN Electronic Journal. doi:10.2139/ssrn.2561739.

[35] Antonopoulou, H., Halkiopoulos, C., Gkintoni, E., & Katsimpelis, A. (2022). Application of Gamification Tools for Identification of Neurocognitive and Social Function in Distance Learning Education. International Journal of Learning, Teaching and Educational Research, 21(5), 367–400. doi:10.26803/ijlter.21.5.19.

[36] Giannakos, M. N. (2013). Enjoy and learn with educational games: Examining factors affecting learning performance. Computers and Education, 68, 429–439. doi:10.1016/j.compedu.2013.06.005.

[37] Wang, H., & Sun, C. T. (2011). Game reward systems: Gaming experiences and social meanings. Proceedings of DiGRA 2011 Conference: Think Design Play, 14-17, 2011, Hilversum, Netherlands.

[38] Gkintoni, E., Boutsinas, B., & Kourkoutas, E. (2022). Developmental Trauma And Neurocognition In Young Adults: A Systematic Review. EDULEARN22 Proceedings. doi:10.21125/edulearn.2022.1332.

[39] Gkintoni, E., Halkiopoulos, C., Antonopoulou, H., & Petropoulos, N. (2021). Gamification of Neuropsychological Tools as a Multi-Sensory Approach to Education. Stroop's Paradigm. Technium Romanian Journal of Applied Sciences and Technology, 3(8), 92–102. doi:10.47577/technium.v3i8.4798.

[40] Stamatiou, Y.C, Benenson, Z., Girard, A., Krontiris, I, Liagkou, V., Pyrgelis, A., Tesfay, W. (2015). Course Evaluation in Higher Education: the Patras Pilot of ABC4Trust. In: Rannenberg, K., Camenisch, J., Sabouri, A. (eds) Attribute-based Credentials for Trust. Springer, Cham, Switzerland. doi:10.1007/978-3-319-14439-9_7.

[41] Gkintoni, E., & Dimakos, I. (2022). An Overview Of Cognitive Neuroscience In Education. EDULEARN22 Proceedings, Palma, Spain. doi:10.21125/edulearn.2022.1343.

[42] Antonopoulou, H., Giannoulis, A., Theodorakopoulos, L., & Halkiopoulos, C. (2022). Socio-Cognitive Awareness of Inmates through an Encrypted Innovative Educational Platform. International Journal of Learning, Teaching and Educational Research, 21(9), 52–75. doi:10.26803/ijlter.21.9.4.