Available online at www. jenams.com

Journal of Engineering and Management Studies

Vol. 1, No. 1, 05, 2025

Privacy Enhancing Technologies for Next-Generation E-Learning Systems: A Systematic Review

Marwa Alghodi*[1], Abdussalam Shibani[2]

[1] Faculty of science and engineering, University of Wolverhampton, Wolverhampton, United Kingdom
[2] Faculty of Engineering, Environent and science, Coventry University,Coventry, United Kingdom
Corresponding author: m.alghodi@wlv.ac.uk

Received: 4/12/2024; **Accepted**: 5/2/2025; **Available online**: 11/03/2025

ABSTRACT

In this day and age, increased attention is being placed on inserting the internet in many spheres of life, as it is known that education is one of the most important areas in our life, thereby, using the internet in education develops every day, this trend leads to a presence of an enormous amount of data, which it must handle it carefully, and it must be protected in a suitable manner, which makes this request a high priority for all users, it will influence the intention to use any system. For that reason, the existence of a system that protects and preserves data enhances privacy and considers culture will greatly assist and support using any system, especially if it is an education system. Therefore, recent research proposed and evaluated several advanced Privacy Enhancing Technologies (PETs) that were designed to depend on privacy needs and rules. Reviewing the recent literature in this area shows that most studies are focused on the business sector while attempts on the education sector remain relatively very limited. In addition, there is no existing study considering culture in adopting the PETs process in e-learning systems. Hence, this paper intends to contribute to the first Systematic Literature Review (SLR) by adopting a strict search protocol to summarise the current PETs used in e-learning systems in higher education.

Keywords: Privacy, Trust, Security, Privacy Enhancing Technologies, Culture, e-learning.

1. Introduction

Privacy and protecting data have become some of the most significant human rights in this modern age, as mentioned in the United National Universal Declaration of Human Rights of 1948 “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.” Also, The European Convention of Human Rights of 1950 stated that “everyone has the right to respect for his private and family life, his home and his correspondence”. Therefore, there is a global consensus about the importance of privacy and the necessity for its protection. Solove (2008) Friedewald and Pohoryles, (2013), nevertheless, the existing technologies restricted these rights, where they permit to collection, process, and storing the personal data to use it from government and private agencies V. Senicˇar et, al (2003), furthermore, persistent reports of online privacy inroads paint a picture of the internet web turning into a more risky place Friedewald and Pohoryles (2013). Also, (Friedewald and Pohoryles,2013), proved their opinion, where they confirming that even the personal data is limited to a specific user, others can use it for many purposes, it may be harmful to personal, political, or used for commercial purposes, to solve all these issues; laws have been enacted called General Data Protection Regulation (GDPR) in Europe United countries to force all organisations to respect users' privacy, also a new technology called privacy enhancing technologies (PETs) have appeared and applied to prevent *unnecessary* access to data to identify who has the rights to change and access personal data. As a significant part of data privacy procedures, privacy enhancing technologies are becoming widespread in system development. However, there has been no systematic literature review on this topic. To fill this gap, this article presents a review of Privacy Enhancing Technologies. This study aims to help the researchers who achieve this goal, this review was conducted using the most five digital scientific databases, the result of this search provided us with 292 studies and 9 studies were selected for further analysis. work on this topic and make it easier for them, in addition to finding possible directions for further research.

The contribution of this paper is three aspects:

- Providing the first systematic literature review on Privacy Enhancing Technologies (PETs) in e-learning systems.
- Providing insight into PETs in e-learning systems and how these technologies could be employed and evaluated.
- Discovering how cultural aspects affect adopting PETs in e-learning systems.

- Providing future research directions for Privacy Enhancing Technologies.

The rest of this paper is structured as follows: Section 2 presents the related work regarding definitions of security and trust in the e-learning systems, in addition, describes the definitions of PETs, types of PETs, and more explanations about e-learning systems including the next generation of it. Section 3 outlines the review methodology, and the process used in this review. Section 4 presents the results of the found literature. Based on the results, findings and research directions for future work are discussed in Section 5. Finally, the conclusion of this paper is in Section 6.

2. Literature Review

2.1. Privacy in E-Learning

2.1.1.Privacy definition

The definitions of privacy differ from study to study, some studies explained it as one of the most important human rights Bieker et al.(2018) Friedewald and Pohoryles (2013) Romansky and Noninska (2018), on the other hand, we found that other studies classified it as one of the individual demands to choose by them self when, how, and what extends their information and how it will be shared with the others? Mason and Lefrere (2003) V. Senicˇar et, al (2003), and Friedewald and Pohoryles (2013) went away where they linked privacy with freedom and personal and public security, also confirmed that there is a need for a new discussion on privacy limits, which is possible as the governments consider it.

Here in this study for Seničar, Jerman-Blažič and Klobučar, (2003), we can conclude that they combined both definitions that are mentioned above, which defined privacy as an ability and/ or right to save and protect the personal secret information, and the ability and/or right to prevent any inroad on the personal zone. On the same hand el-Khatib et al., (2003), agreeing with the studies above formulated a professional definition of privacy, where they confirmed that privacy can be defined as a user's ability to preserve a personal zone that the user can manage and control which personal information is shared with others.

According to Friedewald and Pohoryles, (2013) study, we can find a comprehensive definition of privacy, they added that privacy is based on confidentiality and data protection. In addition, they described privacy as a significant aspect of one of the constitutive, vital, major polarities that format human beings, that is, the relationship between the individual and their society. In 2006, Solove attempted to identify the common privacy violations by categorising information privacy into four challenges: Information Collection, Information Processing, Information Dissemination, and Invasion of Privacy.

Who will break the privacy?

Many studies assured that two areas could abuse data; business organisations; and government systems, V. Senicˇar et, al (2003) assured that protecting privacy in government bodies is impossible, for example: when people fill out forms for tax returns or apply for licenses; they can not control what kind of personal data will be shared. One of the most important factors in privacy protection is control of personal data, that almost absent in government systems.

How can we protect privacy?

There are two measures to protect privacy which include the application of legislation and implementation of privacy enhancing technologies V. Senicˇar et, al (2003).

2.1.2. Threats Privacy

Regarding privacy; there is an important part has to be explained to identify the privacy enhancing technologies, is privacy threats V. Senicˇar et, al (2003), in order to get an overview of the privacy enhancing technologies that protect data and implement the privacy policy as stated in legislative acts, it is an important part have to been explained, is privacy threats in the communication network such as disclosure the identity and data, observability of data, location disclosure, V. Senicˇar et, al (2003), Several studies have emphasized that there are several types of threats such as HTTP chattering, Cookies and e-privacy threats. E-profiling, and Embedded software. Nowadays, privacy faces various threats, to avoid these threats; and the most common function of PETs is to manage these threats, one of these PETs suggested in a G.W. van Blarkom et, al (2003) study, where it proposed a technology called Identity Protector (IP), this technology controls the exchange of the user's identity across information system, the IP technology could apply in two ways in an agent-based environment:

1. Between the user and the agent: in this case; the IP works to prevent any exchange of personal data from the user to the agent without the IP and the user and approval.
2. Between the agent and the external environment: here the IP helps the agent to protect the user's data.

2.2. Security And Trust In E-Learning

2.2.1.Security in e-learning

The security in e-learning environments examines the means and methods to implement data protection and integrity policies that organisations use in e-learning environments El-Khatib et al., (2003). Security in E-Learning systems can be defined by detecting and preventing processes for unauthorised use of personal computer systems Ahmad and Elhossiny (2012). Using privacy in E-learning is one of the most preferred features by students, it positively affects and leads to better performance in their studies Aïmeur and Hage, (2010). In a study carried out by Analysis of Control Security and Privacy Based on e-Learning Users (Husain and Budiyantara, 2020), where the results confirmed that one of the most effective and important impacts on the user's intention to use E-Learning is the control of privacy and security. This is supported by Hayaati, Alwi, and Fan, (2010) Yang et al., (2002) (Masadeh, Zraqou and Alazab, 2018). On the other hand, (Yong, 2007)

(Bandara, Ioras and Maher, 2014) assured that the attacks will not necessarily come from the outside, they can come from inside the system, therefore, to create a secure e-learning system, the information security management has a significant role Hayaati, Alwi and Fan (2010). In the middle of all these studies which confirm that the security and privacy aspects receive considerable attention, we can find studies which insist that the security and privacy issues in e-learning systems are still neglected Masadeh, Zraqou and Alazab (2018) Warren and Hutchinson (2003), Gan, Chua and Wong (2019) stated that PETs could contain security, where stated where the privacy's main role lies on choosing who has the rights to change and access personal data, and security's role is to execute these choices.

2.2.2. Trust in E-learning

It is worth considering the definition of trust, trust was identified as confidence in someone's efficiency and his/her commitment to a target. In addition, trust is a critical enabler factor for the significant, and mutually useful transactions that encourage cooperation between the student and their institution (May and George, 2011), to keep users safe from threats, and get rid of privacy concerns, we do not just need the technologies resolutions, also, this matter is related with trust (Handy 1995). Hence, May and George (2011) confirmed that there is a strong relationship between trust and privacy, also they complement each other, as well they can work together to create a stable educational environment, May and George (2011) added that, in the real world, in closed educational environment (such as a university or any other trusted and reliable source) where all learning activities are conducted in an internal condition. In this case, the students will be able to work safely and collaboratively with their colleagues and their teachers because they have high confidence that their personal information will be treated securely, on the other side, in an open education environment with anonymous provisioned (such as external or private education systems provisioned) the privacy concern issues will be raised. At the same time, the students' trust level will be affected by the perceived privacy level presented by those provisions Anwar, Greer and Lab (2006) Nickel and Schaumburg (2004) Mason and Lefrere, (2003) As a result, May & George (2011) concluded that privacy and trust are circularly related in any learning systems. This means that if the trust level is high, the privacy concerns will be lower, then the learners will feel more secure, then this situation will encourage them to use their learning system, which can make the educational process more collaborative and stable (May and George, 2011).

On the other hand, M.Anwar and J. Greer (2006) disagreed with this perspective, where they pointed out that until now, in the educational environment, privacy is still considered a natural concern issue, and meanwhile, trust is a particularly crucial factor in an interactive educational environment. In this point, Liu, Xiong and Luo (2013) explained the relationship between privacy and trust in E-learning, where they stated that privacy and trust are very important factors in disseminating knowledge; this can be achieved when trust and privacy work together, where privacy enhances a secure learning environment and the trust promotes a collaborative, healthy competitive, and attractive learning environment. In conclusion of this discussion, if there is any misuse of trust; this will lead to a serious threat to privacy, to resolve these differences, May and George (2011) emphasised that privacy concerns will be resolved by using the technologies approaches, via the best preserving privacy tools, as required by the educational environment, that means integration and development of Privacy Enhancing Technologies (PETs).

2.3. Privacy Enhancing Technologies (Pets)

2.3.1. What are the PETs?

There are many definitions of Privacy Enhancing Technologies in different studies and rules, Coopamootoo (2020) mentioned that the EU Agency for Cyber Security defined the Privacy privacy-enhancing technologies (PETs) as technologies designed depending on the privacy needs and rules, and PETs must be included in a wider extent of technologies that aim to support the data protection and the privacy. Also, Coopamootoo (2020) assured that firstly and before any action, the current uses of PETs must be fully understood to achieve the typical implementation for the PETs.

In line with the prevailing saying that the internet is a dangerous space, the United Kingdom government issued an official report explaining extent the people are harmed on the internet, on this report the UK government suggested a mission that can reduce the dangerous effect of the internet and at the same time preserve the creativity on the internet, Coopamootoo (2020) stated that the most important part in this mission was empowering the PETs in our real life, this official authorisation to introduce these technologies in E-learning environments. Considering one of the most important aspects of our life is education. However, so far there are not enough serious studies that cover using PETs in E-learning environments, especially in higher education.

For more inclusivity study, until now around the world, there is no global privacy or data protection legislation that covers the whole internet *Coop Mootoo* (2020), For example, in Europe, the General Data Protection Regulation (GDPR) is applied in the whole of Europe as one of the most important data protection and privacy laws. On the other hand, In the USA there is not an inclusive law as GDPR (General Data Protection Regulation) Coopamootoo (2020), while the privacy and data protection legislations still vary from country to country, a set of national and international privacy structures have mostly been meet in some points to formulate basic privacy rules, that institute a fair data practice for organisations, businesses and for customers (Coopamootoo, 2020). Regarding the UK, in 2018 the government issued a law to protect the data that considers the users of the internet that was implemented as the GDPR (77), to comply with these governmental rules, lots of organisations invested in PETs to provide protection for personal data Gan, Chua and Wong (2019). On the other side, Pelkola and Canada (2012), argued that privacy attitudes differ significantly from country to country, this contradiction in the opinions leads us to an important question as stated in, Pelkola and Canada (2012) study, which is: what approaches should organisations efficiently and sufficiently protect privacy?

Pelkola and Canada, (2012) emphasised that the solution to this dilemma lies in implementing a framework depending on PETs. Pelkola and Canada, (2012) supported his idea that at present, in this situation that most organisations face, the traditional privacy framework, despite it still being important, but is not working adequately. To achieve a comprehensive understanding of what PETs are; first, the main elements of privacy must be explained, according to W. Staden (2011) data, users of data, and purposes of access to data can form the main elements of privacy in general; he added that to make relationships between them, it could organise them in a hierarchy; allowing more specific descriptions of these categories, for example, in the data pyramid; the privacy will be more specific as one moves downward in the hierarchy of the categories. To link this concept with our subject, the table below explains these elements in the education sector, where it explains the three privacy elements, users of data refer to who can access data, data part refers to what data can users' access, and the purpose of access refers to what is users' reason to access data

Table 1. Privacy Elements in The Education Sector

Purpose of access	Users of data	data
Knowing the university's activities.	Anyone	University name.
Registration, Check their account	Students, staff, teachers	Name, age, postal address, email.
Knowing the results, Payment.	Technics	Results, credit card information

On the other hand, in 1980, the Organisation for Economic Cooperation and Development (OECD) issued a set of main principles of privacy protection; where the most important principles were related to the purpose of access to data; this means that there should be a limiting access to data depending on the purposes that the data will be used for, also, the data is only released if the announced intent matches with the purposes bound to the data. Regarding the PETs elements, (OECD) stated that there are four main elements of PETs: Personal PETs, web-based technologies, information brokers, and network-based technologies, on the other hand, W. Staden (2011) disagreed with this concept, where he confirmed that it is important to realise that the PETs could be classified in many ways, and in his study, he classifies it into four types: Anonymity, Pseudonymity, Unobservability, and Unlikability.

- Anonymity: this is also categorised into three types: Sender anonymity, Recipient anonymity, and Sender/recipient anonymity.
- Pseudonymity: is divided into two types: initial private pseudonyms, and Transactional pseudonyms. W. Staden (2011) clarified that Transactional pseudonyms are the stronger type of pseudonyms.
- Unobservability: the idea behind Unobservability is that the attacker should not be able to observe a particular person communicating with others.
- Unlikability: this means that it should not be possible for an attacker to link two people as they communicate with each other.

2.3.2.Privacy Enhancing Technologies (PETs) Uses

Nowadays, there are many available privacy enhancing technologies, especially for internet users Klobuchar et, al (2003), the PETs appeared with the spread of the use of emails, where there are many PETs technologies have emerged, starting with Remailers: Type-0, Cypherpunk, MixMaster, and MixMinion. And then many technologies have appeared such as The Onion Router (TOR), Flocks, Blender, Dining Cryptographers, and Accountability in the Face of Anonymity. The first PETs model was proposed in 1981 by David Chaum W. Staden (2011) and Elpidoforos Arapantonis (2014). These technologies concentrate on users, where some of them allow users to control the website cookies, others give users more protection, they are able users to surf on the Internet anonymously so that users can get the full technology benefits.

2.3.2.1. Chaum's Mixes

Chaum model concentrates on protecting the email's contents, as the anonymity of the person communicating, the idea for this model lies in encrypting e-mail contents by public keys, thereby preventing attackers from reading the content, there are two types of this MIX:

i. A single MIX: this type is the simplest one, it is a single machine that works as the MIX service provider.
ii. Cascades: this type is more complex, it consists of multiple MIXs as a chain, this process provides more anonymity, where this chain of MIXs prohibits the identity of the sender and the receiver.

Brandi and Olivier (2006) study suggested using P3P technology. This technology allows users to access web servers through a proxy server, where if the user does not agree with the conditions, then the user has the right to take suitable action. However, Ashley, P et, al (2002) and Schunter, M et, al (2002) disagreed with this idea, where they stated that P3P is not a trusted technology because it depends on the extent to which organisations adhere to privacy policies, so there is an opportunity for an organisation to act mala fide.

From this point of view, Valk and Vijfvinkel (2014) discussed in their study how users can choose a server to store their data, and they suggested a new policy called Sticky Policy, this policy allows users to specify what will happen to their data when it across multiple organisations, in addition, users have the control on which servers will store data or choose trust servers to store their data in, to achieve this goal, users can specify:

1. Allow the data to be used on only a specific platform.
2. The third parties that are allowed to process the user's information.
3. Blacklists or deletion/minimization of personal data after a certain time
4. Trusted authorities.
5. The use of personal data, for example, processing of location information or types of market research.

2.3.3.The PETs Types

There are many classifications for these technologies, according to W. Buchanan et, al (2013), PETs refer to a set of technologies that protect sensitive personal data within information systems, there was consensus regarding PETs classifications, where some types almost exist in the majority of studies, the difference is that some studies have considered some technologies as PETs but other studies disagreed with this classification. The table below provides some studies that agreed with some categorised PETs in different classifications as Anonymization, Encryption, and Authentication and Authorisation, these types are virtually in the majority of studies, PETs types may vary depending on the area that will be used in, some areas particularly concerned about the Anonymization more than Authentication and Authorisation, however, other areas concentrate on encryption.

Table 2. Pets Classifications

(Gan, Chua and Wong, 2019)	**W. Buchanan et, al (2013)**	**Eidóforos Arapantonis (2014)**	**B. Shapira et, al (2004)**
-Encryption tools. -Policy tools. - Filtering tools. -Anonymity tools.	-Data minimisation. -Authentication and Authorisation Quality-Enhancing Technology, Separation of data, Privacy, management systems, -Anonymization	-Anonymity and pseudonymity tools for emails: -Type-0 remailers. -Type-I remailers. -Type-II remailers. -Type-III remailers -Anonymity and pseudonymity systems: -Anonymous Proxy Servers -Java Anonymous Proxy (JAP). -Encryption Tools: -TrueCrypt. -Pretty Good Privacy (PGP).	Security-oriented technologies: anonymizers. encryption. identity protectors. Privacy oriented technologies: trust centers.

So these technologies exist in all types of information systems, they also categorised the types of Data minimisation. Authentication and Authorisation Quality-Enhancing Technology, Separation of data, Privacy management systems, and Anonymization, Elpidoforos Arapantonis (2014) illustrated that PETs are one of the types of ICT (Information and Communication Technology) systems that protect privacy by preventing or minimizing personal data leakage thereby banning unwanted processing of personal data, with maintaining the functionality of the information system. Also, Elpidoforos Arapantonis (2014) classified the current implementations of the PETs. Later in 2005, the Danish Government issued a study which separated PETs into Privacy Protection tools or Privacy Management tools:

Table 3. pets' classifications according to the Danish government

PETs	
Privacy Protection tools: • Pseudonymize tools. • Anonymizer products and services. • Encryption tools. • Filter and blockers. • Track and evidence erasers.	Privacy Management tools: • Informational tools. • Administrative tools.

To preserve online privacy, the use of an anonymous network is not enough. The users need to be cautious and also to follow certain standards to maintain a high level of anonymity.

2.3.4.PETs adoption

Despite PETs being widely acknowledged by governments including the UK's Centre for Data Ethics and Innovation Blog CDEI 2021, which supports the adoption of PETs by exploring the role of privacy-enhancing technologies (PETs) in enabling trustworthy use of data, the CDEI confirmed in their report that before adopting PETs, it is necessary to understand the limitation and/or consequences of these technologies, also, it is not possible considering PETs as a comprehensive solution to privacy concerns. In addition, CDEI emphasized that adopting one PET does not guarantee privacy improvement unless comes with a perfect overall privacy design.

2.4. The Benefits of Privacy Enhancing Technologies

The benefits of PETs are numerous, thereby, many studies argued if these technologies have benefits in all areas or it depends on the requirements in every area, in John J. Borking (2011) stated that it seems to be difficult to evaluate PETs economically compared with other protective measures, this happened because the existing ambiguity around PETs, therefore often more traditional measures are chosen instead, however, there is a study from Pelkola and Canada (2012) divided the benefits into two unique ways: quantitative and qualitative, that aimed to more satisfied customers, next table concluded these benefits:

Table 4. Pets Benefits

Quantitative	**Qualitative**

1. Databases will be connected. 2. Data processing will be streamlined. 3. Making privacy easier. 4. services will be more efficient. 1. Decreasing the administ rative load. 2. It can request minimum processing, editing, and inserting of personal data. 3. It can decrease the organization's burden; this enhances confidence and trust in data protection. 4. Reduce the cost of the su pervisory, management, audit, and supervisory fines for data violations.	1. It can help to apply some applications that are not possible to implement manually. 2. It supports submissiveness with privacy data protection regulations. 3. It can raise personal data control. 4. It can help to manage the breaches of privacy risks.

In addition, , (Pelkola and Canada, 2012)assured that manager privacy officers must adopt using PETs early in the life cycle of the project; to get the maximum benefits from PETs, also to make it more efficient, likewise to decrease the cost, where the PETs' cost ranged between 1 to 10 percent from the total of the project cost, to reduce these costs; the privacy concerns must be considered through designing the project, because the cost of inserting PETs in the new applications it will be lower than inserting it in the currently applications (Pelkola and Canada, 2012).

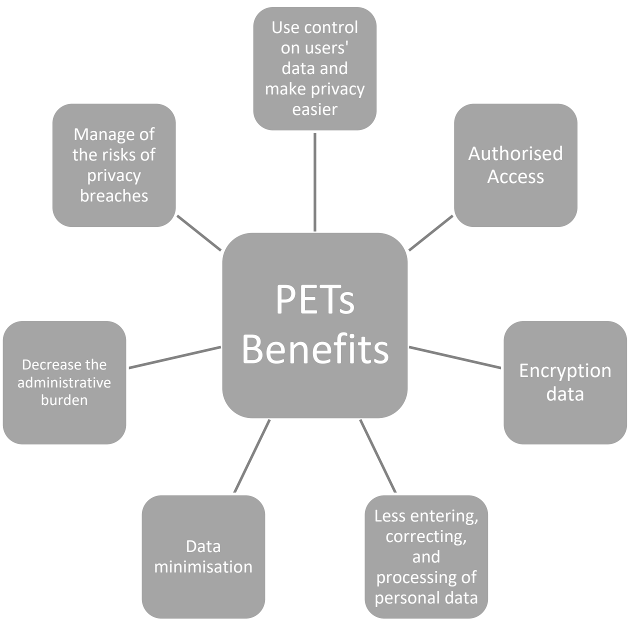

Fig 1. Concludes the Benefits of Pets.

In addition, (Gulhane et al., 2010) pointed out that recently, the industry and educational agencies adopted privacy preserving data to save personal privacy, however, they also argued that PETs can be beneficial just in limited domains, According to G.W. van Blarkom et, al (2003), using the inspections traditional processes to ensure that all organisations that collect personal data are complying with privacy regulations, these inspections are time-consuming and expensive, therefore, using PETs will save time, effort, and costs.

2.4.1.Privacy By Design (PbD)

In the rapidly growing technological change, the privacy protection requirements have to be taken into the account in first steps in the designing process, because the new technological systems may contain hidden dangers which are very difficult to overcome after the basic design has been worked out, therefore logically, identifying possible data protection problems when designing new technology and to integrate privacy protections into the overall design, would substitute for having to come up with laborious and time-consuming "corrections" later on. This approach is known as "Privacy by Design" (PbD). Therefore, new privacy principles have emerged (Peter Schaar 2010).

2.4.2.PET Classification

Generally, privacy enhancing technologies have been classified according to the life cycle of privacy information ((Kang et al., 2007), in this study the life cycle of privacy information was divided into six stages: collection, storage, management, use, provision, and disposal.

2.4.3.Data Masking Approaches

Data masking or data obfuscation can be defined as the process by which sensitive, classified, or personal data is removed or hidden, and manipulated employing character substitution or data replacement by dummy information or fake data (Aslanyan and Boesgaard, 2019). The main job of applying masking to a data field is to protect data that is classified as personally identifiable information, sensitive personal data, or commercially sensitive data from unauthorized access (Sarada et al., 2015), there are many data masking techniques as: Substitution, Shuffling, Number and Date Variance, Encryption, Nulling Out or Deletion, and Masking Outs. Also, Kang et al., (2007) support this definition as they confirmed that various data masking techniques are used to protect sensitive data items, in other studies data masking was identified as a process whereby the information in a database is masked or 'de-identified (Gujjary and Saxena, 2011), adoption of using data masking techniques is the most an effective procedure to secure privacy while preserving usability, where masking data works to encrypt the source of data (Aslanyan and Boesgaard, 2019).

2.5. E-Learning Systems

2.5.1.Definition

To a more comprehensive understanding of how the concept of E-Learning systems has developed over the past decades, the table below gives a review of old E-Learning definitions, starting with using computers to support teaching inside classes, via the advent of the Internet:

Table 5. E-Learning Definitions

Year	Author	Definition
1958	R.F. MAGER (Mager, 1958)	"Known learning principles cannot be efficiently applied in the traditional classroom environment. To achieve efficient learning, it is necessary to remould the teaching-learning configuration to one in which the state of the art can be applied. Teaching machines provide such a configuration and have proved to be dramatically effective in teaching a wide variety of subject matters"
1969	LEON 0. CHUA (Chua, 1969)	"There is no doubt, that the implementation in an on-line environment with rapid man-machine interaction capability would certainly be advantageous"
1999	Hiltz S.R. Turoff M.(Hiltz and Turoff, 1990)	"A Virtual Classroom" [TM] is a teaching and learning environment located within a computer-mediated communication system. Rather than being built of bricks and boards. Participation is "asynchronous," that is, the Virtual Classroom participants can dial in at any time around the clock, and from any location in the world accessible by a reliable telephone system"
1993	DorothyE. Leidner,Sirkka L. Jarvenpaa (Leidner and Jarvenpaa, 1993)	"An electronic classroom is a classroom equipped with computer facilities which an instructor and/or students can use to store, manipulate, or retrieve information during class for presentation, analysis, or communication"
1999	Y. S. Ong H. B. Gooi (Ong and Gooi, 1999)	"The web-based Power Flow Simulator (WPFS) for Power Engineering Education is a newly developed portable software package. It can be accessed by any authorized personnel via the Internet using a Java-enabled browser. Its purpose serves as a means to: • evaluate a possibility for curriculum update; provide an interactive distance learning environment. • enhance student interest and knowledge in power systems over the Internet"

In addition, the following studies such as (Ahmad and Elhossiny, 2012) (Edapeci and Vagarinho, 2020) (Kumar Basak, Wotto and Bé, 2018) (Edapeci and Vagarinho, 2020) (Shetu et al., 2021) (Romansky and Noninska, 2018) (Shivshankar and Paul, 2015) were unanimous in concluding that E-Learning is the term that describes using the web and /or other internet technologies to support learning and teaching processes, E- Learning systems are widespread, varied, and huge. Also, they are characterised by the dynamic with various resources and users, which is considered as the most important feature, where the essential components of any E-learning system are the collaboration and sharing data (Bandara, Ioras and Maher, 2014) (O'leary and Ramsden, 2002) (Shetu et al., 2021) (Johnston, 2020) (O'leary and Ramsden, 2002) (Ahmad and Elhossiny, 2012) (Kidson, 2007) (Hayaati, Alwi and Fan, 2010), On the same hand, the E-Learning systems can be considered as a type of learning that occurs out the traditional learning classrooms (Shetu et al., 2021) (Ahmad and Elhossiny, 2012) (Shetu et al., 2021) (Romansky and Noninska, 2018), In addition, the E-learning systems can be referred to many expressions as online learning, distance learning, or virtual learning, digital collaboration (Ahmad and Ellhossiny, 2012) (Hayaati, Alwi and Fan, 2012).

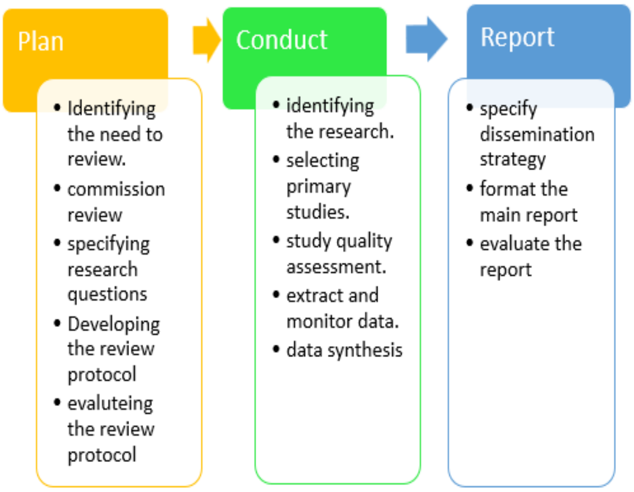

Fig. 2. Phases were conducted in this systematic literature review (SLR)

2.5. Next-generation e-learning environment

The E-Learning sector has experienced considerable development over the past decades, maybe it is going to lead to adopt more technologies to deal with these new privacy challenges (el-Khatib et al., 2003) predicted that in the future, there will be an increasing need for high exacting standards trust and privacy in the E-learning environment, and to face these challenges; the security technologies must be applied to meet these requires. On the other hand, (Aïmeur and Hage, 2010), do agree with this reasoning, they assured that even though the present E-learning standards provide some procedures for security and privacy needs for an E-learning environment, despite this, they still do not satisfy varied levels. To support this result, (May and George, 2011) added that the privacy and security concerns issues have grown by using the current technologies in the existing E-learning systems, that privacy and security will be the most important issues for users in the E-learning environment. At the same time, (May and George, 2011) stated that privacy and security levels are according to students' activities in their learning environment, as a result of this, the standards of security and privacy will differ. In addition, in their study, they assured that they witnessed the collaboration activities between the learners in their learning environments, then in this situation, we cannot guarantee that the learners' data was protected except if their work in an environment that was designed to meet these requirements. According to Hwee et al. (2020), there is a necessity for a reconceptualization of the current E-Learning environments as next-generation e-learning environments, and they also stated that the next-generation e-learning environments have the ability to meet collaborative and individual requirements. The students' perspective could change radically on their E-learning system; when they are just aware that their personal information is used even for academic purposes, as a result of this, this can negatively affect their academic outcomes May, Iksal and Usener (2017).

Regarding E-learning environments in higher education; Matthew Montebello (2017) concluded that Learning Analytics (LA) and Adaptive Learning are considered important developments in educational technology for higher education, in addition, A. Mavroudi et, al (2017) assured that LA and Adaptive Learning are both enhance technologies that support learner-centred education, also they integrate to form a new education way called Adaptive Learning Analytics (ALA), the understanding of ALA is so important not just to students and researchers; but also for e-learning sellers.

2.6.1.Adaptive learning

After the Coronavirus pandemic; the whole world depended on e-learning in higher education, where some of these systems were not at the appropriate state of readiness, also most currently e-learning systems introduce the same education materials for all students with no consideration of individual differences; this may decrease the efficiency of these systems (A. Sarıyalçınkaya et, al 2021), the Adaptive learning emerged to make the e-learning systems more effective, the adaptive learning is defined as educational technology, rather than a method according to Philip Kerr (2015), there is another explanation from A. Mavroudi et, al (2017) which assures that adaptation in e-learning systems is making modifications in an educational environment to accommodate individual differences, the creation of adaptation model is the first step to design adaptation, this model will contain all information about what can be adapted, when and how (Vandewaetere, Desmet, & Clarebout, 2011). The studies refer to the multiplicity of Adaptive learning definitions, such as intelligent adaptive learning systems (E. Herder 2017), adaptive educational hypermedia systems (Peter Brusilovsky 2003), (C. Mulwa et, al 2010), despite all these different definitions; the main goal of all is to provide an effective learning environment suitable for its attributes (A. Sarıyalçınkaya et, al 2021).

2.6. Adaptive goals

The main objectives of the Adaptive goals are as follows:

- *Predicting future student performance.*
- *Providing students with immediately effective feedback.*
- *Providing Personalizing for every student's learning process to know their strengths and encouraging their development.*

2.6.2.Learning Analytics (LA)

There are many studies linking Adaptive learning to Learning Analytics (LA) because they both enhance technology-supported learner-centred education. (A. Mavroudi 2017), LA is also defined as (Simon Paul Atkinson 2015). Furthermore, O. Adejo &T. Connolly (2017) defined LA as a set of analytics methods that improve gathering, analysing, and managing the learners' data to improve the study environment and develop the student learning experience, this definition clarifies that LA emerged as a result of the increasing in education data, this data needs to be taken with caution, this leads to a variety of challenges.

2.6.3.Challenges

Collecting large amounts of students' data may lead to many challenges (O. Adejo &T. Connolly 2017), these challenges relate to privacy and security issues, regarding how to collect and store this data ethically, therefore Cavanagh (2013) confirmed the presence of a significant disruption to privacy rules and regulations in the event of misuse to students' data in Learning Analytic (LA), to overcome these challenges, there must be new procedures against the invasion of privacy in the data analysis process.

2.7. Culture Influences

This section explores how local cultures around the world have influenced the acceptance and use of PETs. It can be expected that taking cultural influences into account will result in more culturally aware PETs. Each society is different in terms of culture, economy, religion, education system, etc. This provides a good opportunity to examine the influence of national culture on the use of PETs. Different attitudes towards various aspects of our lives, as identified by Zivkovic (2017), are the result of culturally shaped behaviours and values. Therefore, in any society, local culture plays a vital role in welcoming or delaying newcomers to technology.

Culture affects privacy concerns and privacy behaviour, for more explanation, according to Lim, Cho and Sanchez, (2009), gender is a key factor, as female and older consumers are generally more concerned about their privacy than male consumers, this leads us to adopt this idea in the education sector, where the female students will be more concern about protecting their personal data.

On the other hand, excessive self-disclosure is considered inappropriate in Eastern culture, and this will lead to increased privacy concerns (Vemou and Karyda, 2013), Also, this study emphasized that culture has a massive impact on users' inclination against using PETs, whilst there is not enough studies coverage on this area.

Our review analysis supported this trend and confirmed that there is still a significant lack of resources that examine the cultural effect of adoption the of PETs, which emphasized the existence of this gap in the previous studies.

3. Review Methodology

The purpose of this study was achieved using a systematic literature review (SLR) as a means of objectively answering our research questions. The protocol follows the SLR guidelines for the computer engineering area proposed by Kitchenham and Charter (2007). These guidelines are divided into three main stages: Planning, Conducting, and Reporting (Figure 1), these steps work together to provide an accurate and reliable methodology. Firstly, the planning stage consists of specifying the main contributions and the research questions. Secondly, the conducting stage, this stage develops the data synthesis and data extraction strategy. Also, the search standards, which include the search strings and search criteria are identified within the conducting stage. Finally, the reporting stage is divided into two steps: identifying the dissemination mechanisms and formatting the main report. These stages of the SLR are repeatedly performed to evaluate comprehensively. Moreover, each stage underwent a review and approval process among the team before moving on to the next stage to reduce bias and to keep objectivity.

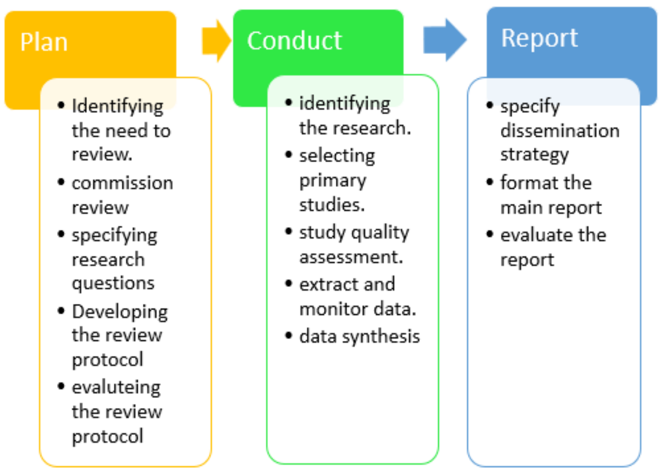

Fig. 2. Phases were conducted in this systematic literature review (SLR)

3.1. Research questions and rationale

Identifying the research questions is the most important step of any systematic review because these questions will drive the whole systematic review methodology Kitchenham and Charters (2007). Furthermore, the goal of this study is to fill a scientific gap in existing research and present valuable help for future research. So, the research questions must be answered to achieve this goal. Next RQ1, RQ2 and RQ3 aim to reveal gaps and key points that exist in present literature and recommendations for future research.

RQ1: How do current frameworks that address PETs support privacy in e-learning systems? OR Which PETs are used to protect privacy in e-learning? The uses and applications of PETs are diverse. Therefore, the answer to this question will summarise a list of all current relevant frameworks that address using PETs in e-learning systems.

RQ2: What are the best PETs that achieved the highest protection level of user data? It is recognised that PETs are rarely used in e-learning systems for various reasons Vemou and Karyda (2013), one of the reasons, that PETs face more challenges in e-learning systems than in other sectors such as the business sector.

To design the research questions effectively, Kitchenham and Charter (2007), proposed The PICOC criteria (Population, Intervention, Comparison, Outcomes, Context) as explained in Table 1 below.

Table 6. Picoc Criteria

PICOC Criteria	Criteria Description
Population	Privacy Enhancing Techniques (PETs) used in e-learning in higher education
Intervention	PETs frameworks that support e-learning
Comparison	Frameworks addressing e-learning and PETs including culture.
Outcomes	Technique
Context	Academic research

3.2. Data sources

The recognisable digital database sources for software engineering research publications have been used in this review as shown in Table 2. This review started in May 2022 and thus reviewed publications up to this date.

3.3. Search strategy

The keywords search and the synonyms must be identified and used to structure the search string by using a Boolean search that uses AND and OR processes to get the best possible search results. The search string was as follows:

(‘Privacy Enhancing Technologies’ OR ‘PETs’ OR ‘PETs frameworks’) AND (‘E-Learning systems’ OR ‘ E-Learning’ OR ‘ education’). Also, this search string used the built-in options within the database search engines from Table 2 for the best outcomes. Moreover, the snowball strategy was applied to make a further relevant study collection.

Table 7. DATABASES

Database	URL
Science Direct	ScienceDirect.com | Science, health and medical journals, full-text articles and books.
Electrical and Electronics Engineers (IEEE)	IEEE Xplore
Scopus	http://www.Scopus.com
ACM Digital library	ACM Digital Library

Google Scholar	http://scholar.google.co.uk

3.4. Selection criteria

The table below demonstrates the strict inclusion and exclusion criteria that were adopted to conclude the relevant studies from the databases to answer the research questions in this review.

Table 8. Inclusion and Exclusion Criteria for The Primary Studies.

Inclusion Criteria (IC)	Exclusion Criteria (EC)
IC1: Must be English language primary study, peer-reviewed	**EC1:** Duplicate studies
IC2: Must contain Privacy Enhancing Technologies (PETs) in e-learning systems	**EC2:** The study is not a framework that supports PETs in e-learning systems**,**
IC3: Must include empirical evidence of PETs framework in e-learning systems	

These criteria were applied after reading the title, abstract, and then the full text of the collected studies Also, each included study has to be qualified for all inclusion criteria, this means these studies must be written in English, peer-reviewed, contain sufficient information on new privacy-enhancing technology in e-learning systems or developed an existing technology.

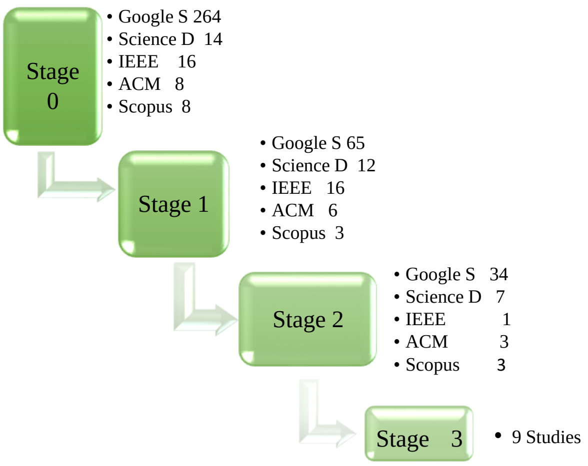

Fig 3. The Selection Process.

3.5. Selection Process

The selection process is multistage (Kitchenham and Charter, 2007), there are three steps in this process as defined in Figure 3. These stages were revised by the authors.

Stage 0__ keyword-based filtering

During this step, the search string was applied to all databases shown in Table 2. This has resulted in a total of (310) studies that were moved to the next stage to filter it.

Stage 1__ Title, Indexing Keywords and Abstract-based Filtering

After the keyword filtering in the last stage, titles, indexing keywords, and abstracts were examined against the inclusion and exclusion criteria. Studies considered to be of any relevance were directly included in the next stage. In conclusion, (208) studies were excluded and (102) studies were included.

Stage 2__ Full text-based filtering

This was the final stage where the full text of (102) studies was read, and the authors discussed and resolved disagreements regarding the relevance of the studies to the study. Upon reconsideration of the inclusion and exclusion criteria, (54) studies were excluded for different reasons. And (48) studies followed the inclusion criteria but some of them did not include any real PETs frameworks that can be applied in the e-learning systems, therefore, the authors decided to add more step that collects the specific studies that can be analysed as a study with real PETs frameworks.

Stage 3__ frameworks-based filtering

The final set of primary studies had a total of (9) remaining studies, these studies contain PETs empirical evidence or framework related to PETs in E-Learning systems.

3.6. *Data Extraction Strategy*

To make sure all included studies had to satisfy with a quality assessment designed as a measure to determine if a given study is suitable to address our research questions. The following quality assessment criteria were applied:

QA1: The study must be related to PETs in e-learning systems.

QA2: The context of the study must be presented in detail to interpret the research accurately.

QA3: The study details must be answered RQ1 and/or RQ2,

QA4: The data must be clearly described how acquired, measured, and reported.

4. Results analysis and discussion

4.1. primary studies

This section aims to analyse the PETs in e-learning systems, in terms of general information (including publication year, number of citations, Authors' names, and countries), as well as the type of PETs employed.

Applying our protocol showed that no primary studies were published before 2003, which indicates that using PETs in e-learning systems is a recent framework. Nevertheless, as Table XI displays, research in using PETs framework in e-learning systems still needs to be studied a lot more, also, this has assured that this research area will be an active research area in the future because it is still adequately undiscovered yet. Our analysis concludes that there were a total number of 10 including studies in the form of journal articles, conference papers, and PhD theses, which were published until May/2022. Our analysis shows most articles were published between 2003 – and 2009, and one study was published in

2014, then the studies came back as one in 2019, another one in 2020, then one in 2021, and two in 2022, which was an early indication that PETs are a research area that started to evolve very recently and needs more effort to discover, especially after some governments issued rules to give users more control over and protect their information. More details are demonstrated in Table 6. There were no effective PETs frameworks assigned to e-learning systems in papers included in Stages 0,1, and 2, they were limited to the recommendations and suggestions for the adoption of PETs, while the 10 selected papers included in Stage 3 provided frameworks to adopt PETs in E-learning system, the PETs frameworks were varied in type, and classification, where some of them are adopted according to specific data protection laws, this means that every data protection law has specific technologies el-Khatib et al., (2003), and some papers focus on one technology which is the basis for the framework.

Table 9 The Distribution Of Primary Studies By Publication Type [Journal Paper (P), Government Framework (G) Or Phd Theses (T)] And Publication Year

SOURCE	03	05	06	08	09	14	19	22	Total
P	2	1	1		1		1	1	7
T						1			1
G				1					1
%	22%	11%	11%	11%	11%	11%	11%	11%	9

4.2. Keywords Analysis

Keyword analysis was conducted on all 10 primary studies to find common subjects between them, the frequency of particular keywords in the primary studies is presented in Table 5. as the table shows that the most repeated keyword among these studies is "user". This indicates that the PETs are centered around supporting users' protection, also in the interest of users in the first place. The second most frequently used keyword is "identity/identification", followed by "Anonymity/anonymous "and "Confidential/confidentiality". This explains the growing research attention on the protection of users' data in e-learning systems. On the other hand, it is clear that the keyword "framework" proves that it is an active but still nascent area of research interest in the context of PETs in the e-learning systems area.

Table 10. Primary Studies' Keyword Analysis

Keyword	Frequent	Studies
User	1621	10
Identity/ identification/s	598	10
Framework	181	10
Anonymity/ anonymous	134	9
Confidential/confidentiality	54	10

' ws various emerging focus areas. Each of these is discussed within section D.

4.4. Chronological Analysis of Main Events

The chronological analysis aims to find the time correlation for the research issuances addressing usage frameworks of PETs in e-learning systems and examine the essential determinants. For more explanations, the primary studies were tabulated in chronological order and organised depending on the publication year and the type of publication, as Table 4. shows.

Notably, the year 2003 was marked by the issuing of the first frameworks (Subirana and Bain, 2003) (el-Khatib et al., 2003), both papers concentrated on the legal aspect, starting with El-Khatib et al., (2003), this study followed Canadian protection laws in which the authors classified a set of privacy technologies for every data protection law, while Subirana and Bain (2003) took into account legal aspects when designing privacy framework for E-learning systems based on software agent, Also, it is noted that papers issued between 2004 - 2009 papers have focused on how to design PETs to protect users' data and empower users to control their data and identify how can access their data. While in the years 2014, and 2019, it was issued two studies were focused on user awareness.

With all these advances in the internet sector, accordingly, e-learning systems have been developed, therefore, in 2022, Marshall et al. (published a study describing a collaborative research project that seeks to overcome the technical and procedural challenges of running a data-driven collaborative research project within an agreed set of privacy and ethics boundaries.

4.5. PETs adoption

Despite PETs being widely acknowledged by governments including the UK's Centre for Data Ethics and Innovation Blog CDEI 2021, which supports the adoption of PETs by exploring the role of privacy-enhancing technologies (PETs) in enabling trustworthy use of data, the CDEI confirmed in their report that before adopting PETs, it is necessary to understand the limitation and/or consequences of these technologies, also, it is not possible considering PETs as a comprehensive solution to privacy concerns. In addition, CDEI emphasized that adopting one PET does not guarantee privacy improvement unless comes with a perfect overall privacy design.

Concerning RQ1, and RQ2, Table 6 below provides a comprehensive description of how current frameworks that address PETs support privacy in e-learning systems. And what types of PETs are adopted in E-learning systems? The PETs were organised in order from most to least used in these studies, as shown in Table 8. Shows that.

Table 8. The Distribution Of Pets By Year, Objective, Typs, And Country.

Year	PETs (RQ1)	Objective	PETs Type (RQ2)	Funded by/ Country
2003	Provide protection traditional based	privacy through or agent- 'Privacy	– Software Agent	Spain

	Enhancing Technologies' (PETs), to reduce or remove threats.		
2003	Satisfying privacy and security requirements for e-learning systems.	– Network Privacy Policy Negotiation. – Trust Mechanisms. – Secure Distributed Logs	National Research Council Canada Institute for Information Technology / Canada
2005	Supporting the learner to define when, how, to whom, and to what extent his/ her personal data is disclosed.	– APPEL P3P language. – XACML format. – Authorization Language (EPAL) seems to be better for the providers than EPAL policies. – authenticate by X.509 public-key certificates or TLS protocol.	This work was supported in part by the EU IST ELENA project / Slovenia.
2006	To enable trustworthy privacy, identity management has to be user-controlled, i.e. each user administrates his/her partial identities being supported by an identity management system running on his/her machines under his/her control.	– User-controlled identity management (pseudonymous, Reputation systems)	Germany
2008	Integration of all technical and non-technical aspects of privacy-enhancing identity management.	– Privacy-enhancing Identity Management – Pseudonyms, unlinkability and credentials that are unfamiliar to many end users.	The PRIME project receives research funding from the Community's Sixth Framework Programme and the Swiss Federal. Office for Education and Science / European United
2009	User-centric Privacy Framework (UPF) is a systematic approach to an overall solution proposal for privacy-enhancing mechanisms in user-adapting systems.	– Opacity Tools, which is also known in the scope of PETs.	The APOSDLE project is partially funded by the European Community (EC)/ Austria
2021	Creating a collaborative research project that seeks to overcome the technical and procedural challenges of running a data-driven collaborative research project within an agreed set of privacy and ethics boundaries.	– Privacy Risk Evaluator – De-identification	Cooperative Research Centres Project - Australian Department of Industry / Australia
2014	To fine-tune the system's internal control and mitigate the associated privacy risks. To address the principles of data minimisation and data sovereignty.	– Customisation of access controls. – User-friendly way of setting privacy. – Data ownership. – No data retention if the user leaves the SN. – Customised search. – Active blocking of information related to users. – Password cracker.	This work is majorly funded through the author's efforts and close relations. /South Africa

As clear above the differences in the adoption of PETs in E-learning from country to country, confirm that PETs types are affected by special needs such as cultural aspects, rules, societal needs, and technique requirements.

4.6. PETs Analysis

To address the main question of how using PETs frameworks and systems that address preserving privacy in e-learning, achieves, the primary studies were arranged in order of the collected evidence of what the technologies used in e-learning systems are.

Even though PETs are widely acknowledged by governments including the UK government's National Data Strategy, the Centre for Data Ethics and Innovation (CDEI) has been exploring the role of privacy-enhancing technologies (PETs) in enabling trustworthy use of data. Which supports the adoption of privacy-enhancing technologies, CDEI in their report 2021 acknowledged that adoption remains relatively nascent. The adoption of PETs by organisations may be hindered by low awareness of technologies, a lack of the expertise required to implement them effectively, or technical limitations.

4.7. Geographic analysis

The goal of the geographic analysis is to provide a better understanding of where the research areas are concentrated. In addition, defining which geographic areas have opportunities for research addressing PETs in E-learning systems. Table 6. shows that the research development is limited to some continents, also it shows that Europe with 62.5% has the highest number of published studies, followed by North America with 12.5%, Australia with 12.50%, and Africa with 12.5%. This emphasises that developing countries are still undiscovered areas and need more research to explore the situation.

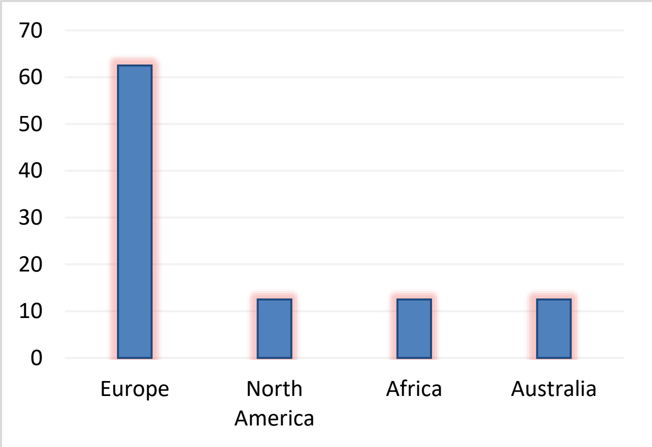

Fig 4. Continental Distribution of Primary Studies

5. Conclusion

It is known that using the internet in e-learning systems led to emerging breaches of users' protection, underscoring the need to adopt PETs to overcome all these breaches. However, despite the importance of using PETs, these aspects have not been extensively considered by researchers in the context of e-learning.

In this review, the analysis of primary studies supports our confirmation that PETs subject still needs more effort for research, many studies concentrated on examining and identifying privacy concerns in e-learning, and explanations on the importance of PETs adoption, but not a real application for those technologies, except the primary studies in stage 3, which offered PETs frameworks to solve different privacy issues and execution the privacy rules.

In this paper, our analysis revealed that PETs technologies vary from country to country and from law to law because each country has its unique characteristics, this means that for adoption any technology must be supported from two aspects, the country's privacy laws, and the country's culture.

As has been noted in our results analysis, several empirical research studies have focused on PETs related to users' protection and awareness. For example, Table 5 identifies the primary studies' main keywords, whilst a summary of primary studies which focused on the types of PETs and their purpose are shown in Table 6. In fact, several empirical research papers presented ways to solve real problems

However, despite the importance of supporting PETs in e-learning systems, these aspects have not been extensively considered by researchers in the context of cultural aspects.

This offers an important question as to considering the cultural aspect as a main aspect when designing and adopting PETs in e-learning systems. However, it is not the aim of this paper to provide the answer but to identify the gaps that can be used in future research directions.

Our analysis emphasizes that funding could be a contributing factor to empirical research in this field of study as Table 6 has shown that almost three-quarters of the primary studies were supported by research grants.

References

[1] Adejo, O. and Connolly, T. (2017) Journal of Education and Practice www.iiste.org ISSN, Online, **8**(15), [online] Available from: www.iiste.org (Accessed 6 December 2021).

[2] Ahmad, A. and Elhossiny, M. A. (2012) E-Learning and Security Threats, *IJCSNS International Journal of Computer Science and Network Security*, **12**(4).

[3] Aïmeur, E. and Hage, H. (2010) Preserving learners' privacy, *Studies in Computational Intelligence*, **308**, pp. 465–483.

[4] Anwar, M., Greer, J. and Lab, A. (2006) Reputation Management in Privacy-Enhanced E-learning,

[5] Arapantonis, E. (2014) Evaluation of Privacy Enhancing Technologies Master of Science Thesis in Networks and Distributed Systems,.

[6] Atkinson, S. P. (2015) Adaptive Learning and Learning Analytics: a new learning design paradigm, [online] Available from: http://www.knewton.com/press- (Accessed 3 December 2021).

[7] Bandara, I., Ioras, F. and Maher, K. (2014) Cyber Security Concerns in E-Learning Education, pp. 728–0734, [online] Available from: http://ecesm.net/sites/default/files/ICERI_2014.pdf (Accessed 14 July 2021).

[8] Bieker, F., Martin, N., Friedewald, M. and Hansen, M. (2018) Data protection impact assessment: A hands-on tour of the GDPR's most practical tool, *IFIP Advances in Information and Communication Technology*, **526**, pp. 207–220.

[9] Brusilovsky, P. (2003) PETER BRUSILOVSKY DEVELOPING ADAPTIVE EDUCATIONAL HYPERMEDIA SYSTEMS: FROM DESIGN MODELS TO AUTHORING TOOLS,.

[10] Buchanan, William J, Ekonomou, Elias, Kwecka, Zbigniew, Buchanan, W J, Kwecka, · Z, Ekonomou, · E, Kwecka, Z and Ekonomou, E (2012) A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services FI-STAR-Future Internet Social and Technological Alignment Research View project Lightweight Cryptography for IoT Devices View project A Privacy Preserving Method U, *Mobile Netw Appl*, **18**, pp. 728–737, [online] Available from: https://www.researchgate.net/publication/255564705 (Accessed 14 October 2021).

[11] Coopamootoo, K. P. L. (2020) Usage Patterns of Privacy-Enhancing Technologies, In *Proceedings of the ACM Conference on Computer and Communications Security*, Association for Computing Machinery, pp. 1371–1390.

[12] Costinela -Lumini, C. and Nicoleta -Magdalena, C. (2012) E-learning Security Vulnerabilities, *Procedia-*

Social and Behavioral Sciences, 46, pp. 2297–2301, [online] Available from: www.sciencedirect.com (Accessed 5 May 2022).

[13] Edapeci, R. and Vagarinho, P. (2020) Issn: 2176 - 171x,.

[14] el-Khatib, K., Korba, L., Xu, Y. and Yee, G. (2003) Privacy and Security in E-Learning, *International Journal of Distance Education Technologies (IJDET)*, **1**(4), pp. 1–19.

[15] Friedewald, M. and Pohoryles, R. J. (2013) Innovation: The European Journal of Social Science Research Technology and privacy, *Innovation: The European Journal of Social Science Research*, **26**, pp. 1–2, [online] Available from: https://www.tandfonline.com/action/journalInformation?journalCode=ciej20.

[16] Gan, M. F., Chua, H. N. and Wong, S. F. (2019) Privacy Enhancing Technologies implementation: An investigation of its impact on work processes and employee perception, *Telematics and Informatics*, Elsevier Ltd, **38**, pp. 13–29, [online] Available from: https://doi.org/10.1016/j.tele.2019.01.002 (Accessed 24 April 2022).

[17] Hayaati, N., Alwi, M. and Fan, I.-S. (2010) E-Learning and Information Security Management,

[18] Herder, E., Sosnovsky, S. and Dimitrova, V. (2017) Adaptive Intelligent Learning Environments,

[19] Husain, T. and Budiyantara, A. (2020) Analysis of Control Security and Privacy Based on e-Learning Users, *SAR Journal*, **3**(2), pp. 51–58, [online] Available from: https://doi.org/10.18421/SAR32-01 (Accessed 14 July 2021).

[20] Hwee, J., Koh, L., Yen, R. and Kan, P. (2020) Students' use of learning management systems and desired e-learning experiences: are they ready for next generation digital learning environments?, [online] Available from: https://doi.org/10.1080/07294360.2020.1799949.

[21] Johannes, W. and Van Staden, C. (2011) A Model for Compound Purposes and Reasons as a Privacy Enhancing Technology in a Relational Database,

[22] Johnston, J. P. (2020) Creating Better Definitions of Distance Education, [online] Available from: https://www.researchgate.net/publication/343916952 (Accessed 14 July 2021).

[23] Kerr, P. (2015) Adaptive learning, [online] Available from: https://academic.oup.com/eltj/article/70/1/88/2450155 (Accessed 24 November 2021).

[24] Kidson, M. (2007) *A discussion paper on*, [online] Available from: http://www.merit.unu.edu/publications/wppdf/2006/wp2006-019.pdf.

[25] Kitchenham, B. A. and Charter, S. (2007) *Guidelines for performing Systematic Literature Reviews in Software Engineering*,.

[26] Kumar Basak, S., Wotto, M. and Bé, P. (2018) E-learning, M-learning and D-learning: Conceptual definition and comparative analysis,

[27] Lakshmi Eswari, P. R. (2011) *A Process Framework for Securing an e-Learning Ecosystem*, *2011 International Conference for Internet Technology and Secured Transactions*.

[28] Lim, S. S., Cho, H. and Sanchez, M. R. (2009) Online privacy, government surveillance and national ID cards, *Communications of the ACM*, **52**(12), pp. 116–120.

[29] Liu, J., Xiong, L. and Luo, J. (2013) Semantic Security: Privacy Definitions Revisited, *TRANSACTIONS ON DATA PRIVACY*, **6**, pp. 185–198.

[30] Masadeh, S. R., Zraqou, J. S. and Alazab, M. (2018) A novel authentication and authorization model based on multiple encryption techniques for adopting secure e-learning system, *Journal of Theoretical and Applied Information Technology*, **96**(6), pp. 1529–1537.

[31] Mason, J. and Lefrere, P. (2003) Trust, collaboration, e-learning and organisational transformation, *International Journal of Training and Development*, John Wiley & Sons, Ltd, **7**(4), pp. 259–270, [online] Available from: https://onlinelibrary.wiley.com/doi/full/10.1046/j.1360-3736.2003.00185.x (Accessed 14 July 2021).

[32] Mavroudi, A., Giannakos, M. and Krogstie, J. (2017) Article in Interactive Learning Environments, [online] Available from: http://dx.doi.org/10.1080/10494820.2017.1292531 (Accessed 24 November 2021).

[33] May, M. and George, S. (2011) Is Using, **1**(1), pp. 1–8.

[34] May, M., Iksal, S. and Usener, C. A. (2017) *The Side Effect of Learning Analytics: An Empirical Study on E-learning Technologies and User Privacy*,.

[35] Montebello, M. (2017) Next Generation e-Learning, [online] Available from: http://dx.doi.org/10.1145/ (Accessed 24 November 2021).

[36] Mulwa, C., Lawless, S., Sharp, M., Arnedillo-Sanchez, I. and Wade, V. (2010) Adaptive Educational Hypermedia Systems in Technology Enhanced Learning: A Literature Review, [online] Available from: http://www.scss.tcd.ie/seamus.lawless/papers/thesis.pdf (Accessed 29 November 2021).

[37] Nickel, J. and Schaumburg, H. (2004) Electronic Privacy, Trust and Self-Disclosure in E-Recruitment,.

[38] O'leary, R. and Ramsden, A. (2002) *Virtual Learning Environments (from The Handbook for Economics Lecturers)*,.

[39] Pelkola, D. and Canada, K. (2012) for Managing Technology, *IEEE Software*, **29**, pp. 45–49.

[40] Review, H. B. and June, M. (1995) Trust and the Virtual Organization Total Quality--Systems Survive , Cultures Change Changing the Role of Top Management : Beyond Systems to People Levi ' s is Leaving China Creating Industry Breakpoints : Changing the Rules of the Game More Boycotts Ahead, *Long Range Planning*, **28**(April), p. 1995.

[41] Romansky, R. P. and Noninska, I. S. (2018) Principles of secure access and privacy in combined e-learning environment: Architecture, formalization, and modelling, *Multidisciplinary Perspectives on Human Capital and Information Technology Professionals*, pp. 152–178.

[42] Sarıyalçınkaya, A. D., Karal, H., Altinay, F. and Altinay, Z. (2021) Reflections on Adaptive Learning Analytics: Adaptive Learning Analytics, [online] Available from:

https://www.researchgate.net/publication/348716769 (Accessed 25 November 2021).

[43] Seničar, V., Jerman-Blažič, B. and Klobučar, T. (2003) Privacy-Enhancing Technologies - Approaches and development, *Computer Standards and Interfaces*, **25**(2), pp. 147–158.

[44] Shetu, S. F., Rahman, M. M., Ahmed, A., Mahin, M. F., Akib, M. A. U. and Saifuzzaman, M. (2021) Impactful e-learning framework: A new hybrid form of education, *Current Research in Behavioral Sciences*, Elsevier B.V., **2**(March), p. 100038, [online] Available from: https://doi.org/10.1016/j.crbeha.2021.100038.

[45] Shivshankar, S. and Paul, S. (2016) E-Learning Environment-The Security and Privacy Challenges Focusing on the Counter Measures, *Proceedings - 2015 International Conference on Developments in eSystems Engineering, DeSE 2015*, Institute of Electrical and Electronics Engineers Inc., pp. 176–179.

[46] Solove, D. (2008) Understanding Privacy, [online] Available from: http://ssrn.com/abstract=1127888 (Accessed 16 July 2021).

[47] Valk, K. and Vijfvinkel, M. (2014) Privacy Enhancing Technologies in Social Networks, [online] Available from: http://www2.uncp.edu/home/acurtis/NewMedia/Social Media/SocialMediaHistory.(Accessed 14 October 2021).

[48] Vandewaetere, M., Desmet, P. and Clarebout, G. (2011) The contribution of learner characteristics in the development of computer-based adaptive learning environments, *Computers in Human Behavior*, Elsevier Ltd, **27**(1), pp. 118–130.

[49] Vemou, K. and Karyda, M. (2013) factors_influencing_PETs_adoption_SNS_draft,.

[50] Yang, C., Lin, O., Lin, H. and Lin, F. O. (2002) Policy-based Privacy and Security Management for Collaborative E-education Systems. * Policy-based Privacy and Security Management for Collaborative E-education Systems 1, p. 44906.

[51] Yong, J. (2007) Digital identity design and privacy preservation for e-learning, *Proceedings of the 2007 11th International Conference on Computer Supported Cooperative Work in Design, CSCWD*, pp. 858–863.