Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Area Six

33rd ECOWAS iSTEAMS ETech Multidisciplinary Conference (ECOWAS-ETech)

Privacy Trust Model in Digital Learning Environments

[1]Ahmed Mai-Inji Yusuf, [2]Longe Olumide Babatope & [3]F Osang, Francis B.
[1,2,3]African Centre of Excellence on Technology Enhance Learning (ACETEL)
National Open University Abuja Nigeria
[2]Faculty of Computational Sciences, Academic City University College, Accra, Ghana
Email: ahmxxd@yahoo.com; longeolumide@fulbrightmail.org; fosang@noun.edu.ng

ABSTRACT

Breach of privacy in the space of internet connectivity is a common event in the massive utilization of digital information in telecommunication technology ground. Securing online information has become one of the biggest challenges in the present day network connectivity. Significant cybersecurity outcome and threat intelligence analysts agreed that cyber related criminal activity is on the increase exponentially. Cyber Security plays an important role in the field of information technology. The adoption of digital learning environment or virtual space for delivery of educational resources in the world of advance technology is widely accepted since the advent of Corona Virus in 2019. Subsequently, this system has several model and level of security trust as well as user privacy while surfing the internet. The confidentiality, Integrity and availability of users' privacy are highly important in the space of billion internet connected devices. Many scientific journals were written on privacy security model and provide a lot of benefit in remodeling users' security threats and vulnerabilities. However, this research is design to improve privacy trust model in relation to online studies for the prevention of personal digital data to curb the present cyber threat in the distance learning environment. The research will adopt conduct review of passed literatures on users' security model and trust privacy in e-Learning environment. It will be established in this paper that digital data breach is imminent and proper security solution. The paper will provide an overview of the techniques and indicators of privacy breach and develop a model that will integrates Trust and Privacy in e-Learning environments by contextualizing the peculiarities of open and distance studies (online learners). The paper is toward improving the existing privacy model in cloud based e-learning environment.

Keywords: - Privacy trust, e-Learning Environment, Digital Data and Security.

Proceedings Citation Format
Ahmed, M.Y., Longe, O.B. & Osang, B.F. (2022): Privacy Trust Model in Digital Learning Environments.
Proceedings of the 33rd ECOWAS iSTEAMS Emerging Technologies, Scientific, Business, Social Innovations & Cyber Space Ecosystem Multidisciplinary Conference. University of Ghana/Academic City University College, Ghana.
29th Sept – 1st Oct, 2022. Pp 27-38. www.isteams.net/ecowasetech2022.
dx.doi.org/10.22624/AIMS-/ECOWASETECH2022P4

1. INTRODUCTION

One of the most essential human rights in the modern world is access to western education, and the key principles in exercising and realizing this right is access to the means of gaining skills, information, and certification. Traditionally, investing in extra educational resources for students outside of schools, such as textbooks and private tutors has always been very expensive. This really limited who had access to the extra resources they needed to succeed in studies.

Digital Learning Environments (DLE) are easily accessible by anyone with an internet connection, whether they're using a laptop, iPad, or smartphone, and many of these resources are available free of charge online. This makes education better, more affordable and available to everyone at any time no matter their financial background. Educational technology makes learning accessible in more ways than just financially; it makes it easier to overcome some of the barriers faced when studying with a disability. For example, digital textbooks can help initiates access to educational resources easier for those who might struggle to go to library due to a physical disability. Digital textbooks often have more options when it comes to how the information is presented, and often the format of a digital textbook can be more easily changed to make the information accessible to visually impaired students [1].

Scholastic technology refers to a wide range of digital educational resources from online courses to games and podcasts that facilitate learning. Educational technology is growing and developing every year, and it is being used more and more by teachers and students today for lesson planning, revision, and self-study. It is transforming the way that students learn, and teachers deliver lesson content. This method is even more pronounced with the emergent of the famous Corona Virus (COVID – 19) [2]. However, the internet is one of the primary means of implementing e-Learning and it has a number of illegal activities and privacy threats.

The issue of security threats, attacks, vulnerability and risks cannot be avoided in the e-Learning environment [3]. Hence, security breaches cannot be extinguished completely in respect to online activities but some remedies can be applied to navigate consciously in DLE. Our research whose thurst is to highlights an integrated security model for DLE is sequences as follows in this report:

Section 1 - Brief introduction.
Section 2 - Rreview of related literatures.
Section 3 - Explores e-Learning environment.
Section 4 - Illustrate the gap in present e-Learning security infrastructures.
Section 5 - Conclusion of paper and remedies offered on DLE privacy breaches in DLE.

2. LITERATURES REVIEW

E-Learning is the fore front in the delivery of education (training and learning) across the world. Online education has indeed shaped the pattern of education and training from the ordinary ways of acquiring knowledge through conventional system [10]. Electronic based education is exceedingly flexible and resourceful education. Accordingly, Doug, L. stated that global pandemic posed by COVID - 19 presented cyber criminals with new opportunities as institutions of learning shifted to DLE [4]. E-learning environment has more tutors and students were commonly online and it can be operated from any location across the globe.

This exposes both parties to greater risk of losing the confidentiality, integrity and availability of vital information. Data trust and privacy can be easily breach particularly when operating from less controlled environments outside the institution networking environment. E-learning platforms provide the opportunity for remote learning, innovation and enhanced learning environments that are student-driven [5]. This rises the concern that the academic record confidentiality, integrity as well availability could be altered. Outline the online challenges at African universities which is mostly relating to connectivity issues, lack of infrastructure, and cost of data, while in Asian countries, such as India and China, the most serious challenges are financial costs, regulations, the digital gap, and the cultural leap for teachers [6].

In Europe, the main obstacles are students' self-motivation and self-organization skills in fully online educational settings. However, the greatest challenge in online education nowadays is the data security which is one of the most critical aspects of e-Learning environment. In July 2020, it was reported that 1,327 data breaches in the education sector had resulted in the exposure of 24.5 million records since 2005 [7]. Higher education accounted for three-quarters of those breaches. Security of digital information remains a serious issue as educational system transverse to online platforms. Primarily, there are four main partners in the e-Learning eco-system. These are Developers, Instructors, Administrators and Learners [8]. However, Jackson's research did not capture privacy trust which a key component in today's online education system. A lot of studies on security breaches and remedies have been put forward in this regards. Consequently, this paper provides a resilience privacy trust model for students and educators on e-Learning environment.

The exiting privacy model for cloud e-learning environment can be as well deployable in all online platforms with little modification. [9] E-learning systems usually store some basic information in the user (learner) profile. Most of this information is very sensitive in the context of privacy. Cause highlights relevant requirements for privacy of users' information in an electronic learning environment.

3. E-LEARNING ENVIRONMENT

During these years of global COVID - 19 pandemic, computers and information technology has changed the world and revolutionized not only the way we work and live our daily lives but also brought rapid changes in online access to DLE. Hence, many institutions opting for online education system bringing improvement and making learning and instructional processes one of the key aspects of the information technology in Education imperative and demanding more than ever before. E-learning platforms provide the opportunity for remote learning, innovation and enhanced learning environments that are student-driven [10]. The DLE enhanced the training method in various circumstances: long distance learning, part-time training, academic courses, and the likes. In fact, the participants can learn courses, take the exams and send the feedbacks or homework online via the website easily and faster.

DLE is an integrated system that includes both information and communication technologies and can be made up of four primary components as follows:

1. Users: Who is individuals' personality that explores the DLE.
2. Data: Is the raw information flows between the users of online education system.
3. Internet: Internet provides the medium for connectivity and transfer of digital information among users.
4. Devices: This cover all devices used in access digital learning environment that stored the running applications.

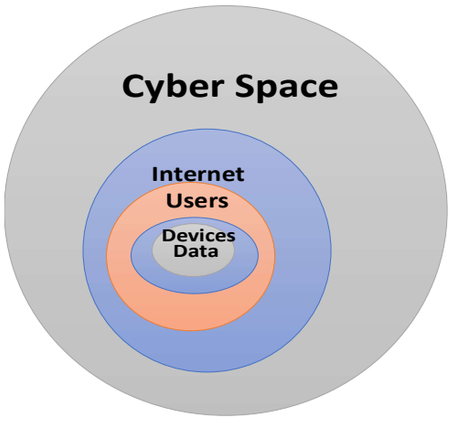

Figure 1: Typical Technological Communication Components.

The technological advancement in educational system brought additional quality to education and save money, time and effort for the learners. In addition, it is convenient and inexpensive means to gain the knowledge and information in pursuing higher education. However, the new opportunities masked with other challenges such as trust and privacy as it relates to the evolution of big data and volume of information stored online. As users of e-learning facilities become more aware of the risks of information disclosure, institutions adopting e-learning will need to do more to assure trust and privacy in e-learning platforms [10, 13].

4. SECURITY CHALLENGES IN E-LEARNING ENVIRONMENT

The biggest challenges faces the DLE development is the increasingly cyber-attack and data breaches. The increased use of technology for teaching, learning and continuing academy operations in today's remote environment, institution have become more vulnerable to cyber-attacks. Doug, L. stated that global pandemic posed by COVID - 19 presented cyber criminals with new opportunities as institutions of learning shifted to DLE [4]. Many programmers have acknowledged the need of designing a safe and trustworthy e-Learning environment. However, many e-Learning application developers continue to struggle with not properly considering data security or encryption in application development. This is typically due to insufficient identification of security implications based on digital data. As e-learning environments become more popular as an instrument of acquiring knowledge online many educational resources have undergone digital modifications. When e-materials become more popular online, they become more prone to attacks. Security and privacy is one of the crucial concerns in e-Learning educational context [14].

Digital educational environment security defilement includes but limited to confidentiality and integrity violation, denial of service attack, unauthorized assessment and authentication bypass. Other challenges may include man in the middle, phishing attacks, IP spoofing and session hijacking. A.A. Maher, H. M. A. Najwa, and I. Roesnita in their paper "Towards an Efficient Privacy in Cloud Based E-Learning" designed a privacy model for e-learning environment. However, personal information security were not spell out explicitly, the model lack comprehensive data security. Figure 2 illustrated the exiting privacy model for e-learning platforms.

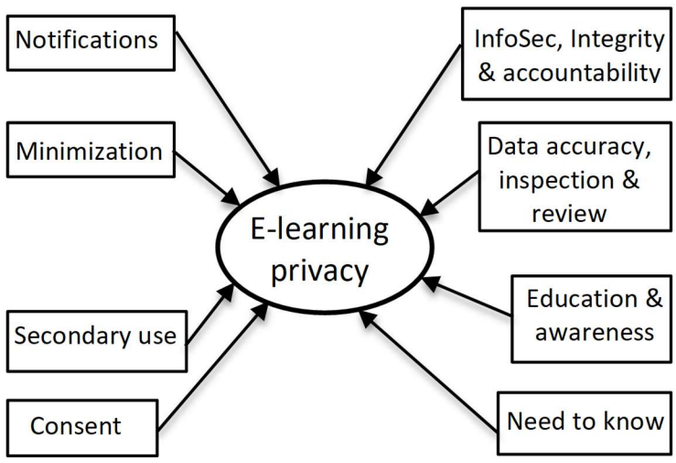

Fig. 2 E-Learning Privacy Requirements [9]

5. Proposed DLE Security Trust Model

Security of digital information is crucial especially in online educations with widely access to internet as a backbone of connectivity in computing networking infrastructure. Privacy issues in distributed learning platforms are somehow difficult to address urging the number of clients, servers, devices and other integrated components in the networks. Since, individual platforms and connected gadgets may have their security policies and appliances. However, in distributed learning environments, security must be considered and developed across the networks (Internet and Intranets).

Digital learning environment security model and mechanisms must be designed to support confidentiality integrity and availability. It may further include authentication, authorization and accountability. Information Security (IS) in ICT can be defined as a combination of properties, which are provided by security services [14]. The first security properties approach is the classic CIA triad that defines the three main targets of information security services: confidentiality, integrity and availability [15].

5.1 Data Protection

Data has never been more plentiful or more valuable, nor has it ever been more at risk from breach. Though billions of dollars are spent each year on cyber security, data breaches continue – everywhere. Enterprises must protect sensitive information. Yet recent industry reports and global surveys show that data is not as secure as it should be (https://www.primefactors.com/). The use of data in organizations usually follows certain guidelines that may reflect consistent procedures and practices of the IT team, especially the database administrator (DBA). As universally understood, the integrity of data (completeness and correctness) is essential to building a robust useful database. Consequently, the security of these data should always be considered a part of its integrity.

5.2 Device Security

A device in this context comprises all gadgets employed in the utilization of DLE. Gadgets connections must be secured, security settings are to be reviewed and smart phone permission is to put on control. Device Security refers to the measures designed to protect sensitive information stored on and transmitted by laptops, smartphones, tablets, wearables, and other portable devices [16]. Devices protection is the goal of keeping unauthorized users from accessing the organization network system.

5.3 Internet Security

The Internet provides a wealth of information and services. Many activities in our daily lives now rely on the Internet, including various forms of communication, shopping, financial services, entertainment and many others. The growth in the use of the Internet, however, also presents certain risks. Internet security is a central aspect of cybersecurity, and it includes managing cyber threats and risks associated with the Internet, web browsers, web apps, websites and networks.

The primary purpose of Internet security solutions is to protect users and corporate IT assets from attacks that travel over the Internet [17]. For the most part, the Internet is indeed private and secure, but there are a number of serious security risks. Risk associated with computer viruses, spyware, phishing scams, spam etc are related to internet once system connectivity is secure many online risk would be eliminated.

5.4 Users Safety

User safety means the practice of identifying, reporting, analyzing and preventing errors that lead to adverse events [18]. Online educators should demonstrate sense of ownership while accessing course platforms. Users neglect much aspect of security authentications as majority of them uses less strong login credentials. Many avoid two factors authentication even though we can secure our devices with just voice recognition permission.

5.5 Digital Learning Environment Privacy Model

Digital learning system frequently stores users' identifiable information in their profile. This information can be used maliciously by an unauthorized entity, as they are very sensitive in the context of privacy. The exiting model lack explicit security layer for users' privacy in DLE. Figure 3 depict improved privacy model. .

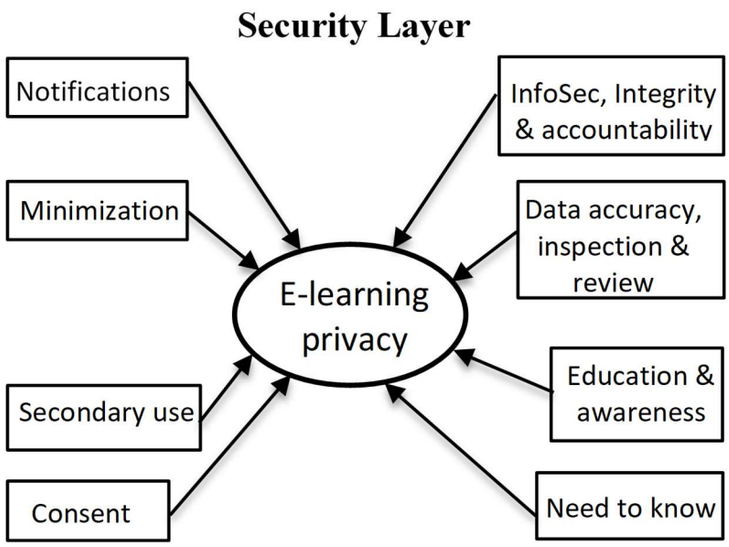

Figure 3: Improve DLE Privacy Model.

The additional security layer consider to provide data protection from all actors involve in planning, designing, execution and the users of online educational system. Figure 4 illustrate the security layer

Figure 4: E-learning Environment Privacy Model Security Layer

a. Digital Learning Environment

The Digital Learning Environment is a suite of technologies that can be used to facilitate and promote good teaching practices and extend your teaching and the learning experience for students beyond the confines of standard teaching spaces in-class and online (https://warwick.ac.uk/services/academictechnology/dle).

b. Facilitators

Facilitators are group of individuals who designed, manage and control the instructional materials on the courseware. They also interact with the learners through the platform and get feedback from their students. Facilitator is commonly defined as a substantively neutral person who manages the group process in order to help groups achieve identified goals [19].

c. Learners

Malik Ghulam Behlol 2010, According to the behaviourists learning is not an active but passive process of memorizing information that requires external reward. According to the humanists learning is a personal act of individual to fully utilize his potential [20]. Online leaners received facilitations from instructors in two major ways. Lectures deliverance can be either synchronous or asynchronous method.

d. Resources

According to the Dictionary.com resource is a source of supply, support, or aid, especially one that can be readily drawn upon when needed [21]. In DLE a resources is the loaded varieties of materials in different format that can be fund and access at the course platform.

e. Devices

A device is a unit of physical hardware or equipment that provides one or more computing functions within a computer system. It can provide input to the computer, accept output or both. A device can be any electronic element with some computing ability that supports the installation of firmware or third-party software. [22]. This couple with internet connection a complete digital learning platform is set to operate.

5.5.1 Security Layer for DLE

Safety on the internet and in the context of educational technology or e-learning is one of the most important aspects of DLE. The e-learning stands nowadays are production systems that require to be safeguarded. This can be attained with a good level of security which may many important elements that must be taken into account: access control, authentication, data integrity and content protection as well as cryptography and network protocols.

a. Access Control

Access control is necessary to prevent illegal accesses to shared resources. Elke Franz, Hagen Wahrig, Alexander Böttcher and Katrin Borcea-Pfitzmann 2006, within eLearning, access control is required in order to protect provided contents and services as well as user data. Usually, access rights are assigned to users of a system. However, in a system that applies privacy-enhancing identity management (PIM) common approaches cannot be directly utilized since users do not act under fix login names [23].

b. Authentication

Authentication is a crucial factor in an e-learning environment. Aeri Leea, Jin-young Han 2020, most of the systems allows students to log into their own space in the e-learning environment through authentication.
Their private space consists of assessments, assignments and discussion. The password-based authentication system is the most cost effective of all and is most commonly used [24].

c. Data Integrity

Anita Lee-Post and Holly Hapke 2017, academic integrity is defined as a commitment to six core values, namely, honesty, trust, fairness, respect, responsibility, and courage, in all aspects of scholarly practices, even in the face of adversity [25]. This is to explore all available security means to ensure data at rest, motion or in modification states are secured.

d. Content Protection

Providing privacy in e-learning focuses on the protection of personal information of a learner in an e-learning system. While secure e-learning focuses on complete secure environments to provide integrity, confidentiality, authentication, authorization, and proof of origin [26].

e. Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages [27].

f. Network Protocols

Networking protocol is a set of rules for formatting and processing data. Network protocols are like a common language for computers. The computers within a network may use vastly different software and hardware; however, the use of protocols enables them to communicate with each other regardless [28].

The DLE security layer measures can be described in table 1.

Table 1: The DLE Security Layer Measures

S/N	Layer	Action	Remarks
1.	Access Control	Strong Login Permission	Used combination of symbols and characters (e.g #$AMIai&232%)
2.	Authentication	Use of biometrics	Thump print, facial recognition etc.
3.	Data Integrity	Secure connection	Avoid public Connection (Free WIFI, hotspots etc)
4.	Content Protection	E-learning environment integrity, confidentiality and availability	Use of authorization and proof of origin
5.	Cryptography	Information encryption	Avoid plain transmission
6.	Network Security	Use of Intrusion Detection System, Intrusion Protection System, firewall.	

6. CONCLUSION

Privacy and information security in e-learning environment is critical. Educational technology makes learning accessible in more ways than just financially; it makes it easier to overcome some of the barriers faced when studying with a disability. Securing online information has become one of the biggest challenges in the present day network connectivity. Significant cybersecurity outcome and threat intelligence analysts agreed that cyber related criminal activity is on the increase exponentially. Scholastic technology refers to a wide range of digital educational resources from online courses to games and podcasts that facilitate learning.

Educational technology is growing and developing every year, and it is being used more and more by teachers and students today for lesson planning, revision, and self-study. The proposed security model is to be used in the improvement of electronic learning platforms. Additionally, the security layer added is to provide more secured environment for online education. Users can adopt various actions describe in the security layer to ensure safety while studying online.

REFERENCES

[1] Giving Knowledge for Free the emergence of open educational resources by Organization for Economic Co-Operation and Development (OECD).

[2] Odili, Ngozi , Adetona, Charity Onoimiuko , Eneh, Anthonia Ebere (2020) Online Resources for E-Learning in Educational Institutions: A Case of COVID-19 Era.

[3] Chen and He, (2013) Handbook of East and Southeast Asian Archaeology.
Susan S Stephen (2010), Trust-Related Privacy Factors in E-Learning Environment.

[4] Doug, L. (2020), Cyberattacks Increasingly Threaten Schools.

[5] Diaz, Golas, & Gautch, (2010). Contemporary privacy theory contributions to learning analytics.

[6] Dodzi Amemado (2020), COVID-19: An Unexpected and Unusual Driver to Online Education.

[7] www.collegiseducation.com accessed on 7 Jun 2022.

[8] Jackson Akpojaro (2019), Security Challenges in Accessing E-Learning System: A Case-Study of Sagbama, Bayelsa State University of African, Toru Orau.

[9] A.A. Maher, H. M. A. Najwa, and I. Roesnita (2014), Towards an Efficient Privacy in Cloud Based E-Learning,

[10] Diaz, Golas, & Gautch, (2010), Privacy Considerations in Cloud-Based Teaching and Learning Environments.

[11] Wannasiri Bhuasiri, Oudone Xaymoungkhoun, Hangjung Zo and Jae Jeung Rho (2012) Critical success factors for e-learning in developing countries: A comparative analysis between ICT experts and faculty.

[12] Ye Diana Wang (2013), Building student trust in online learning environments.

[13] EdTech Series (2020), Education During COVID-19 Crisis: Opportunities and Contstraints of Using EdTech in Low Income Countries.

[14] Luminita (2011), Information security in E-learning Platforms.

[15] Harris, (2002), Democratic leadership for school improvement in challenging contexts. Copenhagen: The International Congress on School Effectiveness and Improvement Conference.

[16] https://www.vmware.com/topics/ accessed 29 Jun 22.

[17] www.checkpoint.com/cyber-hub/cyber-security accessed 29 Jun 22.

[18] www.lawinsider.com/dictionary accessed 29 Jun 22

[19] Glyn Thomas (2010), Facilitator, Teacher, or Leader? Managing Conflicting Roles in Outdoor Education University of the Sunshine Coast 2010.

[20] Malik Ghulam Behlol (2010), Concept of Learning by Malik Jinnah Women University.

[21] https://www.dictionary.com accessed 5 July 2022.

[22] www.techopedia.com accessed 5 Jul 22.

[23] Access control in a privacy-aware eLearning environment by Elke Franz, Hagen Wahrig, Alexander Böttcher and Katrin Borcea-Pfitzmann.

[24] Effective User Authentication System in an E-Learning Platform by Aeri Leea and Jin-young Hanb 2020.
[25] Online Learning Integrity Approaches: Current Practices and Future Solutions by Anita Lee-Post and Holly Hapke of University of Kentucky 2017.
[26] Secure E-Learning and Cryptography
[27] E-learning system using cryptography and data mining techniques by VijayaPatil, Aditi Vedpathak, Pratiksha Shinde, Vishakha Vatandar and Prof. Surekha Janrao of Terna Engineering College, Maharashtra, India 2018.
[28] www.cloudflare.com/learning accessed 5 Jul 22.