e-ISJN: A4372-3114
p-ISJN: A4372-3115

ISSN: 2321-7782 (Online)
ISSN: 2347-1778 (Print)
Impact Factor: 7.529

Volume 10, Issue 7, July 2022

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Online Class: Student Data Privacy

Joey De la Cruz
College of Information and Communications Technology
Nueva Ecija University of Science and Technology
Cabanatuan City, Philippines.

Abstract: ***Cyberspace refers to the Internet as unlimited space. Cyber Security is the body of rules set up to protect this cyberspace. Numerous studies have reported the growing use of online classes and have shown continued growth; Slight consideration has been devoted to protecting student data in education.***

Online classes' privacy is indeed a specific challenge as thousands of people connect and manage various systems over thousands of networks through the Internet. It also emphasizes the incidence of internal cyber-attacks and the lack of acceptable IT policies and procedures in the online class, taking into account their primary characteristic and relevant security specifications.

Discuss the most critical threats and issues on student data, the countermeasures, and strategies for enhancing online classes' security policies and frameworks. It also provides an awareness-raising mechanism to address the need for more robust security measures. Such as Prevention of Threats, Identification Security, compliance with the Law of Academic Institutions, and Ethical Conduct to Protect Student Personal Information both now and in the future.

Keywords: Online Education, Data Privacy, Cyber Attacks, Cyber Risk, Internet.

I. INTRODUCTION

COVID-2019 seriously impacts several countries' economies. The outbreak also changed operating conditions around the world within a period. The consequences of the pandemic are imminent and unmanageable for many industries worldwide. Later, almost 120 countries stopped face-to-face learning; with COVID-19, nearly one billion students are taught worldwide. Much of the higher education system operates through online classes [1]. Meanwhile, almost every country, including the Commission on Higher Education, has mandated closing public and higher education as a matter of urgency to prevent infection transmission and resolve the COVID-19 pandemic.

In response to learners' needs, particularly the 3.5 million tertiary students enrolled in approximately 2,400 HEIs, some HEIs in the country have adopted constructive policies for continuing education despite the closure. These policies provide updated modes of online classes that are intended to promote student learning activities. Online learning can be synchronous, real-time lectures and time-based evaluation of results or asynchronous, delayed-time tasks, such as pre-recorded video lectures and time-independent assessments [2].

Various factors must be addressed as the Philippines is entering a new way of learning. This includes the instructor's ability, the learner's circumstance, meaning, student data privacy, and the quality of the learning environment. These are the top of the more obvious problems of Internet latency, content costs, and delivery. The best way forward is to take a step back and formulate a plan that engages teachers, students, parents, school administrators, and technology-based businesses. Based on a shared vision, this collaborative response is the innovative solution that this new problem warrants [3]. As stated, when the

information is revealed, the mutual ownership of the shared information emerges. There are several ways to exchange information, and there is a need to manage data privacy. If data is shared with instructors, administrators, parents, or higher education personnel in school information systems, personal data is moved to a collective privacy limit. [4].

This position paper aims to focus on where online classes focus on three main pillars: (a) how to mitigate attacks and threats on student data; (b) what are the countermeasures and strategies for enhancing online education security, and (c) what are the security policies and frameworks for online learning.

A. Online Class

Online classes are learning opportunities in synchronous or asynchronous settings utilizing different devices. (e.g., cell phones, laptops, etc.) and the Internet. Students learn and communicate with teachers and other students in this setting, anywhere (independent) [5].

Online education relies on networks. Students may have their learning sequenced, guided, and evaluated with the instructor's aid. This exchange occurs within the research group, using a combination of synchronous and asynchronous internet-based activities (video, audio, computer conferencing, chats, or virtual world interaction) [6]. The synchronous and asynchronous online environments facilitate social, collaboration skills, and personal relationships between participants.

B. Online Class Technology

The online class is "a form of the delivery method used in remote learning and allows synchronous and asynchronous information exchanges over a communications system" [7]. Uses internet technology to help learners communicate with teachers and other learners. [8]. Modern web-based innovations, such as social media have enabled instructors to make different choices about learning. [9]. Social networking enables learners to produce their content openly and form learning groups, as the media facilitates collaboration between learners and teachers. [10]. More recently, extensive open online courses (MOOCs) have gained much attention from higher education institutions worldwide. [11].

C. Data security

In online classes, protection means that "information resources are available and unchanged to all legitimate personnel when needed" [12]. Since online learning occurs through the Internet, any part of the online learning system can be hacked or attacked. It can result in unauthorized alteration and devastation of educational properties. [13]. Online classes must recognize the Internet's inherent security threats, such as identity theft, impersonation, and insufficient authentication [14]. Online class technology has attracted cybercriminals who rely on their ability to hack into these systems. The danger is significant; online classes' functionalities and features become more complex; online classes are exposed to growing security threats [15].

D. Online Security

According to [16], Digitalization may pose many security threats in an online class, such as loss of privacy and accessibility, exposure to sensitive data, and public information services vandalism. As protection mechanisms have been put in place in online classroom programs, insufficient user knowledge of security measures, lack of interference, and lack of education have usually triggered security issues in the online classroom. For example, major online learning providers have introduced firewalls and anti-virus software to protect their learning tools in virtually every organization. [17]. Their online classroom services continue to expand content and technology to ensure learning opportunities. [15][18]. However, thus user protection awareness and skills have improved greatly. Security problems such as misuse of information by associates (students or insiders) and lack of privacy continue to occur from time to time. [19]. Security is important to preserve users' confidence in the online classroom environment, as any threat can dramatically impact students' expectations of the system's functionality and reliability. [12].

II. METHOD

This work reviewed published studies and research on risks and challenges to student data privacy in online learning, specifically, (a) how to mitigate attacks and threats on student data; (b) what are the countermeasures and strategies for enhancing online education security, and (c) what are the security policies and frameworks for online learning.

A. Data Sources

The stages of the literature search began with literature reviews as a basis for this research before 2020.

B. Criteria for selection

The researcher used extensive literary research using academic databases, including the Research Gate and the Google Scholar Web Search Engine. Thirty articles were chosen to answer research questions: (1) How to mitigate attacks and threats on student data? (2) What are the countermeasures and strategies to enhance protection in online teaching? (3) What are the security policies and frameworks for online learning??.

Data Analysis

The researcher noted security risks and threats in online learning and classified the themes based on the theoretically defined paradigm of data protection and privacy and proper use of student data. The researcher categorizes the findings into three primary areas: mitigation of attacks and threats, countermeasures to improve security online, and security policies. The approach will be used in the qualitative information collection to process data [20].

III. RESULTS AND DISCUSSIONS

A. Attacks and threats on student data

Educational institutions should carefully develop cybersecurity expertise at the institutional level of top management as the ultimate authority accountable for all kinds of security, including users, students, academic staff, and employees. These policies can then be enforced and applied at all levels of management to ensure protection and compliance. [22] Suggested that lack of information is a serious problem for every organization and should be appropriately assessed as part of its overall security management and evaluation strategy. Also, [23][24] suggested that the system comes from the academic organization's top leadership. IT services can be better governed to benefit from customers' cooperation and compliance with their commitments to use facilities and services. Besides, users must track and control their conduct for any breach of security as set out in the academic institution's rules and laws relating to the country's general law and other international regulatory bodies, as they may be. Users must also monitor and manage their behavior for any security breach in the guide[23]. Once the safety implications have been measured, they can be reduced by increasing security knowledge through educational/training initiatives within the academic institution's atmosphere by holding seminars or workshops to promote these security resources and facilities' active use.

B. Countermeasures and Solutions

Some of the technologies that ensure the protection of online classes are listed below. The malicious attack, computer viruses, malware, and Trojan are malicious programs that alter or destroy the operating system without the user's permission. We should use spam filters to prevent malicious spam, Trojan, and virus email attachments. Some malware and Trojans are usually connected to emails as students or instructors download materials from the systems. We also use the Secure Protocol (HTTPS) to search websites and applications to protect the device's privacy and data. [28]. Two types of attacks are available: flood and block attacks such as DoS (Denial of Service) and communications infrastructure threats. [26]. It is highly recommended that you use the IDS (Instruction Detection System) or Firewall to detect these attacks. Regular backup is also one of the best means of preserving stable data and battling possible attacks. An authentication attack means hackers can access

a device using stolen passwords or keys. One precaution against this assault is using a biometric authentication method, as it is difficult to steal or reuse passwords easily. The web browser can use HTTPS (Secure Socket Layer). [26]. Session eavesdropping and Session Traffic Analysis are some of the forms of this attack[27]. This attack attempts to expose private and confidential data to unauthorized users. We use a robust cryptography mechanism to fight this kind of attack. Instead of placing it in plain text, we encrypt personal information in storage to enable hackers to access this necessary information. Authorization should be taken seriously by separating the user's right to access each data requirement.

C. Policies and Mechanism on data privacy

The transition to digital, which has had a growing impact on the higher education environment and has recently been intensified due to the global COVID-19 pandemic, provides many learning analytics opportunities to improve student learning. Growing the usage of digital technologies to support learning and teaching implies an increase in data production that can be analyzed to provide insights into student conduct and academic achievement. However, with this increased flow of data and an ever-changing variety of analytical methods and techniques, it is essential to pause and consider whether the data is being used ethically and does not cause threats or harm to students [30]. From a policy perspective, effective policies and procedures need to be put in place and implemented to ensure the protection, privacy, and ethical use of student data. In designing such policies, it is essential to understand students' views on what data they can share and for what reasons to balance their interests and concerns with the processes and protections in place [29].

IV. Conclusion and Recommendation

Online classes are gradually becoming a primary learning method for all, especially during the COVID-19 pandemic. Information is collected during the online study, and mastering the necessary skills for learners to protect their data and privacy in online classes is urgent. On the other hand, this study focused on possible security problems and countermeasures in the online class culture. It also provides a sensitization framework to satisfy the need for other extensive protection measures. Trust the security of identity and conformity with the laws and ethical conduct of academic institutions, both now and in the future. Faculty and student data should always be protected and kept private. Robust implementation of data confidentiality is essential. Every educational institution should provide a data security system to secure student and faculty files, databases, and network accounts. By promoting a secure system, datasets are then protected from external threats.

References

1. "Effects of COVID-19 in E-learning on higher education institution students: the group comparison between male and female | SpringerLink." https://link.springer.com/article/10.1007/s11135-020-01028-z.
2. "Exploring asynchronous and synchronous tool use in online courses - ScienceDirect." https://www.Science direct.com/science/article/abs/pii/S0360131512001935?via%3Dihub.
3. J. J. B. Joaquin, H. T. Biana, and M. A. Dacela, "The Philippine Higher Education Sector in the Time of COVID-19," Front. Educ., vol. 5, 2020, doi: 10.3389/feduc.2020.576371.
4. C. Mullen and N. Fox Hamilton, "Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence," Comput. Hum. Behav., vol. 60, pp. 165–172, Jul. 2016, doi: 10.1016/j.chb.2016.02.026.
5. V. Singh, "How Many Ways Can We Define Online Learning? A Systematic Literature Review of Definitions of Online Learning (1988-2018).," Am. J. Distance Educ., vol. 33, no. 4, pp. 289–306, 2019.
6. M. Malik, G. Fatima, A. H. Ch, and A. Sarwar, "E-Learning: Students' Perspectives about Asynchronous and Synchronous Resources at Higher Education Level," p. 13.
7. Khan, B. H. (1998). Web-based instruction (WBI): An introduction. Educational Media International, 35(2), 63-71.
8. Sasikumar, M. (2013). E-learning: opportunity and challenges. Retrieved from http://www.cdacmumbai.in /design/corporate_site/override/pdf-doc/e-learning.pdf
9. Neville, K., & Heavin, C. (2013). Using social media to support the learning needs of future IS security professionals. Electronic Journal of e-Learning, 11(1), 29-38.
10. Redecker, C., Ala-Mutka, K., & Punie, Y. (2010). Learning 2.0-The impact of social media on learning in Europe. Policy brief. JRC Scientific and Technical Report. EUR JRC56958 EN. Retrieved from http://www.ict-21.ch/com-ict/IMG/pdf/learning-2.0-EU-17pages-JRC56958.pdf

11. Meyer, J.P., & Zhu, S. (2013). Fair and equitable measurement of student learning in MOOCs: An introduction to item response theory, scale linking, and score equating. Research & Practice in Assessment, 8(1), 26-39.
12. Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. Usability Evaluation of Online Learning Programs, 331-359.
13. Zuev, V. (2012). E-learning security models. Management, 7(2), 24-28.
14. Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2011). Towards e-learning security: A machine learning approach. In Information Society (i-Society), 2011 International Conference (pp. 490-492). IEEE.
15. Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. International Journal of Digital Society (IJDS), 1(2), 148-156.
16. Graf, F. (2002). Providing security for eLearning. Computer & Graphics, 26(2), 355-365.
17. Weippl, E., & Ebner, M. (2008). Security privacy challenges in e-learning 2.0. World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education (Vol. 2008, No. 1, pp. 4001-4007).
18. Srivastava, A. & Sinha, S. (2013). Information security through e-learning using VTE. International Journal of Electronics and Computer Science Engineering, 2(18), 528-531.
19. Dietinger, T. (2003). Aspects of e-learning environments (Unpublished doctoral thesis). Institute for Information Processing and Computer Supported New Media (IICM), Graz University of Technology, Austria.
20. S. Cavanagh, "Content analysis: concepts, methods, and applications," Nurse Res., vol. 4, no. 3, pp. 5–13, Apr. 1997, doi: 10.7748/nr1997.04.4.3.5.c5869.
21. S. Al-Janabi and I. Al-Shourbaji, "A Study of Cyber Security Awareness in Educational Environment in the Middle East," J. Inf. Knowl. Manag., vol. 15, no. 01, p. 1650007, Mar. 2016, doi: 10.1142/ S0219649216500076.
22. Yeo, AC, MM Rahim, and L Miri (2007). Understanding factors affecting the success of information security risk assessment: The case of an Australian higher educational institution. In PACIS Proceedings, 74pp.
23. Hu, Q, T Dinev, P Hart and D Cooke (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture*. Decision Sciences, 43(4), 615–660, doi: 10.1111/j.1540-5915.2012.00361.
24. Goo, J, MS Yim and DJ Kim (2013). A pathway to successful management of individual intention to security compliance: A role of organizational security climate. In Proceedings of International Conference on System Sciences (HICSS), 46th Hawaii, pp. 2959–2968, doi: 10.1109/HICSS.2013.51.
25. Chan, H and S Mubarak (2012). Significance of information security awareness in the higher education sector. International Journal of Computer Applications(0975–8887), 60(10), doi: 10.5120/9729-4202.
26. Rjaibi, N., Rabai, L.B.A., Aissa, A.B., Louadi M.: Cyber Security Measurement in Depth forE-learning Systems. International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 11, 1-15. (2012).
27. Hye-jin Kim, "E-learning Privacy and Security Requirements," Journal of Security Engineering, 10(5), pp.591-600, (2013).
28. N. Huu Phuoc Dai, A. Kerti, and Z. Rajnai, "E-Learning Security Risks and its Countermeasures," J. Emerg. Res. Solut. ICT, vol. 1, no. 1, pp. 17–25, Apr. 2016, doi: 10.20544/ERSICT.01.16.P02.
29. Sharon Slade, Paul Prinsloo, "Learning Analytics: Ethical Issues and Dilemmas - 2013." https://journals.sagepub.com/doi/10.1177/0002764213479366 (accessed Jan. 12, 2021).
30. D. Ifenthaler and C. Schumacher, "Student perceptions of privacy principles for learning analytics," Educ. Technol. Res. Dev., vol. 64, no. 5, pp. 923–938, Oct. 2016, DOI: 10.1007/s11423-016-9477-y.

