Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 21(1): 32-44, Mar. 2023 Regular paper

Information Security on Learning Management System Platform from the Perspective of the User during the COVID-19 Pandemic

Mujiono Sadikin[1]*, Rakhmat Purnomo[1], Rafika Sari[1], Dyah Ayu Nabilla Ariswanto[2], Juanda Wijaya[3], and Lydia Vintari[3]

[1]Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Bekasi 17121, Indonesia
[2]Faculty of Business, IPB University, Bogor, Indonesia
[3]Faculty of Computer Science, Universitas Mercu Buana, Jakarta 11650, Indonesia

Abstract

Information security breach is a major risk in e-learning. This study presents the potential information security disruptions in Learning Management Systems (LMS) from the perspective of users. We use the Technology Acceptance Model approach as a user perception model of information security, and the results of a questionnaire comprising 44 questions for instructors and students across Indonesia to verify the model. The results of the data analysis and model testing reveals that lecturers and students perceive the level of information security in the LMS differently. In general, the information security aspects of LMSs affect the perceptions of trust of student users, whereas such a correlation is not found among lecturers. In addition, lecturers perceive information security aspect on Moodle is and Google Classroom differently. Based on this finding, we recommend that institutions make more intense efforts to increase awareness of information security and to run different information security programs.

Index Terms: Information security, E-learning, Moodle, Google Classroom, User perception, COVID-19

I. INTRODUCTION

Currently, the e-learning systems are becoming increasingly important because of the digitalization of education. Most educational institutions utilize e-learning systems considering the significant advantages. These include flexibility in terms of time and space, cost, and infrastructure efficiencies, and also overcome traffic jams, which is a common problem in major cities [1,2]. The COVID-19 pandemic, the importance of e-learning systems in education and teaching mushroomed. Many studies have shown that online learning system environments, such as Moodle and Google Classroom have been widely appreciated [3-6]. As the learning process enabler, e-learning provides numerous benefits such as flexibility in learning material format (text, audio, video, image) and storage media for teaching materials, lower cost for students, and increase in the capacity of classrooms [7]. Furthermore, the decrease in energy consumption and paper usage reduces the negative impact of education-related activities on the environment [8]. E-learning systems also offer benefits in terms of instructor - student interactions, such as flexibility, usability, and efficiency in face-to-face learning [9]. According to Fatoni et al. [10], the most advantageous feature of e-learning systems is the comfortable educational environment.

The security concerns associated with the COVID-19 pan-

Received 2 December 2022, **Revised** 21 January 2023, **Accepted** 25 January 2023
***Corresponding Author** Mujiono Sadikin (E-mail: mujiono.sadikin@gmail.com)
Faculty of Computer Science, Universitas Bhayangkara Jakarta Raya, Bekasi 17121, Indonesia

Open Access https://doi.org/10.56977/jicce.2023.21.1.32 print ISSN: 2234-8255 online ISSN: 2234-8883

demic forced humankind to pursue all possible activities online, including education and teaching. Thus, e-learning systems have become a necessity, and the entire academic community must be familiar with them [11,12]. However, e-learning during the pandemic faces various challenges and risks that must be overcome [13-15]. Most of the risks that have been identified are related to information security issues, such as Internet traffic, which is specific to COVID-19/data availability, lack of data processing, illegitimate use, data integrity disruption, and privacy violation [11,16,17]. Accordingly, several approaches have been proposed to address the information security issues of e-learning systems during the pandemic era, such as the framework of intrusion detection [18], online learning quality assessment [12], and cryptography [17].

The Learning Management System (LMS) is the most important component of e-learning systems. Owing to the increasing demand for LMS during the COVID-19 outbreak, numerous LMS applications have been developed and recommended, either as open source, proprietary, cloud, or on-premises models. Meanwhile, as a response to the COVID-19 outbreak, UNESCO released a distance learning system recommendation comprising 11 systems. Two of these are Moodle and Google Classroom [19].

Moodle LMS is one of the most popular LMSs [20-22]. Various implementation models of the Moodle LMS have been demonstrated, ranging from the standard version to the customized module. The deployment of Moodle LMS customization covers a wide range of scope to fulfill the specific requests of each organization that implements the system [23,24]. To achieve better performance and continuity of services, various architectures have also been implemented, such as the load-balancing clustering scenario [25].

The usage of Google Classroom also increased dramatically during the pandemic [26]. Google Classroom is one of the three most adopted ready-to-use LMSs in developing countries during the outbreak [27-29]. It is also among the top three learning tools chosen by students [30]. In areas where a limited LMS system, such as global contact lens education, was used prior to the pandemic, Google Classroom is the third most used below Zoom and WeChat [31]. Google Classroom is also the most popular LMS platform for various of educational institutions in Indonesia owing to the fact that it is readily usable and can be easily set up. To be precise, the user is not required to install and set up the application, which is required for the Moodle LMS. Some studies regarding the benefits of using Google Classroom by Indonesian education institutions are presented in [5,6,32-34].

However, several risks are embedded in these LMSs. One such risk is the disruption of information security, which can appear in various forms, such as viruses, spyware, malware, ransomware, Denial of Service (DOS), or information accessed by unauthorized users [35]. The access of information/data by an unauthorized user is based on various objectives, including abuse of authority, changing data on activities, stealing information, or for certain trivial reasons [36,37]. The risk of unauthorized access to information typically increases if the system environment does not support information and system protection. In addition, users who lack information security knowledge or information security awareness are exposed to a greater risk of information security disruption. The literature review study presented in [38] shows the importance of human factors for any organization to ensure a culture of information security.

The information security concept represents the balancing of *Confidentiality, Integrity,* and *Availability (CIA)* [39,40]. "Confidentiality" refers to the condition that information sources remain hidden to all parties except for those with authorization. The principle of "Integrity" stipulates that data/information integrity and consistency are maintained at various levels and in various forms of presentations. Finally, "Availability" requires that all necessary data/information must always be available to authorized users. The basic rule of information security is that all three elements must be balanced. For example, a request to increase the level of confidentiality should not result in inaccessibility of the data/information, which it is a decrease in availability.

The risk of disruption of information security must be governed properly to ensure that whenever gaps in the security are exploited, the impacts can be minimized [41]. Accordingly, the disruption potentialities must be identified. Typically, sources of information security disruption vary, ranging from hardware or software malfunction, to human activities, such as hacking or misuse by internal users [42]. In most cases, internal user disruptions have more serious repercussions.

Various models, methods, and deterrents of information security disruptions have been studied and practiced. Lavanya et al. [43] proposed an elliptic curve cryptography algorithm (ECC) to protect data confidentiality and integrity in cloud-based e-learning systems. This method was used to counteract DOS attacks and DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). Hasan [44] proposed an approach to achieve more comprehensive security of e-learning systems in terms of management depending upon the target organization. In the proposed approach, the author evaluated the security requirements of e-learning applications as a basis for preparing security models. The case studies of security approaches of e-learning applications were used as a basis for modeling security requirements that ensure the control of access, privacy, and integrity. In the early stages of compiling, an information security model was used to conduct an agent-based environmental analysis on an e-learning platform, which revealed that the critical issues for MAS (Multi-Agent Services) security were trust, authority, and authentication. The proposed security model considers this aspect and combines it with the PMA3 platform.

Security is one of the major influencing factors in e-learning adoption in Jordan, as published in [22]. According to this study, information security has a significant impact on the learning success. The survey concluded that most e-learning participants have information security awareness, as they consider information security as a major e-learning success factor. Another exploratory study that recommended levels of authentication for e-learning activities was conducted by [45]. In response to previous research, this study explores the need to identify authentication levels that are specifically suitable for e-learning activities to prevent misuse. According to the descriptive statistical data collected, a certain set of e-learning activities exists, in which users feel that their identifying partners can potentially assume their identity. The results show that e-learning systems need to be authenticated even at the level of activities for summative e-assessment using appropriate authentication to secure the identity of remote users.

In an integrated e-learning system study conducted in Japan [46], information security was involved in the initial stage of development as one of the main factors. Numerous international students study in Japan, giving rise to diverse information ethics and cultures. Thus, information security education was considered highly important to ensure that these differences were accommodated. In the proposed system, the information security aspects were reflected in questionnaires related to topics such as copyright and personal information. The answers to the questions were collected and assigned priority values calculated from the learner's consciousness factor scores. Finally, the importance of each influencing factor was determined based on the priority values.

Furthermore, the drastic increase in the use of e-learning systems exacerbated the risks. Several academicians and practitioners have proposed ideas to address this problem. Giatman et al. [12] proposed a university framework for Online Learning Quality Control to guarantee the minimum standard of the learning process along with quality of the results. The framework covers the establishment of a Quality Control unit, preparation of the readiness of instructors and students, and settlement of quality assessment methods and materials. At the technical level, a cryptography mechanism to protect the CIA of an e-learning system environment was also proposed by [17]. However, cryptography alone is insufficient for this purpose. It must be combined with other techniques, such as firewalls, IDS, biometric authentication, security process models, and digital watermarking. A specific Distributed DOS (DDoS) model based on the characteristics of the e-learning system application was investigated by Vitic et al. [18]. The DDoS model considers the specifics of the operation of e-learning systems during the pandemic and can separate flash crowd events from outliers in the communication network.

Furthermore, the potential sources of disruption must be identified to protect e-learning system against them [37,47]. In this study, we elaborate on the potential disruptions from the perspective of LMS users based on their knowledge, awareness, and behavior related to LMS information security aspects. In addition, we attempt to validate hypotheses that correlate users' knowledge and awareness of information security, perceived information confidentiality, perceived data integrity, and perceived system availability with perceived LMS trustworthiness (called the User Perceived of LMS / UPoLMS model). Furthermore, we present the security event management (SEM) approach, which was the research framework adopted in [48,49]. The objective of this study is to provide recommendations for improving the information security aspects proposed to e-learning system administrators.

II. RESEARCH METHOD

A. Research Model and Hypothesis

Descriptive and comparative research methods were used to conduct the study. The research model was constructed based on the Technology Acceptance Model (TAM) using external variables that influence the user perception of information security aspects. The TAM is widely used to identify correlations between factors in descriptive or comparative research [9,48,50,51]. In our model, the proposed factors are categorized into two groups: the first group is user knowledge or experience of the LMS and the second is a user-perceived information security triad (the CIA triad). The proposed UPoLMS model is depicted in Fig. 1.

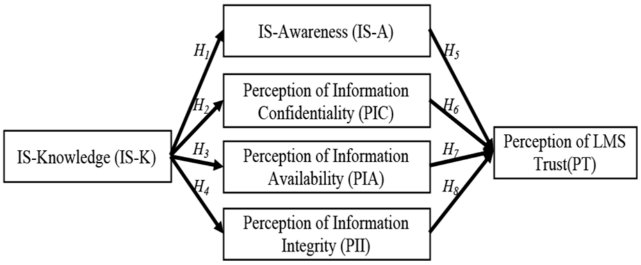

IS-Awareness (IS-A)
Perception of Information Confidentiality (PIC)
Perception of Information Availability (PIA)
Perception of Information Integrity (PII)
IS-Knowledge (IS-K)
Perception of LMS Trust(PT)
H1
H2
H3
H4
H5
H6
H7
H8

Fig. 1. The proposed UPoLMS model.

The proposed model is based on two initial assumptions: first, more experienced and more knowledgeable users will be more aware of information security-related aspects, and, second, the user's trust in an LMS is influenced by the performance of the LMS information security aspects as experienced by users. Information Security Knowledge (IS-K) and Information Security Awareness (IS-A) play dominant roles in securing the systems, information, or data contained within.

Several studies show that 70-80% of information security-related incidents occur due to negligence or unawareness of users [52]. IS-A is referred to as a state of consciousness about information security where the user ideally commits to the rules, recognizes potential risks, understands the importance of responsibilities, and acts accordingly [53-55]. User experience (UE), in this context, is the time spent by users on the LMS to perform learning activities. In this study, we treat UE as a part of IS-K because the components of UE are only measured by the time spent by the user using the LMS. PIC, PIA, and PII refer to the user perception of the information security triad, whereas the Perception of Trustworthiness (PT) refers to the user's acceptance or trust of the LMS.

To validate these two assumptions, we provide eight study hypotheses, as listed in Table 1. Each of the study hypotheses is validated with the statistical associative hypothesis, as described in Table 1. Thus, H_1 of the study is validated with statistical hypotheses $H_{1.0}$ and $H_{1.1}$, and so on for H_2-H_8.

Table 1. Research hypotheses

Hypothesis	Description
H_1	IS-K positively affects the user's IS-A
$H_{1.0}$	IS-K is not positively associate with the user's IS-A
$H_{1.1}$	IS-K is positively associate with the user's IS-A
H_2	IS-K positively affects the user's PIC
$H_{2.0}$	IS-K is not positively associate with the user's PIC
$H_{2.1}$	IS-K is positively associate with the user's PIC
H_3	IS-K positively affects the user's PIA
$H_{3.0}$	IS-K is not positively associate with the user's PIA
$H_{3.1}$	IS-K is positively associate with the user's PIA
H_4	IS-K positively affects the user's PII
$H_{4.0}$	IS-K is not positively associate with the user's PII
$H_{4.1}$	IS-K is positively associated with the user's PII
H_5	IS-A positively affects the users PT
$H_{5.0}$	IS-A is not positively associated with the user's PT
$H_{5.1}$	IS-A is positively associated with the user's PT
H_6	PIC positively affects the users PT
$H_{6.0}$	PIC is not positively associated with the user's PT
$H_{6.1}$	PIC is positively associated with the user's PT
H_7	PIA positively affects the user's PT
$H_{7.0}$	PIA is not positively associated with the user's PT
$H_{7.1}$	PIA is positively associated with the user's PT
H_8	PII positively affects the user's PT
$H_{8.0}$	PII is not positively associated with the user's PT
$H_{8.1}$	PII is positively associated with the user's PT

Overall, the study comprised the following stages: survey, statistical data analysis, comparison of results, and summarization. The survey was conducted during the early stage of the pandemic outbreak in Indonesia in 2020, and it was updated by a second survey in 2022. The feedback collection was performed using both the Google form application and hard copy, which were manually collected, whereas the data processing and analysis were performed using MS Excel and the SPSS application. The detailed steps of this study are shown in Fig. 2.

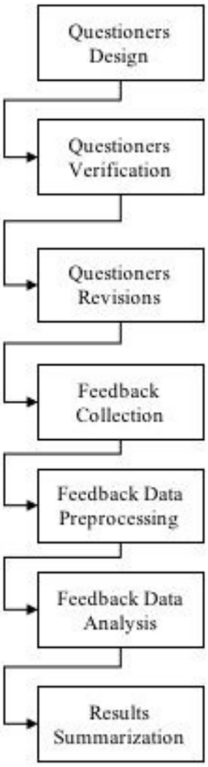


Fig. 2. The study stages

B. Survey Design and Respondents

The survey and questionnaires were designed on the basis of the model described above. Therefore, the questionnaires were divided into four groups. The first group of the questionnaires focused on general information about the respondent (gender, institution where they come from, what the most used LMS platform is, user role in the e-learning system, i.e., lecturer or student, department, and age), and the indication of their LMS experiences. The second group of questionnaires focused on the knowledge and experience of respondents in information security. The third group of questionnaires focused on the information security triad, and the last group assessed the perceived trustworthiness of the LMS. For all groups, we developed a collection of questionnaires with 44 questions; the number of questions in each category is presented in Table 2.

Students and lecturers are central to e-learning systems in terms of numbers and intensity of use. Other additional user roles, such as system administrators, process business owners, process business administrators, and management also exist. In the survey, we focused only on students and lecturers as respondents.

Table 2. Number of each questioner category questions

Questionnaires Category	#Quest.
IS-K: User's Information Security Knowledge (incl. User Experience)	15
IS-A: User's Information Security Awareness	7
PIC: User Perception of Information Security	7
PIA: User Perception of Information/Data availability	4
PII: User Perception of Information/Data Integrity	4
PT: User Perception of Trustiness to the LMS	7

We also developed open and closed questions. The open questions were mostly directed at collecting user comments and opinions regarding the LMS the respondents used. The closed questions were multiple-choice models with five answer choices ranging from "Strongly agree," "Agree," "Neutral," "Disagree," and "Strongly disagree." All questions were formulated to reflect a positive opinion. Thus, a higher Likert scale score given to a certain question indicates a better (more positive) response to the opinion represented by the question. A few of these questions are listed in Table 3.

Table 3. The samples of survey questions

Category	Question
IS-K	The e-learning system should maintain a balance between availability, confidentiality, and data integrity
IS-K	The e-learning password is the "I know" authentication factor
IS-A	I change my password periodically, retaining it for a maximum of 6 (six) months
IS-A	I always have backups of my e-learning data on my personal computer
PIC	The current state of the e-learning system does not allow unauthorized users to access module files
PIC	The current state of the e-learning system does not allow unauthorized users to access end user data
PII	The condition of the module file that I uploaded in e-learning was identical to that when it was downloaded by a student and to that on my computer
PIA	In the past semester / six months I have not experienced a failure in downloading student grades
PIA	In the last semester / six months I have not experienced a module upload failure
PT	The e-learning system has a good reputation in carrying out e-learning -based learning activities
PT	The e-learning system can guarantee the security of its information

C. Questionnaire Validation and Questionnaire Revisions

In the first round of surveys, we distributed questionnaires only to a limited number of users to validate the questionnaires and obtain feedback on quality. The purpose of the first survey round was to ensure that some quality parameters were achieved. These parameters are all questions that can be clearly understood; no bias or overlap is present in the questions, and which are grammatically correct.

D. Feedback Collection, Data Preprocessing, and Data Analysis

Two feedback collection mechanisms were employed: online and offline. Online feedback collection was performed using the Google form application, whereas offline collection was performed using the hard copy form distributed in the classrooms.

The main function of the data pre-processing stage was to provide clean and ready-to-process feedback data. Activities performed in this stage included the removal of user privacy information, data entry of offline feedback, and removal of invalid data. The main activity was converting users' answers on closed questions into scores on the Likert scale: "*Strongly agree*" (5), "*Agree*" (4), "*Neutral*" (3), "*Disagree*" (2), "*Strongly disagree*" (1).

The first task in the data analysis stage was feedback reliability validation testing. We used Cronbach's alpha validation tools to perform the testing, since it was the most popular [56]. The next data analysis task was correlation testing to validate each hypothesis, as presented in Table 1. We used the following linear correlation function:

$$\boldsymbol{Y} = \beta\mathbf{1} + \beta\mathbf{2X}, \qquad (1)$$

where Y is the average of the Likert scale values of the affected IS factor X is the average of the Likert scale values of the affected IS factor

For example, when applying the formula for H_1, Y is the average IS-A Likert scale value, X is the average of IS-K Likert scale value, In the case of H_2, Y is the average PIC Likert scale value, X is the average of IS-K Likert scale value, and so on for the remaining H_i, where i = 3,4,5,6,7,8.

III. RESULT AND DISCUSSION

A. Respondents Profile

We distributed the questionnaire in Google Form format through messaging systems and social media platforms such as WhatsApp, Facebook, Instagram, and Twitter. A total of 1033 respondents from various institutions spread across the globe were surveyed. Since the Google Form questionnaires were openly distributed through various media, all user ranging from lecturers and students to industry practitioners and government staff were part of the survey. Most of the respondents are affiliated to universities followed by members of the government and private sector. Meanwhile, Moodle and Google Classroom were the two most used LMSs. In

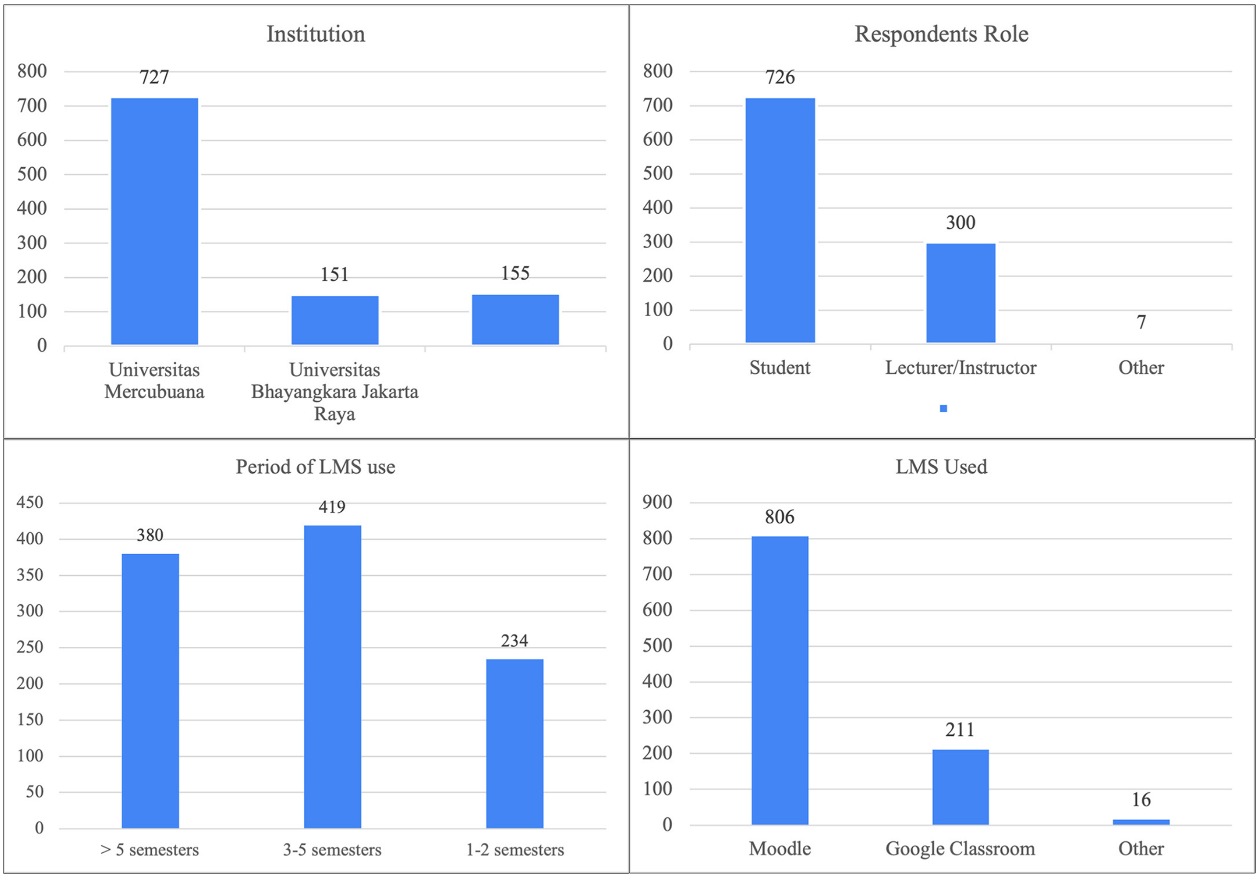


Fig. 3. The respondent profile.

addition, the global summary of respondent profiles is shown in Fig. 3, which presents the institutions, respondents' roles, LMS used, and time spent on the LMS. In the analysis of the feedback results, Moodle and Google Classroom were selected as the representative LMS platforms, and lecturers and students as the representative users. Thus, we present four categories of analysis: The Moodle LMS Information Security aspect from the instructor's perception, Moodle LMS Information Security aspect from students' perception, Google Classroom Information Security aspect from instructor's perception, and Google Classroom Information Security aspect from students' perceptions.

B. Reliability Validation

The overall reliability validation testing of the sample using an Cronbach's alpha variable is presented in Table 4. Cronbach's alpha coefficient justifies factors as reliable if their value is 0.70 or greater [57,58]. The Cronbach's value of each factor (variable) for each user role and LMS platform, as presented in Table 4, varies from 0.35 0.98. A few of the Cronbach alpha values are less than 0.70, which indicates that the factor is unreliable. Accordingly, we ignore the corresponding factors in the subsequent stage of analysis The unreliable factors are: the IS-A factor of lecturers on Google Classroom, P-II factor of lecturers on Google Classroom, IS-A factor of lecturers on Moodle, and P-II factor of students on Moodle, which have, which have Cronbach values of 0.35, 0.42, 0.67, and 0.68, respectively.

Table 4. The Cronbach alpha value

	UE-ISK	IS-A	P-IC	P-II	P-IA	PT
Student-Moodle	0.84	0.76	0.94	0.68	0.86	0.93
Student-Google Classroom	0.87	0.93	0.98	0.72	0.90	0.94
Lecturer-Moodle	0.85	0.67	0.95	0.72	0.95	0.94
Lecturer-Google Classroom	0.77	0.35	0.90	0.42	0.81	0.86

C. Hypothesis Analysis

To validate our hypothesis, we applied the linear regression model presented in Section 3. In this section, we elaborate on the analysis of each category based on the dominant respondent role.

Table 5. The student hypothesis analysis result

Hypothesis	Description	Moodle				Google CR			
		β1	β2	P-val	Results	β1	β2	P-val	Results
$H_{1.0}$	IS-K->ISA	2.1125	0.2941	0.0000	reject $H_{1.0}$	-1.3629	1.2233	0.0000	reject $H_{1.0}$
$H_{2.0}$	IS-K->PIC	2.2204	0.2660	0.0000	reject $H_{2.0}$	-0.9815	1.1502	0.0000	reject $H_{2.0}$
$H_{3.0}$	IS-K->PIA	2.3234	0.3683	0.0000	reject $H_{3.0}$	1.5105	0.6653	0.0000	reject $H_{3.0}$
$H_{4.0}$	IS-K->PII*	3.0917	0.2567	0.0000	N/A due to Cronbach alpha	1.6713	0.6465	0.0000	Reject $H4_{.0}$
$H_{5.0}$	IS-A->PT	3.1475	0.6332	0.0000	reject $H_{5.0}$	1.7723	0.6452	0.0000	reject $H_{5.0}$
$H_{6.0}$	PIC->PT	3.1475	0.1603	0.0001	reject $H_{6.0}$	2.4191	0.4943	0.0000	reject $H_{6.0}$
$H_{7.0}$	PIA->PT	1.8714	0.4774	0.0000	reject $H_{7.0}$	1.7549	0.6153	0.0000	reject $H_{7.0}$
$H_{8.0}$	PII->PT*	0.6155	0.7453	0.0000	N/A due to Cronbach alpha	-0.0666	0.9919	0.0000	reject $H8_{.0}$

1) Student Respondents

Table 5 presents the overall hypothesis analysis of the student-Moodle and Google Classroom UPoLMS model. As presented on the left side of Table 5, seven out of eight $H_{x.0}$ hypothesis of the student-Moodle UPoLMS are contradicted by the questionnaire's feedback data; therefore, all $H_{x.0}$ are rejected and $H_{x.1}$ are accepted. The results indicate that IS-K influences IS-A (*β2 = 0.2941, P-value = 0.000)*, PIC (*β2 = 0.26600, P-value = 0.000*), PIA *(β2=0.3683, P-value = 0.000*), and PII (*β2 = 0.2567, P-value = 0.000)* factors, respectively. The last three rows, except for PII that is ignored, indicate that PT factors are consistently influenced by IS-A, PIC, and PI-A, as shown by the *β2 coefficient* and *P-value*. For, IS-A, *β2 = 0.6332,* and *P-value = 0.0000*; for PIC, *β2 = 0.0163,* and *P-value = 0.000*; and for PIA, *β2 = 0.4774*, and *P-value = 0.0000.* Based on the results of the data correlation analysis, the Moodle students' UPoLMS model was revised, as shown in Fig. 4.

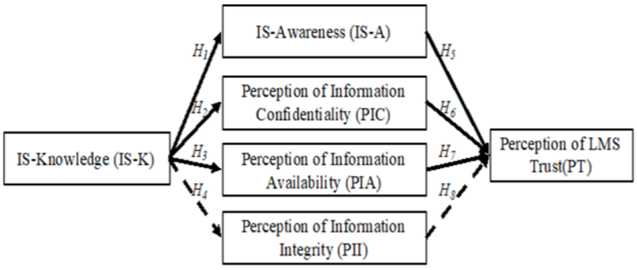

IS-Awareness (IS-A)
Perception of Information Confidentiality (PIC)
Perception of Information Availability (PIA)
Perception of Information Integrity (PII)
IS-Knowledge (IS-K)
Perception of LMS Trust(PT)
H1
H2
H3
H4
H5
H6
H7
H8

Fig. 4. The revised student-Moodle UPoLMS model

The results of Cronbach's analysis of the student-Google Classroom differed slightly from the Moodle results, as shown in Table 4. We can use all the model factors of Google Classroom to perform further hypothesis validation of the student-Google Classroom UPoLMS. Overall, seven out of 8 $H_{x.0}$ *hypotheses* (since we ignore the PII factor) are contradicted by the questionnaire's feedback data; therefore, all $H_{x.0}$ are rejected and $H_{x.1}$ *are* accepted. The results indicate that IS-K influences IS-A (*β2 = 1.2233, P-value = 0.000*), PIC (*b2 = 1.1502, P-value = 0.000*), and PIA (*β2 = 0.6683, P-value = 0.000*). The last four rows of data of *β2 coefficient* and *P-value* confirm that PT factors are consistently influenced by IS-A, PIC, PI-A, and PII, as well as by their positive *β2 coefficient* and zero *P-Value.* Based on the correlation data results, the UPoLMS student-Google Classroom model matches the proposed model, as depicted in Fig. 3. Therefore, the proposed model does not require modification.

2) Lecturer Respondents

A hypothesis analysis of the lecturer UPoLMS model is presented in Table 6. The IS-A factor was ignored in the hypothesis analysis stage because its Cronbach's value was under 0.7. Based on the P-value of each factor, which is above 0.05 for both Moodle and Google Classroom LMS, most of the Hx.0 hypotheses are accepted. The exceptions are the PIA and PII factors for Moodle, which influence the PT factor. The hypothesis analysis results reveal that the lecturers' Information Security Knowledge and the Information Security triad are not correlated. However, the perception of trustworthiness in both Moodle and Google Classroom is influenced only by the perception of information availability and integrity.

3) Lecturer - Student Analysis:

In this stage, we investigate whether the characteristics of perception of Information Security differ significantly between lecturers and students. The samples collected included 726 students and 300 lecturers/instructors; thus, based on this number of samples, we can assume that the sampling is normally distributed. Accordingly, we conducted a t-test validation as an independent sample test tool to determine the differences in perception of information security factors. The proposed hypothesis of the test is as follows:

H_0: $\mu_1 \leq \mu_2$ (lecturer's rating of Information Security is less than or equal to that of the student)

H_1: $\mu_1 > \mu_2$ (lecturer's rating of Information Security is better than that of the student)

Table 6. The student hypothesis analysis result

Hypothesis	Description	Moodle				Google CR			
		β1	β2	P-val	Results	β1	β2	P-val	Results
$H_{1.0}$	IS-K->ISA*	3.2283	-0.0013	0.9761	N/A due to Cronbach alpha	1.8776	0.0968	0.3757	N/A due to Cronbach alpha
$H_{2.0}$	IS-K->PIC	3.5590	-0.0227	0.7695	accept $H_{2.0}$	1.3858	-0.0864	0.5466	accept $H_{2.0}$
$H_{3.0}$	IS-K->PIA	3.3155	0.1135	0.1840	accept $H_{3.0}$	1.7601	0.0021	0.5494	accept $H_{3.0}$
$H_{4.0}$	IS-K->PII	3.7406	0.0550	0.3434	accept $H4_{.0}$	3.2627	-0.1460	0.2416	accept $H4_{.0}$
$H_{5.0}$	IS-A->PT	3.7952	0.0273	0.7855	accept $H_{5.0}$	4.5633	-0.3320	0.1146	accept $H_{5.0}$
$H_{6.0}$	PIC->PT	3.9885	-0.0304	0.5941	accept $H_{6.0}$	4.9183	-0.1966	0.0113	accept $\mathrm{H}_{6.0}$
$H_{7.0}$	PIA->PT	2.4956	0.3674	0.0000	reject $H_{7.0}$	4.8593	-0.2131	0.0248	accept $\mathrm{H}_{7.0}$
$H_{8.0}$	PII->PT	1.5109	0.5984	0.0000	reject $H_{8.0}$	3.5973	-0.0287	0.3175	accept $\mathrm{H8}_{.0}$

The t-test results, using a = 0.05, are presented in Table 7, which shows a significant difference between lecturers and students in their perception of the Moodle and Google Classroom information security factors. In the case of Moodle, for four of the six factors t-stat > t-critical one-tile, whereas for the remaining two factors present t-stat < t-critical one tile. Thus, for the four factors, as H_0 is rejected and H_1 is accepted, the lecturer perception of information security in Moodle is better than the student perception. Conversely, in the Google Classroom t-test, for five of the six t-test factors, t-stat < t-critical one tile, indicating that the confidence level of students is better than that of lecturers. In contrast, the PII and PT factors exhibit similar perception patterns for both Moodle and Google Classroom. In the PII factor for both Moodle and Google Classroom, the students' perception is better than that of the lecturers, whereas for the PT factor, the lecturer's perception is better than the student's perception.

The next analysis was performed to determine the level of user perception of the information security aspect. As described in Section 3.3, all questions were formulated as positive opinions. In other words, a higher value of the user's answer, represents a more positive perception. Here, we employed mean value analysis by comparing the mean value to 3.5 as the minimum threshold of good perception. Fig. 5 depicts the chart of the Likert scale mean of the information security-related perception factors of lecturers and students for (a) Moodle and (b) Google Classroom. These charts show the different information security-related perceptions of lecturers and students. For Moodle, the results indicate that, in general, lecturers have more positive perceptions compared with students, whereas the converse is true for Google Classroom, for which students have better perceptions.

On comparing the two LMSs, both lecturers and students are seen to have a better perception of Google Classroom, which could be attributed to the fact that Google Classroom services are provided by a mature company, whereas Moodle is managed independently, which results in different management standards depending upon the institutions. These standards lead to different levels of service. However, further investigation is required to validate this assumption. Overall, both user roles have a positive perception of the two LMSs, as indicated by the average level of perception above the threshold of 3.5. Table 8 shows the detailed results of the Likert-scale mean level presented with the variance of each factor. As shown in the Table, in general, the perception level is above the threshold. However, the perception level of both user roles is below the threshold for IS-A and PIC. In particular, information security awareness needs to receive more attention for Moodle and Google Classroom because both lecturer and student perceptions of this factor are below the threshold. Meanwhile, for Google Classroom, only the perception of the lecturers is below the threshold.

Table 7. Correlation analysis of lecturer UPoLMS model

Factors	Moodle		Google Classroom	
	t Stat	t Critical one-tail	t Stat	t Critical one-tail
IS-K: User's Information Security Knowledge (1)	2.1534	1.6484	-5.4962	1.6606
IS-A: User's Information Security Awareness (2)	1.9821	1.6483	-12.3654	1.6522
PIC: User Perception of Information Security (3)	3.3472	1.6492	-6.5524	1.6561
PIA: User Perception of Information/Data Availability (4)	0.1068	1.6493	-5.9765	1.6587
PII: User Perception of Information/Data Integrity (5)	-3.0639	1.6496	-6.8155	1.6583
PT: User Perception of Trustiness to LMS (6)	3.9142	1.6486	6.0757	1.6524

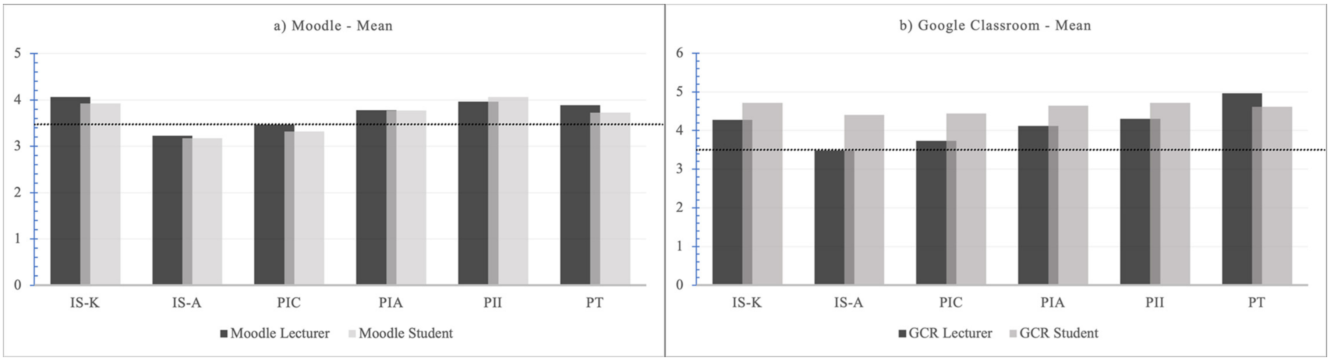


Fig. 5. Likert scale mean of information security related factors.

Table 8. Likert scale mean - variance of information security related factors

Factors	Moodle		Google Classroom	
	Mean	Variance	Mean	Variance
IS-K: User's Information Security Knowledge (1)				
Lecture	4.0628	0.4897	4.2768	0.2784
Student	3.9264	0.5882	4.7156	0.2343
Difference	0.1364	-0.0985	-0.4387	0.0441
IS-A: User's Information Security Awareness (2)				
Lecture	3.2229	0.2170	3.4891	0.0925
Student	3.1693	0.2530	4.4057	0.5811
Difference	0.0537	-0.0359	-0.9166	-0.4886
PIC: User Perception of Information Security (3)				
Lecture	3.4669	0.6696	3.7337	0.4110
Student	3.3183	0.5303	4.4425	0.6881
Difference	0.1486	0.1392	-0.7089	-0.2770
PIA: User Perception of Information/Data Availability (4)				
Lecture	3.7766	0.8197	4.1186	0.3174
Student	3.7714	0.6236	4.6480	0.3534
Difference	0.0052	0.1961	-0.5294	-0.0360
PII: User Perception of Information/Data Integrity (5)				
Lecture	3.9639	0.3772	4.3023	0.1492
Student	4.0637	0.2538	4.7200	0.1764
Difference	-0.0998	0.1234	-0.4177	-0.0272
PT: User Perception of Trustiness to LMS (6)				
Lecture	3.8831	0.4984	4.9661	0.0666
Student	3.7270	0.5057	4.6150	0.3264
Difference	0.1561	-0.0073	0.3511	-0.2597

In practice, the results of user perceptions of these LMSes can be considered for institutions that use Moodle or Google Classroom. Based on the perception and differences between lecturers and students, institutions need to customize their LMS information security policies separately, according to the needs of lecturers and students.

IV. CONCLUSION

In this study, we investigated the perception of two dominant user roles, lecturer and student, of LMS Information Security factors. We proposed a model of user perception for Moodle and Google Classroom LMSs (UPoLMS) based on information security-related aspects. The model was then validated using statistical testing tools with input data collected from feedback surveys.

According to the feedback from respondents, statistical testing was applied to the defined factors. The results show that lecturers and students perceive information security aspects of LMSs differently. In the case of students, user knowledge of information security influences the user perception, which, in turn, influences the user perception of trustworthiness of both Moodle and Google Classroom. Conversely, in the case of lecturers, information security knowledge and information security-related perceptions do not affect the perception of trustworthiness of an LMS. Only the PI-A and PII factors affect user perception of trustworthiness of Moodle among lecturers.

Based on the Likert scale threshold, which represents an adequate IS user perception, lecturers and students have significantly different perceptions of Moodle and Google Classroom. Lecturers have a better perception of Moodle, whereas students have a better perception of Google Classroom. In any case, both user roles have a relatively good perception of the information security factors of the two LMSs, as indicated by their Likert scales, which are all above 3.5. However, both the lecturer and student users have a better perception of the information security offered by Google Classroom, compared to Moodle LMS.

The lack of information security awareness has the potential to expose organizations to security risk. Moreover, the majority of information security-related incidents can be attributed to negligence or a lack of awareness on the part of users [52]. Considering that the results of this study indicate a general lack of awareness, institutions that use Moodle, in particular, need to conduct information security awareness programs such as trainings and social events to emphasize the importance of information security and the leadership's commitment to comply with information security governance. We also recommend that institutions implement different information security programs depending on user characteristics and the LMS (Moodle or Google Classroom) used.

Despite in general the objectives of this study were achieved; this study revealed several drawbacks in the results of the study. One of the drawbacks is that the large number of respondent data is invalid when tested with Cronbach's alpha analysis, causing the UPoLMS mode to be revised. Because of the revision, we were unable to elaborate on the relationship between some of the TAM model factors.

This study does not explore synchronous online learning models that can be integrated with Moodle or Google Classroom as LMS objects under study, such as Google Meet for Google Classroom and Big Blue Button for Moodle LMS. In future studies, apart from working on improving data collection techniques to improve data quality, we will elaborate on the information security aspects of the synchronous model. Several problem formulations related to this research include the ease of integration with LMS (integrity aspect), how stable synchronous applications are when integrated with LMS (availability aspect), and how authentication and authority are managed (confidential aspect).

APPENDIX

N/A

ACKNOWLEDGMENTS

The authors would like to thank LPPM Universitas Bhayangkara Jakarta Raya, who supported this research through research funding contract No.: PK/ 16 / IV /LPPMP-UBJ/PENELITIAN/2022.

REFERENCES

[1] M. Sadikin and S. K. Purwanto, “The implementation of e-Learning system governance to deal with user need , institution objective , and regulation compliance,” *Telecommunication Computing Electronics and Control,* vol. 16, no. 3, pp. 1332-1344, Jun. 2018. DOI: 10.12928/telkomnika.v16i3.8699.

[2] M. Sadikin and S. Purwanto, “To govern e-learning system: A proposal to deal with regulation complience, institution objective and user need,” in *83rd ISERD International Conference*, Barcelona, Spain, pp. 33-38. 2017. [Online]. Available: http://www.worldresearchlibrary.org/up_proc/pdf/1021-150536458933-38.pdf.

[3] N. R. Maulana and A. P. Lintangsari, “The use of Moodle in English language learning during the pandemic: The students voice,” *The Journal of English Literacy Education*, vol. 8, no. 1, pp. 27-41, May 2021. DOI: 10.36706/jele.v8i1.14020.

[4] R. Quansah and C. Essiam, “The Use of Learning Management System (LMS) Moodle in the midst of Covid-19 Pandemic: Students’ perspective,” *Journal of Educational Technology and Online Learning*, vol. 4, no. 3, pp. 418-431, Sep. 2021. DOI: 10.31681/jetol.934730.

[5] Sukmawati, “Implementasi pemanfaatan Google Classroom dalam proses pembelajaran online di era industri 4.0,” *Jurnal Kreatif Online*, vol. 8, no. 1, 2020.

[6] R. Atikah, R. T. Prihatin Titik, H. Hernayati, and J. Misbah, “Pemanfaatan google classroom sebagai media pembelajaran di masa pandemi covid-19,” *Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, vol. 7, no. 1, pp. 7-18, Mar. 2021. DOI: 10.31980/jpetik.v7i1. 988.

[7] B. Kwofie and A. Henten, “The advantages and challenges of e-learning implementation:The story of a developing nation,” in *3rd World Conference on Educational Science*, Istabul, Turkey, 2011. [Online] Available: https://vbn.aau.dk/en/publications/the-advantages-and-challenges-of-e-learning-implementation-the-st.

[8] M. M. Alkharang and G. Ghinea, “E-learning in higher educational institutions in Kuwait: Experiences and challenges,” *International Journal of Advanced Computer Science and Application.*, vol. 4, no.

4, pp. 1-6, Apr. 2013. DOI: 10.14569/IJACSA.2013.040401.

[9] W. M. Al-Rahmi, N. Yahaya, A. A. Aldraiweesh, M. M. Alamri, N. A. Aljarboa, U. Alturki, and A. A. Aljeraiwi, “Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students’ intention to use e-learning systems,” *IEEE Access*, vol. 7, pp. 26797-26809, Feb. 2019. DOI: 10.1109/ACCESS.2019.2899368.

[10] A. Purwanto, “University students online learning system during Covid-19 pandemic: Advantages, constraints and solutions,” *Systematic Reviews in Pharmacy*, vol. 11, no. 7, pp. 570-576, 2020. DOI: 10.31838/srp.2020.7.81.

[11] M. P. A. Murphy, “COVID-19 and emergency eLearning: Consequences of the securitization of higher education for post-pandemic pedagogy,” *Contemporary Security Policy*, vol. 41, no. 3, pp. 492-505, Apr. 2020. DOI: 10.1080/13523260.2020.1761749.

[12] M. Giatman, S. Siswati, and I. Y. Basri, “Online learning quality control in the pandemic covid-19 era in Indonesia,” *Journal of Nonformal Education*, vol. 6, no. 2, pp. 168-175, Aug. 2020. [Online]. Available: https://journal.unnes.ac.id/nju/index.php/jne/article/view/25594.

[13] M. Hafeez, Q. A. Kazmi, and F. Tahira, “Challenges faced by the teachers and students in online learning during covid-19,” *Journal Cakrawala Pendidikan*, vol. 41, no. 1, pp. 55-70, Feb. 2022. DOI: 10.21831/cp.v41i1.35411.

[14] N. Islam, M. Beer, and F. Slack, “E-Learning challenges faced by academics in higher education: A literature review,” *Journal of Education and Training Studies*, vol. 3, no. 5, pp. 102-112, Jul. 2015. DOI: 10.11114/jets.v3i5.947.

[15] M. V. Zharova, S. Y. Trapitsin, V. V. Timchenko, and A. I. Skurihina, “Problems and opportunities of using LMS moodle before and during COVID-19 quarantine: Opinion of teachers and students,” in *Proceedings of the 2020 International Conference Quality Management, Transport and Information Security, Information Technologies*, Yaroslavl, Russia, pp. 554-557, 2020. DOI: 10.1109/ITQMIS51053.2020.9322906.

[16] F. Shersad and S. Salam, “Managing risks of E-learning during COVID-19,” *International Journal of Innovation and Research in Educational Science*, vol. 7, no. 4, pp. 348-358, Jul. 2020. [Online]. Available: https://www.ijires.org/index.php/issues?view=publication&task=show&id=593

[17] L. C. R. Salvador, C. L. A. Llerena, and H. P. Dai Nguyen, “Digital education: Security challenges and best practice,” *Security Science Journal*, vol. 2, no. 2, pp. 65-76, Dec. 2021. DOI: 10.37458/ssj.2.2.4.

[18] I. Cvitić, D. Peraković, M. Periša, and A. D. Jurcut, “Methodology for detecting cyber intrusions in e-learning systems during COVID-19 pandemic,” *Mobile Networks and Applications*, Jun. 2021. DOI: 10.1007/s11036-021-01789-3.

[19] Unesco, “UNESCO’s Covid-19 education response: Distance learning solution,” 2020. [Online] Available: https://webarchive.unesco.org/web/20221007040001/https:/en.unesco.org/covid19/educationresponse/solutions.

[20] W. Fenton, “The Best LMS (Learning Management Systems) of 2017 | PCMag.com,” 2017. [Online] Available: https://www.pcmag.com/roundup/336308/the-best-lms-learning-management-systems.

[21] J. T. Nagy, “Using learning management systems in business and economics studies in Hungarian higher education,” *Education and Information Technologies*, vol. 21, no. 4, pp. 897-917, Jul. 2016. DOI: 10.1007/s10639-014-9360-6.

[22] M. Shkoukani, “Explore the major characteristics of learning management systems and their impact on e-learning success,” *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 1, pp. 296-301, 2019. DOI: 10.14569/ijacsa.2019.0100139.

[23] B. Warin, O. Talbi, C. Kolski, and F. Hoogstoel, “Multi-Role Project (MRP): A new project-based learning method for STEM,” *IEEE Transactions on Education.*, vol. 59, no. 2, pp. 137-146, May. 2016. DOI: 10.1109/TE.2015.2462809.

[24] R. K. Kampa and P. Kaushik, “Integrating the Library within the Moodle Learning Managament system: A case study,” *Journal of Library & Information Science*, vol. 6, no. 4, pp. 702-710, Dec. 2016. [Online]. Available: http://irjlis.com/integrating-the-library-within-the-moodle-learning-management-system-a-case-study/.

[25] M. Sadikin, R. Yusuf, and A. R. Dwiyanto, “Load balancing clustering on Moodle LMS to overcome performance issue of e-learning system,” *Journal of Telecommunication Computing Electronics and Control*, vol. 17, no. 1, pp. 131-138, Feb. 2019. DOI: 10.12928/telkomnika.v17i1.10284.

[26] M. Hossain, “Unequal experience of COVID-induced remote schooling in four developing countries,” *International Journal of Educational Development*, vol. 85, pp. 102446, Sep. 2021. DOI: 10.1016/j.ijedudev.2021.102446.

[27] M. Jebbour, “The unexpected transition to distance learning at Moroccan universities amid COVID-19 : A qualitative study on faculty experience,” *Social Sciences & Humanities Open*, vol. 5, no. 1, pp. 100253, 2022. DOI: 10.1016/j.ssaho.2022.100253.

[28] R. M. Saidi, A. A. Sharip, N. Z. Abd Rahim, Z. A. Zulkifli, and S. M. M. Zain, “Evaluating students’ preferences of Open and Distance Learning (ODL) tools,” *Procedia Computer Science.*, vol. 179, pp. 955-961, 2021. DOI: 10.1016/j.procs.2021.01.085.

[29] S. M. Saha. S. A. Pranty, M. J. Rana, M. J. Islam, and M. E. Hossain, “Teaching during a pandemic : Do university teachers prefer online teaching ?,” *Heliyon*, vol. 8, no. 1, p. e08663, Jan. 2022. DOI: 10.1016/j.heliyon.2021.e08663.

[30] A. Q. Noori, “The impact of COVID-19 pandemic on students’ learning in higher education in Afghanistan,” *Heliyon*, vol. 7, no. 10, p. e08113, Oct. 2021. DOI: 10.1016/j.heliyon.2021.e08113.

[31] S. A. Naroo, P. B. Morgan, L. Shinde, and A. Ewbank, “The impact of COVID-19 on global contact lens education,” *Journal of Optometry.*, vol. 15, no. 1, pp. 60-68, Jan. 2022. DOI: 10.1016/j.optom.2020.11.002.

[32] S. Yani, “Pemamfaatan E-Learning Berbasis Google Classroom Sebagai Media Pembelajaran Pada Masa Pandemic Covid-19,” *Prosiding Seminar Nasinal.*, vol. 1, no. 1, 2021.

[33] H. S. Su’uga, E. Ismayati, A. I. Agung, and T. Rijanto, “Media e-learning berbasis Google Classroom untuk meningkatkan hasil belajar siswa SMK,” *Jurnal Pendidikan Teknik Elektro*, vol. 9, no. 3, pp. 605-610, Sep. 2020. [Online] Available: https://ejournal.unesa.ac.id/index.php/jurnal-pendidikan-teknik-elektro/article/view/36253.

[34] S. Soni, A. Hafid, R. Hayami, Y. Fatma, and F. A. Wenando, J. A. Amien, E. Fuad, M. Unik, H. Mukhtar, H. Hasanuddin, “Optimalisasi pemanfaatan google classroom sebagai media pembelajaran di SMK NEGERI 1 Bangkinang,” *Jurnal Pengabdian Untuk Mu negeRI*, vol. 2, no. 1, pp. 17-20, 2018. DOI: 10.37859/jpumri.v2i1.361.

[35] M. Button, R. Klahr, J. N. Shah, P. Sheriffs, T. Rossington, G. Pestell, and V. Wang, “Cyber Security Breaches Survey 2016,” *Department for Digital Culture Media and Sport*, 2018. DOI: 10.13140/RG.2.1.4332.6324.

[36] “Electronic Record Systems and Individual Privacy,” *Computers & Security*, vol. 5, no. 4 pp. 361-362, Dec. 1986. DOI: 10.1016/0167-4048(86)90061-1.

[37] N. Sakiba, “Security challenges for e-learning ecosystems,” Norwegian University of Secience and Technology, 2017. [Online] Available: https://www.researchgate.net/publication/319130727_

Security_challenges_for_e-learning_ecosystems

[38] H. W. Glaspie and W. Karwowski, "Human Factors in Information Security Culture: A Literarture Review," *Advances in Intelligent Systems and Computing,* vol. 593, pp. 269-280, 2017. DOI: 10.1007/978-3-319-60585-2_25.

[39] M. Dark, R. Epstein, L. Morales, T. Countermine, Q. Yuan, M. Ali, M. Rose, and N. Harter, "A Framework for Information Security Ethics Education," in *Proceedings of the 10th Colloquium for Information Systems Security Education*, vol. 4, pp. 109-115, 2006.

[40] ISACA, "Audit/Assurance," 2014. http://www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/Pages/Audit-Assurance-Programs.aspx.

[41] ISACA, *CGEIT Review Manual*, 7th ed. Rolling Meadow, IL, USA: ISACA, 2017. [Online] Available: www.isaca.org.

[42] W. Q. Qwaider, "Information Security and Learning Content Management System (LCMS)," *International Journal of Advanced Computer Science and Applications,* vol. 8, no. 11, pp. 588-593, 2017. DOI: 10.14569/IJACSA.2017.081174.

[43] N. A. Lavanya, M. Buvana, and D. Shanthi, "Detection of Security Threats and Vulnerabilities of E-Learning Systems In Cloud Computing," *Advances in Natural and Applied Sciences*, vol. 11, no. 7, pp. 550-559, May. 2017.

[44] S. H. Hasan, D. M. Alghazzawi, and A. Zafar, "E-Learning Systems and their Security," *MAGNT Research Report*, vol. 2, no. 3, pp. 83-92, 2016. DOI: 14.9831/0971-9563.2014/2-3/BRIS.10.

[45] S. Beaudin, "An empirical study of authentication methods to secure e-learning system activities against impersonation fraud," Ph. D. dissertation, Nova Southeastern University, vol. 4, no. 1, pp. 42-61, 2016. DOI: 10.36965/OJAKM.2016.4(1)42-61.

[46] K. Nagata, Y. Kigawa, and T. Aoki, "Trial for e-learning system on information security incorporate with learning style and consciousness factors," *International Journal of Engineering Pedagogy*, vol. 8, no. 3, pp. 120-136, May. 2018. DOI: 10.3991/ijep.v8i3.8163.

[47] Piyushika and K. N. Singh, "Review of cloud security for e-Learning system," *International Journal of Computer Science and Technology.*, vol. 6, no. 2, pp. 85-89, Jan. 2015. [Online] Available: https://www.researchgate.net/publication/281096002_Review_of_Cloud_Security_for_E-Learning_System.

[48] F. Kanwal and M. Rehman, "Factors affecting e-learning adoption in developing dountries - Empirical evidence from Pakistan's higher education sector," *IEEE Access*, vol. 5, pp. 10968-10978, 2017. DOI: 10.1109/ACCESS.2017.2714379.

[49] J. C. Roca, J. J. García, and J. J. de la Vega, "The importance of perceived trust, security and privacy in online trading systems," *Informtion Management Computer Security*, vol. 17, no. 2, pp. 96-113, Jun. 2009. DOI: 10.1108/09685220910963983.

[50] Y. H. Lee, Y. C. Hsieh, and C. N. Hsu, "Adding innovation diffusion theory to the technology acceptance model: Supporting employees' intentions to use e-learning systems," *Educational Technology and Society*, vol. 14, no. 4, pp. 124-137, 2011. [Online]. Available: https://eric.ed.gov/?id=EJ963285

[51] S. Asiyah, C. W. Budiyanto, and A. G. Tamrin, "Technology acceptance model in the analysis of the influence of e-learning implementation to students' motivation," *Indonesian Journal of Informatics Education*, vol. 2, no. 1, pp. 55-60, Jun. 2018. DOI: 10.20961/ijie.v2i1.14496.

[52] Y. K. Mittal, S. Roy, and M. Saxena, "Role of knowledge management in enhancing information security," *International Journal of Computer Science Issues*, vol. 7, no. 6, pp. 320-324, Nov. 2010. [Online] Available: https://www.ijcsi.org/papers/7-6-320-324.pdf.

[53] A. R. Ahlan, M. Lubis, and A. R. Lubis, "Information security awareness at the knowledge-based institution: Its antecedents and measures," in *The Third Information Systems International Conference*, vol. 72, pp. 361-373, 2015. DOI: 10.1016/j.procs.2015.12.151.

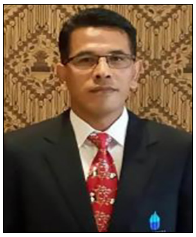
[54] F. J. Haeussinger and J. Kranz, "Information security awareness: Its antecedents and mediating effects on security compliant behavior," in *34th International Conference on Information System*, Milan, Italy, pp. 1-16, 2013. [Online] Available: https://www. researchgate.net/publication/258926834_Information_Security_Awareness_Its_Antecedents_and_Mediating_Effects_on_Security_Compliant_Behavior.

[55] T. Gundu and S. V. Flowerday, "Ignorance to awareness: Towards an information security awareness process," *SSAIEE Africa Research Journal.*, vol. 104, no. 2, pp. 69-79, Jun. 2013. DOI: 10.23919/SAIEE.2013.8531867.

[56] D. G. Bonett and T. A. Wright, "Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning," *Journal of Organizational Behavior*, vol. 36, no. 1, pp. 3-15, Jan. 2015. DOI: 10.1002/job.1960.

[57] J. C. Nunnally and I. H. Bernstein, "Psychometric Theory" Third. New York, USA: McGraw-Hill, New York, 1994.

[58] M. Saunders, P. Lewis, and A. Thornhill, "Research Methods for Business Students," *4th edition Pearson Education Limited,* England, vol. 6, no. 3, 2008.



Mujiono Sadikin

was born in 1970, in Magetan, East Java, Indonesia. He acquired his Bachelor's degree in Informatics and Magister's degree in Informatics from Bandung Institute of Technology, followed by a doctoral degree in Computer Science from Universitas Indonesia, Jakarta in 2017. He currently serves as a member of the Faculty of Computer Science Universitas Bhayangkara Jakarta Raya and IT Director of the University. His area of research includes AI, Machine Learning, and IT Governance. The focus of his publications are mainly machine learning and e-Learning. He can be contacted via email: mujiono@dsn.ubharajaya.ac.id.

Rakhmat Purnomo

He holds a master's degree in computer science from STMIK Nusa Mandiri Jakarta, Indonesia for his thesis "Application of Greedy Forward Selection and Bagging in Logistic Regression for Software Defects Prediction". His research interests include Software engineering, Data Mining, Networking, and e-Learning. He currently serves as a tenured lecturer at the Department of Informatics, Universitas Bhayangkara Jakarta Raya. He can be contacted via email: rakhmat.purnomo@dsn.ubharajaya.ac.id.

Rafika Sari

She received her Magister's degree in computational science from the Mathematics and Natural Science Institut Teknologi Bandung (ITB), West Java, Indonesia. She currently serves as a member of the Computer Science Faculty at Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia. Her research interests include computational science, machine learning, data science and artificial intelligence. She is also a member of the Indonesian Computational Society, Asosiasi Profesi Perguruan Tinggi Ilmu Komputer (APTIKOM), Asosiasi Ilmuwan Data Indonesia (AIDI), and Relawan Jurnal Indonesia (RJI).

Dyah Ayu Nabilla Ariswanto

Dyah Ayu was born in Jakarta, Indonesia in 1997. She is currently enrolled in a doctoral program in Business at IPB University, Bogor, Indonesia. She holds a bachelor's degree in business from Prasetiya Mulya University, Jakarta, Indonesia, and a master's degree in marketing management from Universitas Indonesia, Jakarta, Indonesia. Her specialization and interests lie in the Business and Marketing fields.

Juanda Wijaya

He was born in Jakarta in 1978. He holds a master's degree in Telecommunication technology from Mercu Buana University Jakarta. His area of research includes mobile network and transmission technology. He can be contacted via email: juanda.wijaya@mercubuana.ac.id

Lydia Vintari

She holds a BS degree in Electro Engineering from ISTN, Jakarta and a master's degree in Telecommunication Management from Mercu Buana University, Jakarta. Her research interests include E-business, Business Intelligence, and Learning Management System.