Assessing the Impact and Effectiveness of Cybersecurity Measures in e-Learning on Students and Educators: A Case Study

Ala'a Saeb Al-Sherideh[1]*, Khaled Maabreh[2], Majdi Maabreh[3], Mohammad Rasmi Al Mousa[4], Mahmoud Asassfeh[5]
Department of Cyber Security-Faculty of Information Technology, Zarqa University, Zarqa, Jordan[1, 4, 5]
Department of Data Science and Artificial Intelligence-Faculty of Science and Information Technology, Irbid National University, Irbid, Jordan[2]
Department of Information Technology-Faculty of Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa, Jordan[3]

***Abstract*—As e-learning has become increasingly prevalent, cyber security has become a major concern. e-Learning platforms collect and store large amounts of sensitive information, such as personal data and financial information, making them attractive targets for cybercriminals. To address these challenges and concerns, e-learning platforms must implement a comprehensive cyber security strategy that includes strong access controls, data encryption, regular software updates, and student training to help them identify and prevent insider threats. This research aims at investigating and determine how satisfied students are with e-learning security and privacy, as well as whether these concerns affect the overall standard of education. A sample study is presented to assess both the impact of the security framework on students' academic achievements and the student's satisfaction with the security countermeasures in an e-learning system. Statistical analysis showed that the use of security and cyber security countermeasures had a significant effect on the frequent use and participation of students in the contents of the system. Furthermore, encouraging feedback and communication from students about their e-learning experience to share their concerns, questions, and suggestions can help in addressing any security issues or concerns, as well as increasing students' participation in the e-learning content.**

Keywords*—*e-learning; security; cyber security; privacy; countermeasure; Moodle; education

I. Introduction

Technological advancements have significantly impacted the field of education, particularly with the rise of online learning (e-learning). e-Learning refers to the use of digital technology to deliver educational content over the internet [1]. With e-learning, students can access learning materials and participate in classes and discussions from virtually anywhere, using their computers or mobile devices. Technological advancements include high-speed internet connections, learning management systems, video conferencing software, and mobile applications. These tools have made it possible for educators to create engaging and interactive online courses that can be accessed by students all around the world. Furthermore, students can learn at their own pace, review materials as often as they need to, and access course materials anytime, anywhere. Additionally, online learning can be less expensive than traditional classroom-based learning since it eliminates the need for travel and other associated expenses. In the age of technological advancement and transformation in the field of education, and for the considerations mentioned above, the significance of improving the security environments for e-learning systems is growing daily.

Now-a-days, many universities have turned to electronic learning as an efficient solution for providing on-demand learning to their instructors and students. Therefore, and because e-learning primarily depends on Internet technology to achieve its function, information security and cybersecurity become hot topics in the e-learning environment to avoid vulnerabilities and security weaknesses regarding user privacy and content protection [1]. As a result, cybersecurity becomes a key concern when dealing with user privacy, authentication, and confidentiality [7][24][25]. Thus, there is an increasing and significant need for the adoption of strong security countermeasures to protect users' information against any malicious attack. The rest of this study is organized as follows: the next section introduces a background about the e-learning platforms and their impact on security. Section III discusses the related works, the study objectives, and hypothesis is presented in Section IV, Section V states the results and finally, the conclusion is drawn in Section VI.

II. Background

Security in e-learning refers to the protection of the system and data from unauthorized access, alteration, or destruction. Cybersecurity, on the other hand, refers to the protection of digital systems, networks, and data from cyber threats such as hacking, malware, phishing, and ransomware attacks. In the context of e-learning, cybersecurity involves protecting e-learning platforms from such attacks, ensuring the integrity of the data, and minimizing the risk of data breaches.

A. e-Learning Platform Architecture

The architecture of an e-learning platform is designed to provide a seamless user experience while ensuring that all data is stored securely and managed efficiently. It typically includes several key components that are integrated to deliver content and services to users. The main components of an e-learning architecture are [2][3]:

1) User Interface: Front-end component that users interact with to navigate the platform, access courses, and manage their profiles.

2) Application Server: The middleware layer that connects the user interface with the e-learning platform's back-end. It receives requests from the user interface, processes them, and sends back responses.

3) Database: The back-end component provides a centralized storage location that stores all data related to courses, users, progress tracking, and other information.

4) Content Management System: The component that manages course content, including the creation, editing, and delivery of course materials.

5) Learning Management System: The component that manages the delivery of courses and tracks user progress. It provides features such as coarse enrollment, tracking, and reporting.

6) Authentication and Authorization: Manages user authentication and authorization to ensure that only allowed users can access the e-learning system.

7) Security: Responsible for ensuring the e-learning is secure from external threats, including attacks on user data and platform infrastructure.

B. Moodle e-Learning System

Moodle is a popular open-source e-learning platform used by many educational institutions and organizations around the world. Irbid National University (INU) as a case study in this research uses the Moodle e-learning system. The Moodle database schema includes a set of tables and relationships that define how data is stored and organized within the system. Some of the key tables in the Moodle database schema include, for example, the Users table, which stores information about each user in the system, including their first and last name, username, password, email address, and role. The courses table stores information about each course in the system, including its name, description, start and end dates, and visibility settings. Grades: This table stores information about the grades earned by each user in each course. It includes fields for the user ID, course ID, module ID, and grade value. Tables in the database schema are linked together through a series of relationships that define how data is accessed and manipulated within the system. Moodle supports the use of a distributed database architecture, where the database layer is designed to be abstracted from the rest of the system, which means that it can be replaced with different database solutions depending on the needs of the installation. With the distributed database, the data is distributed across multiple nodes, providing greater scalability and fault tolerance than a single database instance [4]. Moreover, it can improve security by replicating data across multiple servers or nodes, making it more difficult for hackers to access or manipulate the data.

C. Security Challenges on e-Learning Arising from the COVID-19 Pandemic

Since the educational process is based primarily or fully on online platforms, the risks presented by e-learning cybersecurity attacks significantly increased during the coronavirus epidemic. Electronic educational tools' reliability and accessibility are now essential, as teaching is impossible without them [5]. Recently, important steps have been taken to create an appropriate legislative framework to ensure an acceptable level of cybersecurity is obtained in Jordan. Jordan is globally ranked 73 on the Global Security Index. They established a National Center for Cybersecurity to strengthen the policies and procedures [6]. The education infrastructure comprises universities, colleges, schools, libraries, teachers, and students. Education infrastructure is more critical when compared to other systems because, for example, universities are designed as open spaces for research and information, making them vulnerable to cyber-attacks even by using simple methods like email attachments [3][13]. So, new cybersecurity measures for educational institutions are necessary. An approach to managing educational resources must take into account the current global environment by adopting new strategies that give digital educational resources far greater consideration [5].

D. Security Issues in e-Learning

e-Learning faces several security issues that organizations and individuals need to be aware of. Some of these issues are:

1) Data privacy: One of the biggest concerns in e-learning is data privacy [7][8][24][25]. e-Learning platforms store a vast amount of sensitive information, including personal information such as names, addresses, and email addresses, as well as sensitive information such as course progress and assessment results [9].

2) Cybersecurity: e-Learning platforms are susceptible to cybersecurity threats, such as hacking, phishing, and malware attacks [10][26][27]. Hackers may target e-learning platforms to gain access to sensitive data or disrupt the system.

3) Identity theft: Identity theft is a severe security issue in e-learning. Hackers may steal personal information to impersonate a user and gain access to e-learning platforms [11].

4) Intellectual property: e-Learning platforms contain valuable intellectual property, including course materials, videos, and assessments [12].

Therefore, e-learning platforms must implement robust security measures to protect sensitive data and intellectual property from cybersecurity threats. Organizations and individuals must also be aware of these security issues and take appropriate precautions to safeguard their information [14]. This research aims to evaluate the degree to which students are satisfied with e-learning security and privacy as well as to examine whether these issues have an impact on the overall quality of education. Measuring the effect of e-learning security on the academic environment is a complex task because other factors can affect it, such as the technology used, how students trust learning as online than others, and the student's background on security challenges and cyberspace.

In conclusion, this research focuses on responding to the following study questions:

- What are the students' attitudes toward e-learning security?

- Does e-learning security affect the quality of education?
- Does the security of the e-learning system influence the students' achievements?
- Do the students trust e-learning content?

III. Related Works

In recent years, there has been an increasing amount of research regarding online learning education. Several studies have begun to examine e-learning regarding design and efficiency. Other earlier studies have concentrated on how the e-learning environment affects student achievement [15][16], while others have discussed and analyzed the performance of those systems. The need for secure online learning environments has given rise to many studies that aim to address the growing significance of the security and sensitivity of an e-learning system's contents. Habib et al. [1] discuss cybersecurity issues related to the e-learning management system, the significance of e-learning, and the database management system also presented, along with the methods that lessen them. Their paper has provided some remedies for obtaining data integrity and recommends that government agencies provide more financial funding to improve the quality of the e-learning system. A survey of the current protections of e-learning systems based on the source of vulnerabilities is presented by Satria et al. [17] They categorize the open-source learning systems as vulnerable points because these systems have suffered many attacks due to security problems. Emad and Mustafa [18] discuss DB integrity and data confidentiality using access control policies and data encryption as two of the main pillars in building information systems.

As e-learning systems are increasingly used by universities due to the low costs associated with education, Ioan et al. [19] presented the security issues related to these platforms. Such issues can be used by cybercriminals for phishing and spamming activities. They suggest law authority enforcement cooperate with academia and private sectors fight to these threats. Anghel and Pereteanu [20] illustrated different approaches that manage the cyber security issues related to e-learning systems. They also showed some practice examples concerning cyber security management techniques and suggested implementing security policies and procedures accepted by individuals to overcome those security threats. The effectiveness of e-learning as well as the potential security issues are discussed by Nguyen et al. [21]. Suggested countermeasures to deal with the security attacks are also outlined. The main recommended countermeasure to make the users feel secure was cryptography.

By reviewing previous studies related to the subject of this research, the researchers focus on the security issues that threaten e-learning systems and suggest effective solutions to mitigate the security attack on the contents of those systems [22]. This research will investigate the security of a database server, which contains the user information and the cyberspace through which this information travels.

IV. Study Objectives and Hypothesis

The study of security in e-learning should equip students with the necessary knowledge and skills to protect themselves and their data, while also promoting the responsible and ethical use of e-learning systems. Important aspects of security and cybersecurity in e-learning systems include:

- Understanding the potential security threats, where students should be able to identify the various types of security threats that can affect e-learning systems, such as hacking, phishing, and malware attacks.
- Knowledge of security measures: Students should learn about the various security measures that can be implemented to protect e-learning systems, such as encryption, firewalls, and multi-factor authentication.
- Learning how to protect personal information: e-Learning students should be taught how to safeguard their personal information, such as usernames, passwords, and credit card details, from theft or misuse.
- Familiarity with data protection regulations: Students should be familiar with data protection laws and regulations that govern e-learning systems, such as the General Data Protection Regulation (GDPR).
- Awareness of ethical considerations: e-Learning students should be taught about ethical considerations regarding the use of e-learning systems, such as respecting the privacy of other students, not plagiarizing content, and using technology responsibly.
- Preparation for emergencies: Students should be taught how to respond to emergencies, such as a cyber-attack or a system failure, and how to protect themselves and their data in such situations.

To evaluate the current situation of the e-learning system as a case study, find the strengths and weaknesses points in the security structure of those systems, and propose suitable recommendations that would improve the services provided, this study aims to suggest and investigate the security measures that are needed to evaluate the satisfaction and acceptance of students towards e-learning services. The measurement process will be analyzed through the following hypothesis: The use of e-learning systems that prioritize security and privacy are more likely to be perceived positively by students and may result in higher levels of engagement, satisfaction, and academic achievement.

A. Methods and Procedures

Methods and procedures are standardized and systematic approaches used to solve problems or answer questions in a study field. They involve a step-by-step process that helps to ensure that the solution is accurate, reliable, and repeatable. The process typically involves the next steps and methods observed:

- Collecting the necessary information on the e-learning security measures and students' perceptions of them.

- Designing a questionnaire that addresses the study's objectives.
- Selecting the right sample of respondents.
- Analyzing the information gathered and concluding the findings.

B. The Population of the Study

As the population of a study refers to the group of individuals that the research is focused on, it must determine the generalizability and validity of the research findings. Since studying the whole population is costly and impractical, a sample is selected to observe and measure the study hypotheses. The population of this study consisted of undergraduate students enrolled in four faculties at the Irbid National University, Jordan. The students are chosen from the second year or higher because they are expected to have some experience using the e-learning system. Their age range is 19 to 23 years old. In this study, the margin of accepted error is assumed to be five, the confidence level needed is 95% and the response distribution is expected to be 80%. Based on the study's objectives, time availability, research budget, and degree of precision, the sample size is 200 students out of 1000 in the four colleges.

C. Sample of the Study

A small-scale survey was created based on the study objectives to measure how students trust the Moodle e-learning system's security and privacy. Two hundred (200) students were chosen at random to receive the questionnaire. One hundred eighty four (184) respondents correctly completed it. The demographic distribution of the students by field of study is shown in Table I.

TABLE I. TOTAL RESPONDENTS BY COLLAGE

Collage	Male	Female	Total Number	Percentage
Faculty of science and information technology	50	28	78	42.40
Faculty of Business Administration and Finance	27	24	51	27.71
Faculty of Nursing	9	19	28	15.22
Faculty of Law	16	11	27	14.67
Total	102	82	184	100

By monitoring the response rate which exceeds 90%, we hope that the sample accurately reflects the population interested in the study.

D. Questionnaire Items

An online survey was used to investigate students' opinions about the security and privacy of the e-learning system operated by Irbid National University. The online survey has been circulated via Facebook and WhatsApp groups. The survey includes 25 questions, distributed as follows: Questions 1–5 were used to collect general information (e.g., gender, year of study, familiarity with using internet resources). Questions 6–15 were used to collect information about students' attitudes toward the level of satisfaction with the current security measures used in the e-learning system. Finally, questions 16–25 were used to measure students' attitudes regarding the influence of the e-learning system with the current security and privacy procedures on their achievements. To facilitate the measurement of the study's hypotheses, questions 6–25 are grouped into eleven categories, as shown in Table II.

E. Study Hypotheses

Ho: e-Learning platforms that are hosted on secure servers do not affect the levels of user trust and confidence.

Ha: e-Learning platforms that are hosted on secure servers will lead to higher levels of user trust and confidence.

V. RESULTS AND DISCUSSION

This study uses a 5-point Likert scale because it balances variation in responses and nuanced opinions while remaining simple and easy to use [23]. Meanwhile, respondents are less likely to become confused or overwhelmed when faced with a complex or lengthy survey. It also lessens the central tendency bias and makes the measurement process easier. Table II shows the percentage of the student responses for each group (strongly agree, agree, strongly disagree, disagree, and do not know). The "do not know" response is used for missing answers or a student's actual answer to some study questions.

As shown in Table II, 56% of students are satisfied with the current security level, which is considered a low indication regarding security and cybersecurity. This may be due to several reasons, including a lack of awareness, which can lead to confusion and frustration and may result in lower levels of satisfaction with the security level, or students may feel that their data is not being adequately protected. Another possible reason may regard some technical issues, such as slow load times or frequent errors, which may lead to dissatisfaction among students. To address these issues, educators and institutions need to prioritize student security and take steps to ensure that students are fully informed and aware of the security measures in place. This can include providing clear and concise instructions on how to use security features, regularly updating security measures, and being transparent about how student data is collected and used. Additionally, educators and institutions should regularly gather feedback from students and take steps to address any issues or concerns that arise.

Data in Table II indicates that there is a reluctance among students to use the system in the event of security attacks (88%), while their confidence increases when the system adopts strict countermeasures (69%). Furthermore, if students perceive the e-learning system as insecure, they may be more likely to seek out alternative ways of accessing course content and resources, such as through unsecured channels or external websites. This could increase the risk of data breaches and compromise the security of student data. Therefore, it is important for educators and institutions to take student concerns about e-learning system security seriously and to take steps to address them. This can include implementing additional security measures, such as two-factor authentication or data encryption, and providing clear and transparent information about how student data is collected, stored, and used. Educators and institutions can help to build trust and confidence among students in the security of e-learning systems. This, in turn, can lead to increased engagement and academic achievement, as students feel more comfortable and

secure in using the system to access course materials and interact with their peers and instructors. By adopting these measures, educators and institutions can demonstrate their commitment to student data privacy and security, fostering trust and confidence among students in the e-learning environment. As long as more than 90% of students expressed their desire to take intensive courses relating to cybersecurity and its latest developments. More than 86% of students, as shown in Table II, concur that improving the security of the Moodle e-learning platform will increase student achievement and engagement, which may either directly or indirectly improve their academic performance.

The use of personal devices in e-learning systems has become increasingly popular in recent years. With the proliferation of smartphones, tablets, and laptops, students now have access to a wide range of digital devices that can be used to support their learning. However, there are also some potential drawbacks to using these devices. One concern, as expressed by 64% of respondents, is that it can increase the risk of data breaches and cyber-attacks due to the potential for unsecured devices and networks. So, it is important for educators and institutions to carefully consider how to effectively integrate these devices into their teaching and learning strategies and to ensure that all students have equal access to learning resources and opportunities. Cloud-based storage allows data to be stored securely on remote servers rather than on individual devices. This means that if a student's device is lost or stolen, their data remains safe and can be accessed from another device. Additionally, cloud-based storage can provide automatic backups of data, reducing the risk of data loss. 67% of students indicated this positively. Enhancing the security countermeasures in the e-learning system can potentially enhance student engagement and achievement. When students feel that their data is secure, they may be more likely to actively engage with the e-learning system and its resources, leading to increased achievement. By implementing the necessary security measures, students may feel more confident in using the Moodle e-learning system and its resources. This, in turn, can lead to increased engagement and achievement, as 86% of students state.

Social engineering is indeed an important aspect of e-learning security that should not be overlooked. 92% of students, report having encountered social engineering-related problems and affirm that intensive training boosts their confidence in the e-learning system and helps them protect their data. Protecting students from such issues requires a combination of technical and educational measures, including educating them about the tactics used by cybercriminals, such as phishing and pre-texting baiting. Providing two or more forms of authentication, including a strong password and a one-time code, makes it more difficult for cybercriminals to gain access to accounts.

TABLE II. RESULTS OF THE STUDY SURVEY

Response Option	Strongly Agree	Agree	Strongly Disagree	Disagree	Do not know
The current Moodle e-learning system is considered a secure and effective learning tool.	0.29	0.27	0.2	0.22	0.02
Students who report concerns about e-learning systems security may be less likely to use the system frequently which could lead to reduced engagement and academic achievement.	0.43	0.45	0.07	0.03	0.02
Students who perceive e-learning systems as secure may be more likely to use the system frequently and engage with it more effectively.	0.41	0.44	0.08	0.06	0.01
Students who are required to use strong security measures such as strong passwords or two-factor authentication may perceive the system as more secure and trustworthy.	0.33	0.36	0.11	0.14	0.06
Students who receive training on e-learning system security best practices may be more likely to engage with the system and use it effectively and may also report higher levels of trust and confidence.	0.47	0.44	0.02	0.04	0.03
Students who receive regular updates and communication about the e-learning system's security can help them feel more informed about the security measures, leading to more positive attitudes and trust.	0.41	0.43	0.03	0.07	0.06
Students who receive training on cyber security practices and awareness may be more likely to protect their personal data and privacy.	0.51	0.41	0.01	0.03	0.04
The use of personal devices in e-learning systems can increase the risk of data breaches and cyber-attacks due to the potential for unsecured devices and networks.	0.31	0.33	0.16	0.19	0.01
e-Learning systems that use cloud-based storage and security measures can help protect student data and privacy when using personal devices and networks.	0.34	0.33	0.15	0.1	0.08
Enhancing the security countermeasures in the Moodle e-learning system will enhance the student’s engagement and achievement.	0.42	0.44	0.03	0.05	0.06
Providing training to students on how to recognize and avoid phishing or fraudulent emails and other forms of cybercrime is an important step in promoting digital safety and security. It can help to develop better digital literacy skills and create a safer online environment for all users.	0.49	0.45	0.01	0.03	0.02

A. Statistical Analysis

The data collected is analyzed using descriptive statistics to summarize their frequency and distribution. The study sample and variables were described using frequencies and standard deviations. To ascertain whether there were any statistically significant differences between the study group means, the one-way analysis of variance (ANOVA) was also utilized to prove the study hypothesis. All statistical analyses were performed using SPSS version 25.0. It specifically evaluates the null hypothesis, thus if there are at least two group means that are statistically significantly different from one another, the alternative hypothesis (Ha) will be accepted.

According to the statistical analysis shown in Table III, the "Strongly Agree" group has the highest mean (0.40), followed by the "Agree" group (0.39). Strongly disagree, disagree, and do not know with respective mean values of 0.07, 0.08, and 0.03. The research reveals that the 'Strongly Agree group' has the highest standard deviation (0.074), which is relatively small and indicates less dispersion than the means of the other groups. Because of this, there is a large statistical difference between the groups. A low standard error indicates that the data points in a sample are tightly clustered around the sample mean, suggesting that the sample accurately represents the population being studied and that the estimated value is closer to the true population parameter. An ANOVA test for the study variables at a 0.95 confidence interval is figured in Table IV. The value of P (9.03518E-23) is less than 0.05, which indicates that the probability of obtaining the observed test statistic under the null hypothesis is very low, and hence, the null hypothesis is unlikely to be true. Consequently, there is evidence to imply that there is a statistically significant difference between the means of the variables for at least one of the groups being compared. As a result, the alternative hypothesis (Ha) has been accepted and the null hypothesis (Ho) has been rejected. So, e-learning platforms that are hosted on secure servers will lead to higher levels of user trust and confidence.

TABLE III. DESCRIPTIVE STATISTICS OF THE STUDY VARIABLES

Groups	Count	Sum	Average	Variance	Std. Dev.	Std. Error
Strongly agree	11	4.41	0.400909091	0.005529091	0.074357857	0.02241974
Agree	11	4.35	0.395454545	0.003887273	0.062347997	0.01879863
Strongly disagree	11	0.87	0.079090909	0.004509091	0.067149765	0.02024642
Disagree	11	0.96	0.087272727	0.004561818	0.067541233	0.02036445
Do not know	11	0.41	0.037272727	0.000581818	0.024120908	0.00727273

TABLE IV. ANOVA TEST FOR THE STUDY VARIABLES AT A = 0.05

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	1.456109091	4	0.364027273	95.44956 14	9.03518E-23	2.55717915
Within Groups	0.190690909	50	0.003813818			
Total	1.6468	54				

VI. CONCLUSION AND FUTURE WORK

With the increasing popularity of e-learning, there has been a corresponding rise in security and cybersecurity concerns. This is because e-learning platforms and tools store and transmit sensitive information, such as personal identification details, financial information, and intellectual property. Therefore, e-learning platforms are also vulnerable to cyber threats due to the large amounts of data they handle, the use of multiple devices and networks, and the diversity of users.

This research aims at exploring whether e-learning security and privacy concerns have an effect on the overall standard of education and can provide valuable insights into the relationship between cybersecurity and educational outcomes. The effectiveness of the security framework on students' academic achievement and their satisfaction with the security countermeasures in an e-learning system are both evaluated using a sample study that is presented. Statistical analysis finding suggests that implementing security and cybersecurity countermeasures can positively impact students' engagement with a system. Encouraging feedback and communication from students about their e-learning experience can be an effective way to address any security issues or concerns and improve their engagement with the e-learning content. By actively seeking and listening to feedback, instructors, and administrators can identify potential areas of vulnerability in the system and take steps to improve security measures.

ACKNOWLEDGMENT

This research is funded by the Deanship of Research and Graduate Studies at Zarqa University /Jordan.

REFERENCES

[1] H. Ibrahim, S. Karabatak, and A. A. Abdullahi, "A study on cybersecurity challenges in e-learning and database management system," in 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-5.

[2] Moodle. (2023, Feb-27-2023). Moodle - Open-source learning platform. Available: https://moodle.org/.

[3] A. M. Udroiu, "The cybersecurity of elearning platforms," in Conference proceedings of» eLearning and Software for Education «(eLSE), 2017, pp. 374-379.

[4] K. Maabreh and A. Al-Hamami, "Implementing new approach for enhancing performance and throughput in a distributed database," Int. Arab J. Inf. Technol., vol. 10, pp. 290-296, 2013.

[5] T.-M. G. Răzvan BOLOGA, "Cybersecurity for Online Learning," in Cybersecurity -Challenges and Perspectives In Education, C. C. Ioan-Cosmin MIHAI, Gabriel PETRICĂ, Ed., ed Romania: Romania Association for Information Security Assurance, 2020.

[6] TresconSyberSec. (2022, Feb-27-2023). World Cybersecurity Summit. Available: https://tresconglobal.com/conferences/cyber-sec/jordan/

[7] M. Alier, M. J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca, "Privacy and E-learning: A pending task," Sustainability, vol. 13, p. 9206, 2021.

[8] A. M. Gabor, M. C. Popescu, and A. Naaji, "Security Issues Related To E-Learning Education," International Journal of Computer Science and Network Security (IJCSNS), vol. 17, p. 60, 2017.

[9] T. Husain and A. Budiyantara, "Analysis of Control Security and Privacy Based on e-Learning Users," SAR Journal, vol. 3, pp. 51-58, 2020.

[10] А. Г. Тецький and О. І. Морозова, "Cybersecurity aspects of E-learning platforms," Radioelectronic and Computer Systems, pp. 93-97, 2020.

[11] D. Korać, B. Damjanović, and D. Simić, "A model of digital identity for better information security in e-learning systems," The Journal of Supercomputing, pp. 1-30, 2021.

[12] Z. Mingaleva and I. Mirskikh, "The protection of Intellectual property in educational process," *Procedia-Social and Behavioral Sciences*, vol. 83, pp. 1059-1062, 2013.

[13] F. Salahdine and N. Kaabouch, "Social engineering attacks: A survey," Future Internet, vol. 11, p. 89, 2019.

[14] O. L. Academy. (2023, Feb-28-2023). eLearning Security: How to Keep Data Protected in Your Open Source LMS. Available: https://www.openlms.net/blog/products/elearning-security-how-to-keep-data-protected-open-source-lms/

[15] K. S. Maabreh, "The impact of e-learning usage on students' achievements: a case study," International Journal of Knowledge and Learning, vol. 12, pp. 193-203, 2018.

[16] J. Paul and F. Jefferson, "A comparative analysis of student performance in an online vs. face-to-face environmental science course from 2009 to 2016," Frontiers in Computer Science, vol. 1, p. 7, 2019.

[17] S. Mandala, A. Abdullah, and A. Ismail, "A survey of e-learning security," in International Conference on ICT for Smart Society, 2013, pp. 1-6.

[18] E. F. Khalaf and M. M. Kadi, "A survey of access control and data encryption for database security," JKAU: Eng. Sci, vol. 28, pp. 19-30, 2017.

[19] I.-C. Mihai, Ș. PRUNĂ, and G. PETRICĂ, "A COMPREHENSIVE ANALYSIS ON CYBER-THREATS AGAINST ELEARNING SYSTEMS," eLearning & Software for Education, vol. 3, 2017.

[20] M. Anghel and G. Pereteanu, "Cyber Security Approaches in E-Learning," in INTED2020 Proceedings, 2020, pp. 4820-4825.

[21] N. Huu Phuoc Dai, A. Kerti, and Z. Rajnai, "E-learning security risks and its countermeasures," Journal of Emerging research and solutions in ICT, vol. 1, pp. 17-25, 2016.

[22] M. Jouini, L. B. A. Rabai, and A. B. Aissa, "Classification of security threats in information systems," Procedia Computer Science, vol. 32, pp. 489-496, 2014.

[23] C. Heumann and M. S. Shalabh, Introduction to statistics and data analysis: Springer, 2016.

[24] A. S. Al-Sherideh, R. Ismail, F. A. Wahid, N. Fabil, & W. Ismail. (2018). Mobile government applications based on security and privacy: a literature review. International Journal of Engineering and Technology (UAE).

[25] A. S. Al-Sherideh, R. Ismail. (2020). Motivating path between security and privacy factors on the actual use of mobile government applications in Jordan. International Journal on Emerging Technologies.

[26] M. R. Al-Mousa, M. Al Zaqebah, A. S. Al-Sherideh, Mohammed. Al-Gghanim, G. Samara, S. Al-Matarneh, M. R. Asassfeh. (2022). Examining Digital Forensic Evidence for Android Applications. In 2022 23nd International Arab Conference on Information Technology (ACIT).

[27] M. Al-Khateeb, M. Al-Mousa, A. Al-Sherideh, D. Almajali, M. Asassfeha, & H. Khafajeh. (2023). Awareness model for minimizing the effects of social engineering attacks in web applications. International Journal of Data and Network Science, 7(2), 791-800.