International Journal of Electrical and Computer Engineering (IJECE)
Vol. 15, No. 1, February 2025, pp. 719~727
ISSN: 2088-8708, DOI: 10.11591/ijece.v15i1.pp719-727

Enhancing online exam security: encryption and authentication in Jordanian and international universities

Ali M. Al-Ghonmein, Yahia Alemami, Khaldun G. Al-Moghrabi, Saleh Atiewi
Faculty of Information Technology, Al-Hussein Bin Talal University, Ma'an, Jordan

Article Info

Article history:

Received May 26, 2024
Revised Sep 2, 2024
Accepted Oct 1, 2024

Keywords:

Authentication
Cryptography
Decision support system
Encryption
Online examination system
Security trends

ABSTRACT

In today's educational landscape, the online examination system has become crucial, particularly due to the challenges posed by the coronavirus disease 2019 (COVID-19) pandemic. Despite its advantages in expediting result dissemination and reducing resource consumption, online examinations face significant security threats like leakage, cheating, fraud, and hacking, which hinder their widespread adoption. This paper addresses these security concerns by proposing integrating advanced security algorithms and biometric devices. It presents a comprehensive literature review on existing online examination systems, focusing on their security mechanisms, and compares these findings with a proposed framework. Additionally, a questionnaire was administered across Jordanian governmental and private universities to explore strategies for safeguarding computerized tests through encryption and authentication methods. The results reveal that Jordanian institutions lack adequate security safeguards and procedural standards. Key recommendations include encrypting the question bank stored in databases and employing biometric identification techniques to enhance the security and effectiveness of student verification. The proposed framework aims to improve the overall security, speed, and secrecy of the online examination process, addressing the critical gaps identified in current systems. This research contributes to developing more secure and reliable online examination systems in higher education.

Corresponding Author:

Khaldun G. Al-Moghrabi
Faculty of Information Technology, Al-Hussein Bin Talal University
King Hussien Bin Talal University Str, Ma'an, Jordan
Email: Khaldun.g.moghrabi@ahu.edu.jo

1. INTRODUCTION

In recent years, the proliferation of technology has significantly transformed various aspects of education, including assessment methods. One of the most notable advancements in this domain is the emergence of online examination systems (OESs) [1], [2]. Also known as e-assessments or computer-based tests, online examinations (OEs) have garnered widespread popularity owing to their convenience, flexibility, and scalability. This mode of assessment utilizes digital platforms to administer tests, quizzes, and exams, thereby eliminating the need for traditional pen-and-paper methods [3]–[5]. The concept of OEs encompasses a wide range of assessments, spanning from simple multiple-choice questions to complex simulations and interactive exercises [6], [7]. These assessments can be conducted remotely, allowing students to participate from any location with internet access, thus breaking down geographical barriers and enabling access to a broader audience. Moreover, OEs offer immediate feedback to participants, enhancing the learning process and enabling instructors to identify areas of improvement more efficiently [8].

The implementation of OES brings forth numerous advantages for both educators and learners. For educators, these systems streamline the assessment process, automating tasks such as test creation, grading, and result analysis. This automation not only saves time but also reduces the likelihood of human errors, ensuring greater accuracy in assessment outcomes. Additionally, OEs provide educators with valuable insights into student performance trends and learning gaps, enabling them to tailor their teaching strategies accordingly [9], [10].

From the perspective of learners, OEs offer unparalleled convenience and flexibility. Participants can take exams at their own pace and preferred time, accommodating diverse schedules and learning preferences. Moreover, the digital format of these assessments often allows for multimedia integration, creating a more engaging and interactive testing experience. Furthermore, OEs promote environmental sustainability by reducing the consumption of paper and other physical resources associated with traditional assessment methods [11]–[14].

However, despite the numerous benefits, OEs also pose certain challenges and considerations. Issues such as technology-related glitches, security concerns, and the potential for academic dishonesty necessitate careful planning and implementation strategies. Additionally, ensuring equitable access to technology and addressing digital literacy disparities among students are critical factors to consider in the adoption of OES [11], [15], [16]. The study aims to enhance the security of OESs by identifying current shortcomings and recommending a combination of advanced security measures tailored to the needs of Jordanian universities. This paper is structured as follows: section 2 discusses literature reviews; section 3 presents the questionnaire findings, including the results and discussion of the study. Finally, section 4 offers the conclusion.

2. LITERATURE REVIEW

In this section, we delve into the realm of safeguarding OEs integrity, focusing on various protective measures, including encryption methods [17]. The authors of this paper present a pioneering approach to OEs security through a fusion of biometric authentication and blockchain technology. By encrypting exam data and fortifying face templates with advanced cryptographic methods, the proposed system offers unparalleled levels of security, privacy, and dispute resolution. This innovative solution, built upon the principles of decentralization and tamper resistance inherent in blockchain, marks a significant advancement in safeguarding OEs integrity [18].

The study implemented a comprehensive framework for OEs in South African universities, emphasizing authentication and continuous monitoring. Authentication involved capturing students' digital signatures through fingerprints and facial recognition, while continuous monitoring utilized remote proctors and various biometric checks. These methods aimed to ensure exam integrity and align with the socio-technical theory's technical subsystems [19]. Rafee and Nema [20] presents a secure e-learning platform for teachers and students, using zero-knowledge proof (ZKP) and Rivest-Shamir-Adleman (RSA) algorithms for registration and login, with advanced encryption standard (AES) encryption for personal and exam data storage. Simulated results confirm the system's security, ensuring passwords are not transmitted explicitly over the internet and data remains incomprehensible to attackers.

Song [21] focus on the development of a collaborative OES leveraging cloud computing (CC) technology. The system's architecture included software as a service (SaaS) deployment and followed a model-view-controller (MVC) three-tier structure. Implementation utilized Java modeling language, XFIE, JSON, web service, data encryption standard (DES) encryption, and a MySQL database. Notably, the study introduced an enhanced parallel genetic annealing algorithm (EPGAA) for efficient resource scheduling within the CC environment.

The proposed OES [22] integrates AES 256 encryption for secure data transfer and QR code generation for candidate authentication. It utilizes a three-layered architecture with MySQL database, Apache server, and Java server pages (JSP) servlet programming. Additionally, android-based QR code scanning is implemented. This comprehensive system aims to enhance examination security and efficiency in educational institutions. The proposed method [23] implements modified AES-electronic code book (CBC) encryption and traditional algorithms like DES and RSA to secure documents exchanged in e-learning, ensuring authenticity and integrity.

Using the DES algorithm, a security system was developed to safeguard exam questions, ensuring they remain unreadable before exam time. Additionally, the Caesar cipher algorithm generated an extra hidden key for added protection. Results indicate DES encryption offers optimal security for transmitted data in virtual storage systems [24]. Haytom *et al.* [25] presents a multimodal remote examination management system (MREMS) to enhance the security of remote exams. It integrates biometric modalities like face recognition and keystroke dynamics, with robust fraud detection measures, ensuring reliable identity verification and privacy protection.

The review examined security advancements in e-learning systems over the past decade, focusing on the confidentiality, integrity and availability (CIA) triad and proposed solutions. Notably, recent studies have highlighted the significance of blockchain technology and cloud-based architectures. Future research should delve deeper into these areas, possibly utilizing quantitative methods like questionnaires and qualitative approaches such as in-depth interviews. Furthermore, exploring open-source processes in e-learning security presents an intriguing avenue for further investigation [26]. This project aims to enhance security in computer-based exams by developing a CBE web application with fingerprint authentication. By integrating this feature into the login interface, the risk of unauthorized candidate impersonation is mitigated, ensuring the integrity of the examination process [27].

Artificial intelligence (AI) integration in online exams has bolstered security through facial and voice recognition technology, surpassing human capabilities in some cases. Professors and students alike find AI-powered testing systems simplify tasks and enhance convenience. As AI methods continue to evolve, online exams are expected to become even more secure and autonomous, potentially eliminating the need for human involvement in the future [17], [28], [29].

Patil *et al.* [30] aims to enhance OES by focusing on candidate authentication and malpractice prevention. Proposed improvements include pixel enhancement for clearer visibility, incorporation of front and rear-facing camera detection, and audio enhancement to reduce background noise. Additionally, data encryption and secure communication protocols will be implemented to ensure the security of the examination process. Sunday *et al.* [31] proposes an e-exam system employing a multi-factor security and authentication mechanism to address security challenges in electronic examinations. Biometric authentication, encryption for data security, and spyware for e-monitoring are integrated to mitigate threats such as collusion and unauthorized internet access. Evaluation of the system demonstrates promising results in enhancing security and authentication for online exams.

The paper discusses the development and integration of a web-based examinations management system at German Jordanian University (GJU), featuring flexible exam structures, automated grading, and stringent security measures including single sign-on authentication and prevention of student impersonation. Deployment results indicate successful usage for online exams, with positive feedback from users. While future work entails exploring biometric authentication methods and additional question types for further system enhancement [32].

When comparing these studies, it is evident that various approaches to authentication and data security are critical for the integrity of OE and learning platforms. While some studies focus on biometric and real-time monitoring techniques, others emphasize encryption and blockchain technologies. The differences highlight the multi-faceted nature of securing online education environments and the need for a holistic approach integrating multiple security measures. Table 1 summarizes various methods and encryption algorithms employed in OES across different years and institutions. It highlights their strengths and weaknesses in terms of protecting examination integrity and ensuring secure authentication. Figure 1 illustrates the key findings from the literature review regarding the use of encryption and authentication methods in OE. It highlights various strategies employed to secure online assessments, ensuring data security and user identity verification.

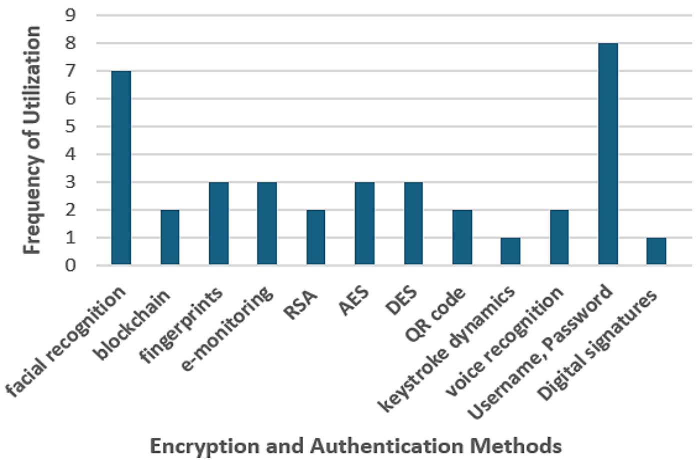


Figure 1. Frequency of utilization of encryption and authentication methods

Table 1. Methods and encryption algorithms in OES

Year	Ref.	Framework	Protected methods/ encryption algorithm	Authentication method	Strength points	Weakness point
2023	[33]	Online exams in Kazakhstan	-	Face and voice recognition	Face recognition boasts high biometric accuracy, making it a reliable identification method. Voice recognition provides a unique and user-friendly biometric authentication method	Accuracy may vary due to factors such as lighting conditions and facial expressions. Background noise and environmental factors can impact the accuracy of voice recognition.
2022	[34]	Moodle	MD5, SSL	Username, password	Enforcing SSL enhances the security of OE. One benefit of employing the MD5 security algorithm is its irreversible hashing, preventing the conversion of its hashed output back to the original format.	The authentication method used traditional and inadequate.
2021	[19]	South African Universities	-	Digital signatures based on fingerprints and facial recognition	Biometric digital signatures boost security by utilizing unique biological features, thwarting unauthorized access.	Biometric authentication, like fingerprint and facial recognition, can be costly
2020	[35]	Universities in Sri Lanka	MD5	Username, password, SMS notification	MD5 works seamlessly across different systems.	SMS may inconvenience users without immediate mobile access.
2020	[22]	Educational Institutes	AES 256	Username, password, QR code, web camera	AES 256 provides strong encryption, making it highly resistant to brute-force attacks.	Relying on web cameras poses potential challenges due to hardware malfunctions or connectivity issues.
2019	[36]	Mumbai University	AES	Username, password	The questions and answers store in the database is an encrypted format by AES algorithm	The authentication method used traditional and inadequate.
2019	[37]	Zambia’s Technical Education, Vocational and Entrepreneurship Training Authority (TEVETA)	Hash functions (Sha3-224), AES	Candidate information (username, password…)	Allows students and other stakeholder to access students’ results through mobile phones and the web.	Only security issues relevant to students' examination results were addressed.
2018	[38]	Adamawa State University, Mubi	MD5	Username, password	Encrypt login details of users by MD5.	Cryptography algorithms are not utilized to protect the question bank from unauthorized modification or leakage. Additionally, the authentication method employed is inadequate.
2018	[39]	Generally (Record Database of Computer Based Test Exam)	Spritz algorithm	Username, password	The Spritz algorithm's high complexity poses challenges for cryptanalysts, making it difficult to find the key.	The key generation process is time-consuming, both encryption and decryption entail lengthy processing times and modern authentication methods to differentiate unauthorized students from authorized ones are not utilized.
2018	[40]	SCSVMV University (India) for Academic management system	SQL injections prevention coding	Username, password	Encipherment username and password. Encipherment cookies and sessions.	The authentication method employed is traditional and inadequate.

3. QUESTIONNAIRE FINDINGS: RESULTS AND DISCUSSION

The experience of online exams in Jordanian universities is an experiment that has been applied for years and has gone through several stages of development in terms of content, performance and safety. The stages of development continue, which lead to taking Jordanian universities as a study sample because of the large number of educational institutions (universities, institutes, and colleges) that adopted online exams as a tool for students' assessment. A questionnaire was conducted in all 30 public and private universities in Jordan. The most important questions were asked through the questionnaire:

a. Does your university use an online examination?

OE has become a critical component of the academic landscape, especially in the wake of technological advancements and the increased need for remote learning solutions. Figure 2 illustrates that all 30 universities employed OE across the majority of their classes. This underscores the significance of OE in higher education.

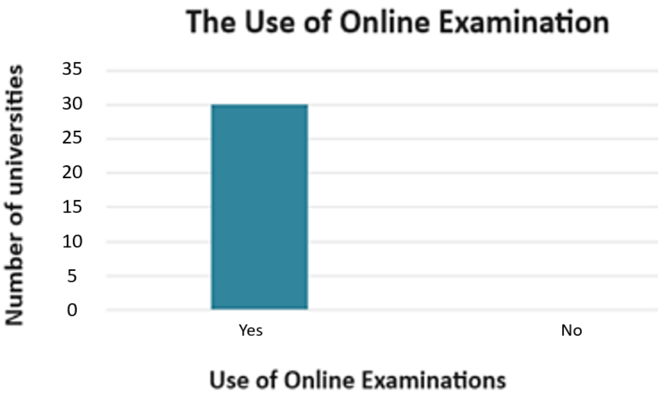
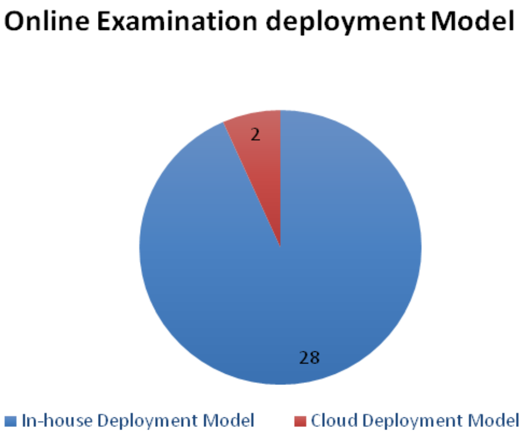


Figure 2. The use of OE

b. How did you deploy your online examination system?

This question describes the way each university implements the OES, whether through an in-house deployment model or a cloud-based model. Figure 3 illustrates that over 93% of Jordanian universities employed an in-house deployment model for OE. It indicates their responsibility for addressing security concerns within the system.



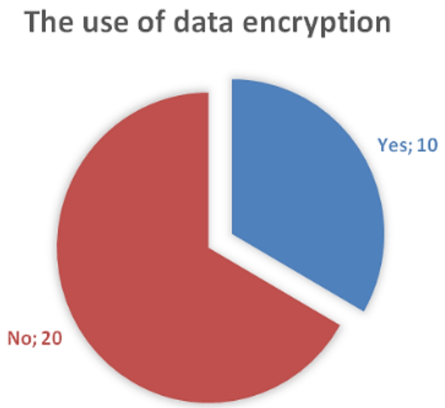


Figure 3. OE deployment model

Figure 4. The use of data encryption

c. Do you use data encryption for your question bank?

This question focuses on how the question bank is stored on a computer server, whether it is encrypted or stored as plain text. Figure 4 reveals that one-third of the universities employ data encryption. While the remaining two-thirds store the question bank without encryption.

d. What type/method of data encryption do you apply at your question bank?

This question explores the methods and algorithms used by universities to encrypt the question bank, as we have seen from Figure 4 only one-third of the universities used data encryption. Additionally, Figure 5 reveals that 7 out of 10 universities are aware of the encryption type used, while the rest are not. Also, we can conclude from Figure 5 that the most used algorithm for encryption is AES, whereas MD5 and 3DES come in second place.

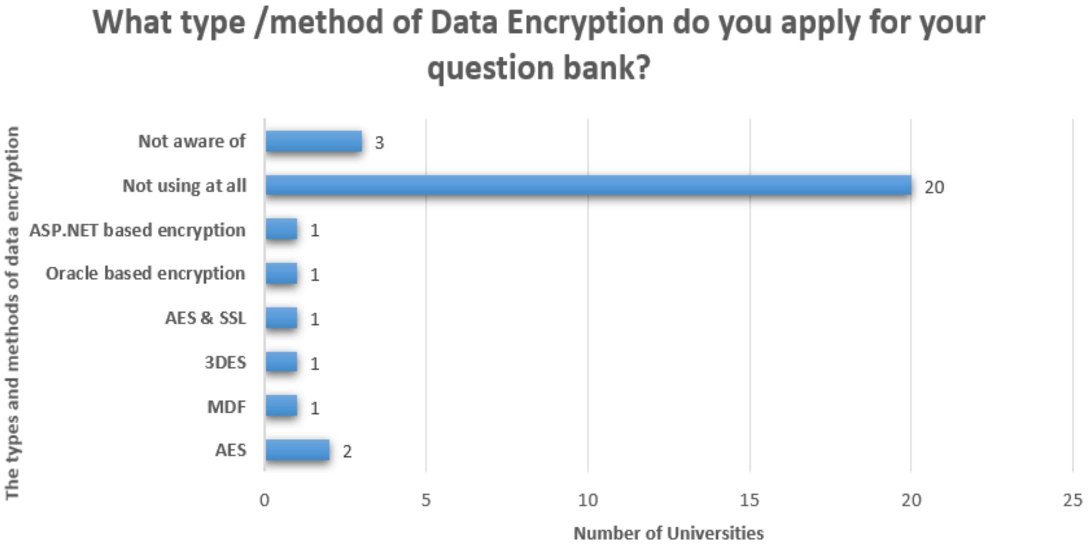


Figure 5. Data encryption algorithms

e. What type of user authentication is applied to your online examination system?

The second important security issue in the OE is user authentication. This question focuses on the type of user authentication. Figure 6 shows that more than 93% of universities use only usernames and passwords. Whereas less than 7% of the universities utilize biometric features in conjunction with usernames and passwords to enhance security levels.

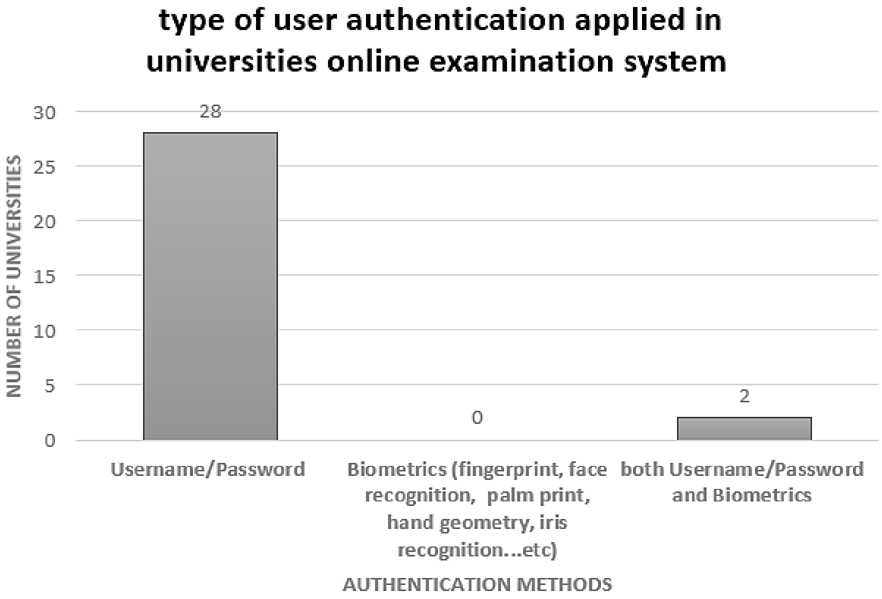


Figure 6. User authentication

4. CONCLUSION

The OES functions through a web interface, allowing administrators, lecturers, and students to log in. Lecturers create a question bank and set constraints such as IP restrictions and exam timeframes, ensuring exams are accessible only during authorized periods. Students take exams online, with automatic evaluation and prompt result display. Encrypting the question bank in the database enhances security, efficiency, and confidentiality, while biometric authentication methods like fingerprint scanning improve student verification. Survey findings on Jordanian universities' OES reveal significant security shortcomings. Implementing robust encryption algorithms and stringent authentication protocols can effectively address these concerns. The paper proposes integrating advanced security algorithms and biometric devices to enhance security and efficiency. A comprehensive literature review identified various approaches to online exam security, underscoring the importance of multiple security measures. Survey results indicated a lack of adequate security safeguards and procedural standards, with over 93% of universities using traditional username-password authentication. The paper recommends adopting robust encryption algorithms and biometric authentication methods to enhance security in Jordanian universities' OES.

REFERENCES

[1] S. Coghlan, T. Miller, and J. Paterson, “Good proctor or ‘big brother’? ethics of online exam supervision technologies,” *Philosophy & Technology*, vol. 34, no. 4, pp. 1581–1606, Dec. 2021, doi: 10.1007/s13347-021-00476-1.

[2] F. Alnasser and A. Elrashidi, “Improving the security of E-exam systems,” in *2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD)*, Mar. 2023, pp. 1–7, doi: 10.1109/ITIKD56332.2023.10100104.

[3] T. AlKursheh, “Higher tertiary education perspectives: evaluating the electronic assessment techniques of the blackboard platform for fairness and reliability,” *Innoeduca. International Journal of Technology and Educational Innovation*, vol. 10, no. 1, pp. 144–165, Jun. 2024, doi: 10.24310/ijtei.101.2024.17813.

[4] N. Selwyn, C. O’Neill, G. Smith, M. Andrejevic, and X. Gu, “A necessary evil? The rise of online exam proctoring in Australian universities,” *Media International Australia*, vol. 186, no. 1, pp. 149–164, Feb. 2023, doi: 10.1177/1329878X211005862.

[5] S. Lu, C. B. Eloanyi, and C. J. Olelewe, “Computer educators’ perception of the utilization of online assessment in the Covid-19 era,” *Computer Applications in Engineering Education*, vol. 31, no. 4, pp. 983–1000, Jul. 2023, doi: 10.1002/cae.22618.

[6] E. Owusu-Oware, H. T.-J. of C. I. In, and U. 2023, “The effectiveness and integrity of online assessments using moodle learning management system: perspectives of a developing country’s University teachers,” *Researchgate.Net*, vol. 26, no. 2, pp. 262–282, 2019, doi: 10.47750/cibg.2023.29.03.011.

[7] A. W. Muzaffar, M. Tahir, M. W. Anwar, Q. Chaudry, S. R. Mir, and Y. Rasheed, “A systematic review of online exams solutions in e-learning: techniques, tools, and global adoption,” *IEEE Access*, vol. 9, pp. 32689–32712, 2021, doi: 10.1109/ACCESS.2021.3060192.

[8] A. Bashir, S. Bashir, K. Rana, P. Lambert, and A. Vernallis, “Post-COVID-19 adaptations; the shifts towards online learning, hybrid course delivery and the implications for biosciences courses in the higher education setting,” *Frontiers in Education*, vol. 6, Aug. 2021, doi: 10.3389/feduc.2021.711619.

[9] A. M. Ghonmein, K. G. Al-Moghrabi, and T. Alrawashdeh, “Students’ satisfaction with the service quality of academic advising systems,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1838–1845, Jun. 2023, doi: 10.11591/ijeecs.v30.i3.pp1838-1845.

[10] R. Scherer, S. K. Howard, J. Tondeur, and F. Siddiq, “Profiling teachers’ readiness for online teaching and learning in higher education: who’s ready?,” *Computers in Human Behavior*, vol. 118, May 2021, doi: 10.1016/j.chb.2020.106675.

[11] Z. Almahasees, K. Mohsen, and M. O. Amin, “Faculty’s and students’ perceptions of online learning during COVID-19,” *Frontiers in Education*, vol. 6, May 2021, doi: 10.3389/feduc.2021.638470.

[12] A.-M. M. Gasaymeh, A. M. Al-Tawel1, K. G. Al-Moghrabi, and A. M. Al-Ghonmein, “University students’ perceptions of the use of digital technologies in their formal learning: a developing country perspective,” *International Journal of Learning and Development*, vol. 7, no. 3, Aug. 2017, doi: 10.5296/ijld.v7i3.11666.

[13] L. Serutla, A. Mwanza, and T. Celik, “Online assessments in a changing education landscape,” in *Reimagining Education - The Role of E-Learning, Creativity, and Technology in the Post-Pandemic Era*, IntechOpen, 2024.

[14] J. Hasan Alkhateeb, “A framework for ensuring online exam authentication at Taibah University,” *International Journal of Software Engineering and Computer Systems*, vol. 6, no. 1, pp. 1–7, May 2020, doi: 10.15282/ijsecs.6.1.2020.1.0064.

[15] Y. Alemami, A. M. Al-Ghonmein, K. G. Al-Moghrabi, and M. A. Mohamed, “Cloud data security and various cryptographic algorithms,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1867–1879, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1867-1879.

[16] M. Aristeidou, S. Cross, K. Rossade, C. Wood, T. Rees, and P. Paci, “Online exams in higher education: exploring distance learning students’ acceptance and satisfaction,” *Journal of Computer Assisted Learning*, vol. 40, no. 1, pp. 342–359, Feb. 2024, doi: 10.1111/jcal.12888.

[17] K. G. Al-Moghrabi and A. M. Al-Ghonmein, “The role of chat generative pre-trained transformer in facilitating decision-making and the e-learning process in higher education,” *Bulletin of Electrical Engineering and Informatics*, vol. 13, no. 3, pp. 2058–2066, Jun. 2024, doi: 10.11591/eei.v13i3.7237.

[18] S. M. Umran, S. Lu, Z. A. Abduljabbar, J. Zhu, and J. Wu, “Secure data of industrial internet of things in a cement factory based on a Blockchain technology,” *Applied Sciences*, vol. 11, no. 14, Jul. 2021, doi: 10.3390/app11146376.

[19] T. Ngqondi, P. B. Maoneke, and H. Mauwa, “A secure online exams conceptual framework for South African universities,” *Social Sciences & Humanities Open*, vol. 3, no. 1, 2021, doi: 10.1016/j.ssaho.2021.100132.

[20] R. M. Rafee and B. M. Nema, “Secure e-learning system based on ZNP and AES,” *Al-Mustansiriyah Journal of Science*, vol. 33, no. 1, pp. 39–44, Mar. 2022, doi: 10.23851/mjs.v33i1.1016.

[21] S. Song, “Construction of university online examination system based on cloud computing technology,” *Scientific Programming*, vol. 2021, pp. 1–10, Dec. 2021, doi: 10.1155/2021/7849255.

[22] M. I. Shruti, “Designing security framework for secure exam system based on QR code,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, no. 6, pp. 1692–1697, Jun. 2020, doi: 10.22214/ijraset.2020.6276.

[23] A. Ghosh, S. Adhikari, and S. Karforma, "A fast and efficient document encryption method for e-learning applications using modified AES-CBC with chaotic logistic pseudo random number sequence," *Advances in Mechanics*, vol. 9, no. 3, pp. 1051–1060, 2021.

[24] O. H. Siyaka, "A Secured CBT examination question using data encryption standard algorithm," *Journal of Science Technology and Education*, vol. 10, no. 4, pp. 195–202, 2022.

[25] M. Haytom, C. Rosenberger, C. Charrier, C. Zhu, and C. Regnier, "Identity verification and fraud detection during online exams with a privacy compliant biometric system," in *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications*, 2020, pp. 451–458, doi: 10.5220/0009874104510458.

[26] P. Sharma, K. Agarwal, and P. Chaudhary, "E-learning platform security issues and their prevention techniques : a review," *International Journal of Advance Scientific Research and Engineering Trends*, vol. 6, no. 8, pp. 51–59, 2021.

[27] L. O. Akingbade and B. E. Eze, "Enhanced computer based examination system with fingerprint authentication," *International Journal of Advances in Engineering and Management (IJAEM)*, vol. 4, no. 11, pp. 64–70, 2022.

[28] M. M. Babitha, C. Sushma, V. K. Gudivada, and others, "Trends of artificial intelligence for online exams in education," *International Journal of Early Childhood Special Education*, vol. 14, no. 01, pp. 2457–2463, 2022.

[29] A. M. Al-Ghonmein and K. G. Al-Moghrabi, "The potential of ChatGPT technology in education: advantages, obstacles and future growth," *IAES International Journal of Artificial Intelligence*, vol. 13, no. 2, pp. 1206–1213, Jun. 2024, doi: 10.11591/ijai.v13.i2.pp1206-1213.

[30] P. A. Patil, A. D. Jha, R. S. Maheshwari, and M. Pandey, "Online exam system with secured approach," *International Journal of Research in Engineering, Science and Management*, vol. 4, no. 12, pp. 87–89, 2021.

[31] A. R. Sunday, I. Idris, H. A. Zubairu, S. O. Etuk, and I. M. Kolo, "Biometry, encryption and spyware (BES): a multi-factor security and authentication mechanism for JAMB E- examination," *International Journal of Applied Information Systems (IJAIS)*, vol. 12, no. 32, pp. 17–26, 2020.

[32] F. Al-Hawari, M. Alshawabkeh, H. Althawbih, and O. Abu Nawas, "Integrated and secure web-based examination management system," *Computer Applications in Engineering Education*, vol. 27, no. 4, pp. 994–1014, Jul. 2019, doi: 10.1002/cae.9.

[33] A. Nurpeisova *et al.*, "Research on the development of a proctoring system for conducting online exams in Kazakhstan," *Computation*, vol. 11, no. 6, Jun. 2023, doi: 10.3390/computation11060120.

[34] S. Ally, "Review of online examination security for the moodle learning management system," *International Journal of Education and Development using Information and Communication Technology (IJEDICT)*, vol. 18, no. 1, pp. 107–124, 2022.

[35] A. C. M. Nafrees and R. K. A. R. Kariapper, "Application of online management information system to the examination department, state Universities in Sri Langka," *Journal of Critical Reviews*, vol. 07, no. 12, pp. 4703–4712, 2020.

[36] T. Waradkar, M. Panvalkar, T. Kamble, and S. Agrawal, "E-examination system," *International Journal of Research in Engineering, Science and Management*, vol. 2, no. 4, pp. 82–85, 2019.

[37] L. Mseteka, J. Phiri, and S. Tembo, "Web and mobile examination results dissemination and verification system using encryption and cryptographic hash functions: a case of TEVETA," *International Journal of Future Computer and Communication*, vol. 8, no. 1, pp. 16–23, Mar. 2019, doi: 10.18178/ijfcc.2019.8.1.533.

[38] A. Suleiman and N. Nachandiya, "Computer based testing (CBT) system for GST exams in Adamawa State University, Mubi," *Asian Journal of Research in Computer Science*, pp. 1–11, Nov. 2018, doi: 10.9734/ajrcos/2018/v2i124776.

[39] T. Zebua, "Encoding the record database of computer based test exam based on spritz algorithm," *Lontar Komputer : Jurnal Ilmiah Teknologi Informasi*, May 2018, doi: 10.24843/LKJITI.2018.v09.i01.p06.

[40] E. Sankar and B. S. Subramanian, "Web based design for academic management system and e-learning portal," *Elixir Computer Engineering*, vol. 115, pp. 49849–49853, 2018.

BIOGRAPHIES OF AUTHORS

Ali M. Al-Ghonmein is an assistant professor at the Department of Computer Information Systems (CIS), Al-Hussein Bin Talal University (AHU), Jordan. He received his bachelor's degree in computer science (2004), a master's degree in CIS (2008), and a doctorate in management information systems (MIS) (2018). His research interests include information retrieval, decision support systems, and cloud computing (CC). He can be contacted through his email address: ali.m.alghonmein@ahu.edu.jo.

Yahia Alemami earned his bachelor's degree in computer science from AHU, Jordan, in 2005, and his master's degree in computer engineering from Anadolu University, Turkey, in 2012. In 2024, he completed his doctorate in computer science in Malaysia. His research interests include cryptography, information security, and cloud security, with additional interests in e-learning. He can be contacted at email: yehea_m@ahu.edu.jo.

Khaldun G. Al-Moghrabi is an assistant professor at the Department of CIS, AHU, Jordan. He received his bachelor’s degree in CIS from AHU (2006) and his master’s degree in CIS from the Middle East University in Jordan (2009). In 2018, he earned his doctorate degree in MIS from OIU, Sudan. His research interests include e-learning, decision support systems, database systems, CC, big data and the IoT. He can be contacted through his email address: khaldun.g.moghrabi@ahu.edu.jo.

Saleh Atiewi received the B.Sc. degree in computer science from Al-Isra University, Amman, Jordan, in 1999, the master degree in internet technology from the Wollongong University, Wollongong Australia, in 2004, and the Ph.D. degree in computer science from Tenaga Nasional University, Putrajaya, Malaysia, in 2017 Since 2004, he has been with Al Hussein Bin Talal University, Maan, Jordan, where he is currently an assistant professor with the Department of Computer Science. He is currently vice dean of scientific research and postgraduate studies. His research interests are in the areas of network security, cloud computing and internet of things. He can be contacted at email: saleh@ahu.edu.jo.