ISSN: 2182-2069 / E-ISSN: 2182-2077

Ensuring the Security of an Internet-based E-learning System through the Use of Integrated Encryption Methods

Sanobar Shadmanova[1*], Nodir Karimov[2], Mukaddaskhon Taylanova[3], Mamurakhon Asrorkhujaeva[4], Umida Mavlyanova[5], Shukriya Nazirova[6], Yulia Isaeva[7], and Zulfiya Pardaeva[8]

[1*]Tashkent State University of Oriental Studies, Uzbekistan.
shadmanova.sanobar@gmail.com, https://orcid.org/0009-0009-6274-2636

[2]Tashkent State University of Oriental Studies, Uzbekistan.
nodir-karimov@list.ru, https://orcid.org/0000-0001-5127-8713

[3]Tashkent State University of Oriental Studies, Uzbekistan.
muqaddas_93@mail.ru, https://orcid.org/0009-0004-6766-188X

[4]Tashkent State University of Oriental Studies, Uzbekistan.
mamurakhonasrorkhujaeva@gmail.com, https://orcid.org/0009-0000-8136-1489

[5]Tashkent State University of Oriental Studies, Uzbekistan.
mavlyanovaumida@mail.ru, https://orcid.org/0000-0002-5941-1336

[6]Tashkent State University of Oriental Studies, Uzbekistan.
doston088@mail.ru, https://orcid.org/0000-0002-8145-9918

[7]Jizzakh State Pedagogical University, Uzbekistan.
yuliya_4265@mail.ru, https://orcid.org/0000-0001-6597-6221

[8]Jizzakh State Pedagogical University, Uzbekistan.
zulfiyapardaeva@jspi.uz, https://orcid.org/0000-0002-7554-5908

Received: July 18, 2024; Revised: August 26, 2024; Accepted: September 27, 2024; Published: November 30, 2024

Abstract

Most schools have used information technology (IT) to enhance and advance their various educational methodologies to attract more learners. Institutions have implemented IT to facilitate E-learning and mobile learning, enhancing the cost and versatility of educational offerings. Most educational institutions are providing online instruction using technology such as cloud computing (CC) and networking. Educational institutions have established their own E-Learning Systems (ELS) to facilitate online learning, enabling remote education. However, ELS must confront several security concerns related to hacks and data breaches via unauthorized entry. Also, a novel idea of Internet-based ELS architecture has emerged to enhance service proximity to the customer. This research presents a novel CC and Internet-based ELS system. This study proposed the implementation of Integrated Encryption Methods (IEM), which incorporates two encryption algorithms, Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES), to meet the safety and latency requirements for communication among the CC and the ELS. The suggested

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 4 (November), pp. 389-400.
DOI: *10.58346/JISIS.2024.I4.024*

*Corresponding author: Tashkent State University of Oriental Studies, Uzbekistan.

technique explicitly extends learning material from the CC to the network's boundary. It enhances the effectiveness of instructional data analysis, alleviates the computational cost of encryption on users' devices by delegating some of the encryption workload to CC servers, and offers limited access to educational material via the encryption of courses and examinations using IEM. Security research indicates that the proposed approach can accomplish information privacy, precise access management, and resistance to conspiracy. Performance studies illustrate the efficacy of the proposed framework, particularly regarding IEM computational costs.

Keywords: Encryption, E-learning, Cloud, Internet, Security, RSA, AES.

1 Introduction and Related Works

E-learning involves students using the web and other Internet technologies to augment educational and instructional experiences. E-learning users often concentrate on the advantages derived from e-learning, which serves the objective of education (Alenezi, 2020). Numerous ELS started IT deployment without a care strategy or comprehension of the associated security issues. E-learning is a contemporary approach that relies on the Internet for its operation. The Internet has evolved into a platform for ELS. E-learning growth has resulted in novel methods and chances for learning. The novel pedagogical approaches have integrated into human existence, facilitating pupils' academic success (Ayu, 2020; Al Rawashdeh et al., 2021).

The Coronavirus pandemic has caused unparalleled disruptions in worldwide educational systems. According to current data from the UNESCO Institute for Statistics, almost 1.45 billion learners have been affected by the closure of schools and institutions worldwide. Education specialists concurred that post-COVID-19 education would differ significantly from its predecessor, particularly due to the advent of a highly mechanized infrastructure using CC and artificial intelligence technologies (Grewenig et al., 2021). Significant and fundamental alterations in educational patterns, methodologies, trends, and policies are anticipated to apply to both general and higher education levels. Indicators of these transformations are already manifesting. One of the most significant shifts in education in the post-COVID-19 period has begun, and researchers have started to explore certain aspects of it. There is a significant upward tendency to use sophisticated technologies to develop more platforms and sites for different educational levels, particularly after their efficacy during the first pandemic outbreak (Bose & Sharma, 2023; Balaji et al., 2022).

Over time, ELS has garnered significant attention due to its extensive applicability in remote education. A substantial volume of data has consistently been sent among learners, examiners, and professors requiring private interchange of this information (Ruzibaeva et al., 2024). E-learning, facilitated by the Internet, has similarly attracted significant illicit activities, such as security concerns, which have adversely impacted the efficacy of information exchange and management (Halim et al., 2024). ELS must be secure to safeguard the sharing process from various security threats—the examination materials, quizzes, answer papers, and tests. The security of ELS necessitates implementing authentication techniques for users, CC servers, or trustworthy servers, along with session key generation protocols that generate keys required for designated periods such as examinations, seminars, or courses (Alassery, 2021). There is a need to uphold trust and authenticity levels to facilitate routine legitimacy assessments for pupils. To guarantee the security and dependability of ELS, a safety evaluation is conducted to identify the merits and demerits of security frameworks (Kurbanazarova et al., 2024).

Fog computing (FC) is an innovative concept that extends CC to the network's edge, providing applications in proximity to customers and end-users. Despite the abundant availability of such apps, they remain deficient in essential data security measures. Developers lack sufficient alternatives that can be thoroughly evaluated (Ibrahim et al., 2020). Data encryption is regarded as one of the most prevalent methods to safeguard data confidentiality and safety. Two stages of the flexible and adaptive extensible model are proposed, whereby the device continuously chooses an encryption technique depending on the rate of access to the encrypted information. Upon consistent data access, the selected model will then identify the suitable and efficient procedure with minimized supplementary complexity. In the subsequent phase, by determining the encryption key size, the framework will use a customized method to assess the requisite security level (Eljak et al., 2023).

The cryptographic method employs a more robust code to encrypt more delicate data dynamically. A more concise code may safeguard routine or less critical information, shielding the FC node from cryptographic depletion. Consequently, CC storage is economical for providing services to manage, evaluate, and store information. The CC network design poses challenges in ensuring compliance with certain standards of IoT systems, such as location-based services, accessibility, and power efficiency. CC seeks to offer rapid, location-aware internet connectivity by integrating diverse devices, including laptops, routers, and mobile phones, dispersed over many geographical areas as CC nodes.

Security hazards in ELS are issues that might negatively impact the security of end users and their information, as well as pertain to user identification, authorization, and privacy. Insecure usernames and passwords for ELS platforms may result in users losing access to these platforms and jeopardizing their private, business, and sensitive transaction data, which unauthorized individuals might employ. Insecure systems may be susceptible to blocking attacks, in which an attacker targets a user's electronic learning material and gains access to ELS materials, as well as flooding attacks, where an adversary inundates the ELS platform with fraudulent requests using a login ID, resulting in the user losing access time (Malhi et al., 2020; Dinesh et al., 2023; Aminah, 2015).

Besides user authentication, there are worries about manipulating user operation processes, which might compromise data patterns and hinder social behavior analysis, threatening user privacy. In addition to user identification and authorization, private details protection, and data reliability, e-learning safety should also address awareness, legitimacy of learning materials, seamless accessibility, geographical privacy, online rights, and user invisibility (Sudipa et al., 2022; Kumar et al., 2019). Accomplishing this will satisfy security requirements like availability, integrity, secrecy, authenticity, confidentiality, and precision. Authors in (Bhatia & Maitra, 2018) used antivirus programs, including Netsparker, to assess vulnerabilities in ELS platforms and offered strategies to enhance security.

Despite the proliferation of e-assessment, which employs integrated IT to facilitate assessment procedures throughout its life cycle in ELS, it confronts three primary threats: identity abuse, information leakage, and fraudulent modification. In an e-assessment period, identity theft may occur if an attacker impersonates the legitimate ELS user being evaluated; the transmission of private and delicate data may expose personal information. As e-assessment and ELS information are maintained in databases, they are susceptible to modification, posing challenges to students and educators over data integrity. The difficulties may be examined and addressed from the educational viewpoint, which considers the scenarios and challenges faced by learners and instructors, and the technological architectural viewpoint, which focuses on securing the information system that supports the e-assessment methods (Garg & Goel, 2022; A Sa'di et al., 2021).

As stated in (Asis & Jarin, 2023), the ELS and its supporting infrastructure must be assessed for threats and vulnerabilities to ensure the integrity of later technical remedy analysis and security procedure audits conducted by financial organizations and payment systems. Cyber-trust confers legal importance to the public sharing of documents online in ELS contexts, therefore aiding in mitigating cyber assaults and cyber-espionage (Otoom et al., 2024).

Network Clock Synchronization (NCS) offers a regulated cyber-trust guarantee for ELS via three tiers of trust parameters extended to the public Internet in conjunction with a standalone NCS source. The three levels of trust parameters are fundamental elements that define a legitimate user's attributes, grounded on five trustworthiness traits: intended, subjective, quantifiable, dynamic, and selectively passed (Rantalaiho, 2024). A standalone NCS source is utilized because built-in time coordinating modules and synchronization network segments reliant on the network period protocol may be compromised, jeopardizing end-user and ELS platform encryption keys and electronic signatures while threatening the entire public key infrastructure that secures communication.

Authors in (Korać et al., 2022) suggested that, for ELS security, denial-of-service attacks and illegal logins may be mitigated by single sign-on authorization. Using trust credentials and biometric authentication resolves issues related to data assessment during login and inside course material. Virtualization tools and secured SSL/TLS channels via the online management panel address architectural difficulties related to information transmission channels and access restrictions (Wu, 2024).

2 Internet-based E-learning System through the Use of Integrated Encryption Methods

This section delineates the system architecture and articulates the security framework. The framework categorizes the shared ELS information into two classifications: data category 1 (F1), encompassing course materials such as presentation slides of lessons, instructional videos, research papers, documents, and audio recordings; and data category 2 (F2), which includes examination materials like quizzes, tests, evaluations, and examinations.

2.1 Architecture of the Proposed System

Figure 1 depicts the novel secure internet-based ELS architecture, including four items: CC servers, FC servers, teachers, and learners.

- **Enrollment Server (ES):** The CC server comprises a smart agent known as the ES, a completely trustworthy entity. ES is responsible for creating system settings, key pairs for FC servers, and private and feature keys for every learner.
- **Fog Servers (FS):** FSs are geographically dispersed servers situated near users, providing various services such as latency reduction, support for applications in real-time, and protection of secrecy.

Upon receiving the information, the FS deciphers F1 using the common secret key and examines the information it contains. Subsequently, FS re-encrypts the shared F1 using the IEM technique. Only authorized students with registered IDs may access this information and benefit from the delivered course. For instance, if the data processed by the FS pertains to a Java course, the roster of learner identities comprises those enrolled in the computing-related college as identified by the FS, along with criteria specified by the instructor, such as possession of a Java certificate, completion of over ten programming modules, and fewer than two examination passes. The FS then archives the re-encrypted

F1 and F2 in the cloud while retaining local memory for information pre-processing. Furthermore, the FS might implement the profile pairing algorithm for two individuals without the pertinent information. After that, the FS transmits the matching results to the relevant users to foster social relationships.

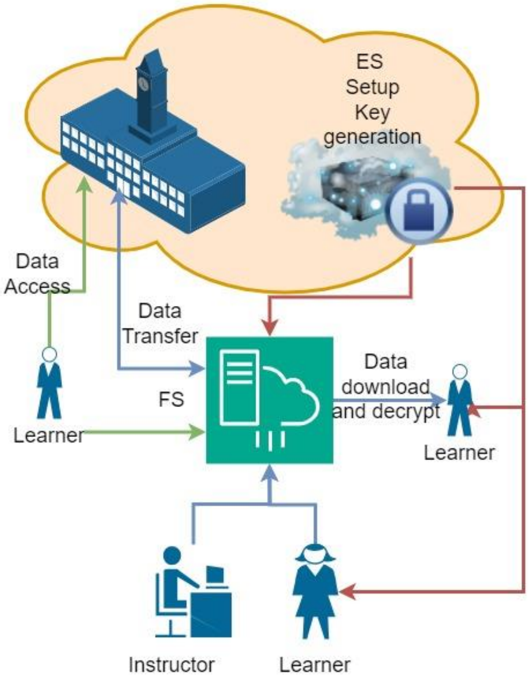

Figure 1: Secure Internet-based ELS Architecture

- **Instructor:** They are the originators of data and have the authority to view, edit, and destroy prior versions of data files. The educator intends to provide instructional information to permitted pupils. They encrypt educational materials (courses, examinations, etc.) using the characteristics of a designated set of students (classroom) and transfer all files to external servers. The educator classifies the disseminated material into two categories: F1, including the course and its associated data (title, sections, modules, etc.), and F2, which pertains to the examination or assessment connected to course F1. F1 has been encrypted with a common key in conjunction with the FS, whereas F2 is encrypted using AES with broad characteristics specified by the instructor. Concurrently, educators with identical social learning profiles may create trapdoors and establish social connections based on their areas of expertise.
- **Learners:** They are the recipients of the ciphertexts and possess the capability to decrypt the information based on their authorization rights: they can decode F1 if they are the designated recipient specified by the FS, and they may examine F2 if their characteristics comply with the access rules established by the instructor.

2.2 Security Framework

In the proposed framework, as a reliable enrollment authority, the ES meticulously gives secret keys to every learner based on their qualities. The FS are presumed trustworthy; nevertheless, their security vulnerabilities vary based on the data category. The FS performs pre-processing operations for F1 (course) to establish the access list of permitted students required for F1's encryption. However, they are curious about the substance of F2 examinations. Some hostile students may attempt to acquire unlawful

E-learning data, particularly by cooperating with their peers to access examinations. According to the security mentioned above postulate for each object, the e-learning transfer scheme presented in this article must be developed to include the following safety components.

1) Information Privacy

Unregistered students who are not the authentic recipients designated by the instructor should be barred from attending the course and the examination. The student must not visit the re-encrypted course until enrolled on the permitted students' list established by the FS.

2) Precise Access Management and Data Security

Precise access control has been provided for educational data produced by educators. Two tiers of security courses (SC) have been examined:

- **SC Stage I:** At this stage, learners may access the courses only if their IP addresses are included in the list specified by the FS.
- **SC Stage II:** At this stage, learners may access the lessons and examinations only if they meet two criteria: their true identities are listed by the FS, and their characteristics comply with the access policies established by instructors to obtain the corresponding examination. Given that the FS can pre-process the course material, we want to ensure SC stage I on the FS and SC stage II for the learners as end users.

3) Resistance to Conspiracy

If none of the learners' qualities in the set can fulfill the conditions for access to the ciphertexts, access to the ciphertext should be unsuccessful.

2.3 Integrated Encryption Methods (IEM)

The increasing use of CC in ELS necessitates the assurance of secure and efficient connectivity among devices. To attain solid security and reduce latency, IEM integrates two recognized encryption algorithms: RSA and AES. This integration fulfills the security and latency criteria of CC-based communication. The integration of RSA and AES amalgamates the advantages of both algorithms, yielding a balanced strategy for security and effectiveness, especially in an internet-based ELS context where data secrecy and rapid transmission are essential.

- RSA provides robust security for encrypting and transmitting private information, including the AES key, ensuring that even if the transmission route is compromised, the AES key remains safeguarded.
- After the safe exchange of the key via RSA, AES efficiently encodes and decrypts the ELS information, mitigating latency issues.

The following outlines the sequential execution of IEM:

Step 1: Key Generation (RSA): The FS produces a public-private key pair for the RSA algorithm. The public key is sent to all authorized devices inside the ELS, including students, teachers, and administrators.

Step 2: AES Key Generation: Each device produces an arbitrary symmetric AES key designated for the encryption of the E-learning material (e.g., documents, examinations, videos). This AES key is compact and efficient, facilitating rapid decoding and encryption of substantial data volumes.

Step 3: AES Key Encryption (RSA): The device-generated AES key is then encrypted using the FC's RSA public key. Encrypting the AES key using RSA guarantees the safe transport of the AES key over the network, preventing illegal interception.

Step 4: Secure Key Transfer: The encrypted AES key is sent to the FS, which employs its RSA private key for decryption. Currently, both the device and the server possess the same AES key.

Step 5: Data Encryption and Transmission (AES): Upon successfully exchanging the AES key, the device and CC server use the AES algorithm for all ensuing connections. The ELS information, including course materials, quizzes, and student data, is secured using AES and sent between devices and the FS.

Step 6: Decryption and Access: Upon receiving data from the cloud, a device employs the same AES key to decrypt the content, guaranteeing that only authorized devices with the requisite AES key may access the data.

Illustrative Application in E-Learning

Upon a learner's login to the ELS platform, their device, and the FS initiate the RSA-based key exchange procedure. Upon the safe exchange of the AES key, all interactions, including downloading learning modules and submitting assignments, are encrypted using AES, guaranteeing rapid access to resources and secure communication. Educators downloading new materials or conducting real-time collaborative sessions (e.g., online examinations in virtual classrooms) benefit from low-latency AES encryption, which guarantees a seamless and secure educational experience. The IEM, integrating RSA and AES, provides a safe and fast method for controlling communication across CC devices in an ELS. IEM employs RSA for key exchange and AES for data encryption, providing strong security against unwanted access while preserving low-latency performance, which is essential for smooth and secure E-learning experiences.

3 Results and Discussion

The experiments are performed on a Windows operating system equipped with an Intel Core i5 CPU operating at 2.5 GHz and 16GB of RAM, utilizing the cpabe toolbox founded on the Pairing-Based Cryptography library (Pairing-Based Cryptography), a free software package that executes the fundamental mathematical operations of cryptosystems and the IEM algorithm.

The outcomes are assessed during the encryption and decryption procedures. It has been presumed that the sizes of both F1 and F2 fluctuate between 1 MB and 100 MB throughout the encryption and decryption processes. The volume of material is contingent upon the nature of the course and examination, which may include video, audio, or electronic document formats. During the data encryption stage, computational operations are performed by the instructor to encrypt F2 according to the learners' characteristics and by the FS to encrypt F1 based on the identity of the learners.

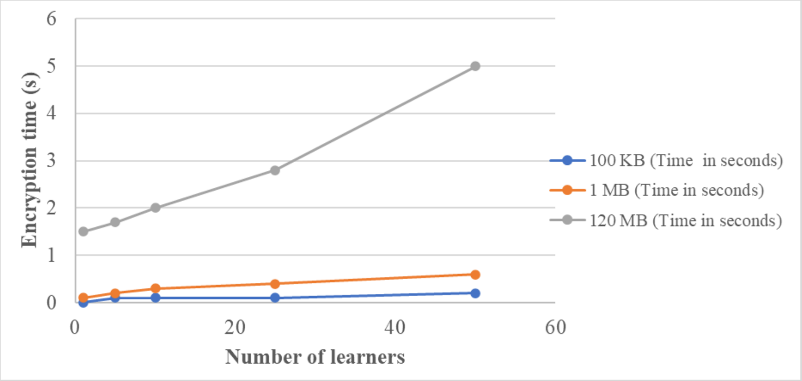

Figure 2: Encryption Time / Computational Cost Versus the Number of Learners for ELS Using IEM

Figure 2 depicts the encryption time / computational cost versus the number of learners for ELS using IEM. Figure 2 illustrates the time required to encrypt various file sizes (100 KB, 1 MB, and 120 MB) as the number of learners increases. For file sizes of 100 KB, the encryption duration remains negligible, at 0.1 seconds with 25 learners, and increases somewhat to 0.2 seconds with 50 learners. The encryption duration progressively escalates for bigger file sizes, such as 1 MB, reaching 0.6 seconds with 50 learners. The most significant time expenditure occurs with 120 MB data when the encryption duration escalates from 1.5 seconds for one student to 5 seconds for fifty learners. This suggests that small file sizes may be managed effectively irrespective of the student count; however, bigger files impose considerable computational expenses as the learner count increases, which is crucial for scalability in ELS using IEM.

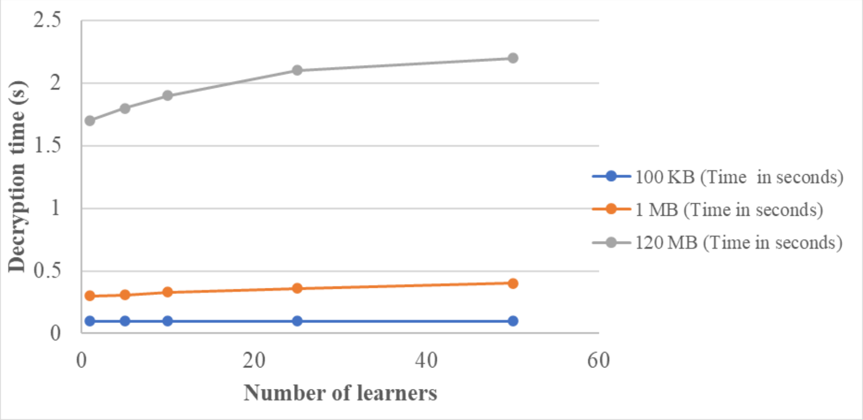

Figure 3: Decryption Time / Computational Cost Versus the Number of Learners for ELS Using IEM

Figure 3 portrays the decryption time / computational cost versus the number of learners for ELS using IEM. Figure 3 illustrates the time required to decrypt different file sizes (100 KB, 1 MB, and 120 MB) as the number of learners increases. For files of 100 KB, the decryption duration consistently stays at 0.1 seconds, irrespective of the number of learners. The decryption time for 1 MB of data increases slightly from 0.3 seconds with one learner to 0.4 seconds with 50 learners, suggesting a negligible computational expense. The decryption time for 120 MB data increases significantly from 1.7 seconds with one student to 2.2 seconds with fifty learners. This indicates that the decryption of smaller files remains mostly unchanged regardless of the number of learners; however, bigger files exhibit a little rise in decryption time with additional learners, highlighting the escalating computational burden in a multi-learner context.

4 Conclusion

This study introduces an innovative CC and Internet-based ELS. This work proposes the implementation of IEM, which combines two encryption algorithms, RSA and AES, to fulfill the safety and latency criteria for communication between the CC and the ELS. The proposed method explicitly expands the learning material from the CC to the network's periphery. It improves the efficacy of instructional data analysis, reduces the computational burden of encryption on users' devices by transferring some of the encryption strain to cloud computing servers, and provides restricted access to educational resources via the encryption of courses and assessments with IEM. The security study suggests that the methodology may provide information privacy, accurate access control, and resilience against collusion. Performance studies demonstrate the effectiveness of the proposed architecture, especially with IEM computational expenses. Results illustrate the time required to encrypt various file sizes (100 KB, 1 MB, and 120 MB) as the number of learners increases. Encryption time suggests that small file sizes may be managed effectively irrespective of the student count; however, bigger files impose considerable computational expenses as the learner count increases, which is crucial for scalability in ELS using IEM.

References

[1] A Sa'di, R., Abdelraziq, A., & A Sharadgah, T. (2021). E-Assessment at Jordan's Universities in the Time of the COVID-19 Lockdown: Challenges and Solutions. *Arab World English Journal (AWEJ) Special Issue on Covid-19*, 37-54. https://dx.doi.org/10.24093/awej/covid.3

[2] Al Rawashdeh, A. Z., Mohammed, E. Y., Al Arab, A. R., Alara, M., & Al-Rawashdeh, B. (2021). Advantages and disadvantages of using e-learning in university education: Analyzing students' perspectives. *Electronic Journal of E-learning*, *19*(3), 107-117. https://doi.org/10.34190/ejel.19.3.2168

[3] Alassery, H. A. A. F. (2021). Securing fog computing for e-learning system using integration of two encryption algorithms. *Journal of Cybersecurity*, *3*(3), 149-166. https://doi.org/10.32604/jcs.2021.022112

[4] Alenezi, A. (2020). The role of e-learning materials in enhancing teaching and learning behaviors. *International Journal of Information and Education Technology*, *10*(1), 48-56. https://doi.org/10.18178/ijiet.2020.10.1.1338

[5] Aminah, K. L. (2015). Implementation of electronic learning in the country and world with investigation of its advantages and problems. *International Academic Journal of Science and Engineering*, *2*(2), 1–8. https://iaiest.com/iaj/index.php/IAJSE/article/view/1282

[6] Asis, J. A. M., & Jarin, S. A. (2023). Management of Learning of Highly Accredited and Ranked Secondary Schools and Universities of ASEAN Countries During Covid–19 Pandemic. *PSU Journal of Advanced Studies*.

[7] Ayu, M. (2020). Online learning: Leading e-learning at higher education. *The Journal of English Literacy Education: The Teaching and Learning of English as a Foreign Language*, *7*(1), 47-54. https://doi.org/10.36706/jele.v7i1.11515

[8] Balaji, R., Logesh, V., Thinakaran, P., & Menaka, S.R. (2022). E-Learning Platform. *International Academic Journal of Innovative Research*, *9*(2), 11–17. https://doi.org/10.9756/IAJIR/V9I2/IAJIR0911

[9] Bhatia, M., & Maitra, J. K. (2018, September). E-learning platforms security issues and vulnerability analysis. In *2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES)* (pp. 276-285). IEEE. https://doi.org/10.1109/CCTES.2018.8674115

[10] Bose, S., & Sharma, H. (2023). Public Spending on School education in Delhi: The Gaps that Covid-19 Highlights. *National Coalition for Education, http://nceindia.org.in/wp-content/uploads/2023/03/Public-Spending-Delhi. pdf*.

[11] Dinesh, E., Sivakumar, M., Rajalakshmi, R., & Sivakumar, P. (2023). Trust based access control with hybrid cryptographic algorithm based data security on cloud for e-learning application. *Journal of Intelligent & Fuzzy Systems*, *45*(5), 7563-7573. https://doi.org/10.3233/JIFS-224287

[12] Eljak, H., Ibrahim, A. O., Saeed, F., Hashem, I. A. T., Abdelmaboud, A., Syed, H. J., & Elsafi, A. (2023). E-learning based Cloud Computing Environment: A Systematic Review, Challenges, and Opportunities. *IEEE Access*, *12*, 7329-7355. https://doi.org/10.1109/ACCESS.2023.3339250

[13] Garg, M., & Goel, A. (2022). A systematic literature review on online assessment security: Current challenges and integrity strategies. *Computers & Security*, *113*, 102544. https://doi.org/10.1016/j.cose.2021.102544

[14] Grewenig, E., Lergetporer, P., Werner, K., Woessmann, L., & Zierow, L. (2021). COVID-19 and educational inequality: How school closures affect low-and high-achieving students. *European economic review*, *140*, 103920. https://doi.org/10.1016/j.euroecorev.2021.103920

[15] Halim, M., Tahiri, A., Ghzizal, Y. E., Adadi, N., & Chenouni, D. (2024). Web Service-Oriented E-learning: Proposition of Semantic Approach to Discover Web Services Related to the E-learning System. *Journal of Internet Services and Information Security, 14*(2), 1-17. https://doi.org/10.58346/JISIS.2024.I2.001

[16] https://crypto.stanford.edu/pbc/

[17] Ibrahim, T. S., Saleh, A. I., Elgaml, N., & Abdelsalam, M. M. (2020). A fog based recommendation system for promoting the performance of E-Learning environments. *Computers & Electrical Engineering*, *87*, 106791. https://doi.org/10.1016/j.compeleceng.2020.106791

[18] Korać, D., Damjanović, B., & Simić, D. (2022). A model of digital identity for better information security in e-learning systems. *The Journal of Supercomputing*, 1-30. https://doi.org/10.1007/s11227-021-03981-4

[19] Kumar, B. V., Dhanapal, A., & Tharmar, K. (2019). An Analysis of Online Courses: With Special Reference to SWAYAM. *Indian Journal of Information Sources and Services*, *9*(S1), 19-22. https://doi.org/10.51983/ijiss.2019.9.S1.572

[20] Kurbanazarova, N., Shavkidinova, D., Khaydarov, M., Mukhitdinova, N., Khudoymurodova, K., Toshniyozova, D., & Alimova, R. (2024). Development of speech recognition in wireless mobile networks for an intelligent learning system in language education. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15*(3), 298-311. https://doi.org/10.58346/JOWUA.2024.I3.020

[21] Malhi, M. S., Iqbal, U., Nabi, M. M., & Malhi, M. A. I. (2020). E-learning based on cloud computing for educational institution: Security issues and solutions. *International Journal of Electronics and Information Engineering*, *12*(4), 162-169. https://doi.org/10.6636/IJEIE.202012_12(4).03

[22] Otoom, A. A., Atoum, I., Al-Harahsheh, H., Aljawarneh, M., Al Refai, M. N., & Baklizi, M. (2024). A collaborative cybersecurity framework for higher education. *Information & Computer Security*. https://doi.org/10.1108/ICS-02-2024-0048

[23] Rantalaiho, V. (2024). *Technical implementation and operational enhancements of a vulnerability management tool in an organization*. Bachelor's Thesis.

[24] Ruzibaeva, N., Makhmaraimova, S., Khaydarov, I., Mukhitdinova, B., Ne'matova, Y., Fayziyeva, K., & Mirzakhmedova, K. (2024). Application of wireless sensors in the design of smart learning of the English language utilizing Zigbee network technology. *Journal of Wireless*

Mobile Networks, Ubiquitous Computing, and Dependable Applications, 15(3), 125-135. https://doi.org/10.58346/JOWUA.2024.I3.009

[25] Sudipa, I.G.I., Aditama, P.W., & Yanti, C.P. (2022). Developing Augmented Reality Lontar Prasi Bali as an E-learning Material to Preserve Balinese Culture. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 13*(4), 169-181. https://doi.org/10.58346/JOWUA.2022.I4.011

[26] Wu, Z. (2024). Integrating Biotechnology Virtual Labs into Online Education Platforms: Balancing Information Security and Enhanced Learning Experiences. *Natural and Engineering Sciences*, *9*(2), 110-124. https://doi.org/10.28978/nesciences.1569211

Authors Biography

Sanobar Shadmanova, an accomplished scholar from Tashkent State University of Oriental Studies, Sanobar Shadmanova specializes in the intersection of education and technology, focusing on innovative pedagogical practices.

Nodir Karimov, a graduate of Tashkent State University of Oriental Studies, combines his expertise in education with technology, exploring ways to enhance learning experiences through digital tools.

Mukaddaskhon Taylanova, is a dedicated researcher at Tashkent State University of Oriental Studies, where she investigates the role of technology in modern education, aiming to improve student engagement.

Mamurakhon Asrorkhujaeva a passionate educator from Tashkent State University of Oriental Studies, Mamurakhon Asrorkhujaeva focuses on integrating technology into educational frameworks to foster better learning outcomes.

Umida Mavlyanova, affiliated with Tashkent State University of Oriental Studies, emphasizes the importance of technology in education, striving to develop innovative solutions for contemporary teaching challenges.

Shukriya Nazirova, is a researcher at Tashkent State University of Oriental Studies, where she studies the impact of technological advancements on educational methodologies and practices.

Yulia Isaeva, from Jizzakh State Pedagogical University, integrates her background in education with technology to promote effective teaching strategies and enhance student learning.

Zulfiya Pardaeva, affiliated with Jizzakh State Pedagogical University, focuses on educational technology, aiming to leverage digital tools to improve instructional methods and learning outcomes.