ISSN: 2093-5374 / E-ISSN: 2093-5382

Blockchain-Integrated Privacy-Preserving Distributed Mobile E-Learning Architectures for Secure and Autonomous Student Data Management

Odiljon Raxmatov[1*], Malohat Narbayeva[2], Nazokat Jurayeva[3], Shakhrizabonu Shamsiyeva[4], Ulugbek Eshqarayev[5], Lenara Islyamova[6], and Matluba Xalmatova[7]

[1*]Fergana State University, Fergana, Uzbekistan; University of Tashkent for Applied Sciences, Tashkent, Uzbekistan. rahmatovodil5@gmail.com, https://orcid.org/0009-0002-5149-746X

[2]Senior Lecturer, Faculty of Foreign Language Education, Department of Higher Education, Tashkent State University of Economics, Tashkent, Uzbekistan. m.narbayeva@tsue.uz, https://orcid.org/0009-0004-5767-8661

[3]Associate Professor, Alfraganus University, Tashkent, Uzbekistan. n.jurayeva@afu.uz, https://orcid.org/0000-0001-6269-6291

[4]Doctoral Researcher, Bukhara State Pedagogical Institute, Bukhara, Uzbekistan. shamsiyevashaxrizabonu@gmail.com, https://orcid.org/0009-0009-5188-7135

[5]Department of Pedagogy and Psychology, Termez University of Economics and Service, Termez, Uzbekistan. ulugbek_eshkarayev@tues.uz, https://orcid.org/0009-0004-1455-3519

[6]Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. s.lenara2101@gmail.com, https://orcid.org/0000-0003-1772-1106

[7]Tashkent State Medical University, Tashkent, Uzbekistan. matlubahalmatova27@gmail.com, https://orcid.org/0009-0007-5332-5123

Received: February 10, 2026; Revised: March 16, 2026; Accepted: May 04, 2026; Published: June 30, 2026

Abstract

The rapid increase in distributed mobile e-learning systems has resulted in numerous security threats, including student data protection, secure access, transparency, and decentralized education management. Traditional cloud-based e-learning systems have been prone to various risks, such as centralization vulnerability, data access violations, identity theft, and lack of scalability in a highly variable wireless learning environment. This paper proposes a blockchain-integrated, privacy-preserving, distributed mobile e-learning architecture for securely and autonomously managing student data. In this framework, blockchain technology will be used for ensuring a decentralized ledger, lightweight cryptography, smart contract-based authentication, and distributed data storage. Blockchain transaction verification, data encryption and sharing, distributed data storage, and smart contract execution are the methodologies utilized by this system to ensure secure academic record and activity management in a mobile environment. The evaluation of the proposed architecture will involve performance measurement of the following parameters: authentication

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 182-195. DOI: *10.58346/JOWUA.2026.I2.010*

*Corresponding author: Fergana State University, Fergana, Uzbekistan; University of Tashkent for Applied Sciences, Tashkent, Uzbekistan.

accuracy, privacy protection capability, transaction processing speed, throughput, and data storage efficiency. It was revealed from experimental studies that the suggested approach provided 98.3% in terms of identification, 97.5% in relation to data privacy protection, and 91.8% concerning storage efficiency compared to other methods, including traditional cloud-based learning systems and previous blockchain-based education platforms. In addition, the suggested system enabled reducing the transaction time to 190 ms and increasing the throughput speed up to 465 transactions per second, which proves its high efficiency and capability of functioning in a distributed wireless environment. Therefore, it can be stated that introducing blockchain technology in distributed mobile e-learning systems enhances the level of privacy, resilience against malicious attacks, traceability, and autonomy in controlling personal information. The introduced concept provides a basis for designing a highly reliable and scalable framework for the future generation of wireless educational communities based on the management of decentralized and reliable data.

Keywords: Blockchain-Based E-Learning, Privacy-Preserving Architecture, Distributed Mobile Learning, Smart Contracts, Secure Student Data Management, Wireless Educational Networks, Decentralized Authentication.

1 Introduction

There has been a paradigm shift in e-learning systems through the proliferation of mobile e-learning platforms, which have led to a revolution in educational processes because of flexibility, real-time accessibility, and location independence. Institutions of higher learning and training, as well as online e-learning systems, make use of distributed mobile learning solutions for facilitating collaborative learning, customization of learning processes, and ongoing engagement (Pal et al., 2025). The increased application of mobile e-learning platforms, however, has posed some threats to data security, privacy, scalability, and trust management in such educational environments (Kavitha, 2024). Student data, including records, behavioral analysis, assessments, and communications, may be stored in centralized cloud storage systems, hence leaving the data susceptible to unauthorized access, breaches, identity fraud, and points of failure (Salendab, 2026). Traditional forms of data and user authentication do not provide effective methods for maintaining data integrity, transparency, and secure data exchanges in decentralized learning environments.

Blockchain has been identified as an ideal platform to overcome the aforementioned challenges because of its inherent qualities. Through the incorporation of blockchain technology into distributed mobile e-learning systems, educational systems will be able to attain secure identity validation for students, reliable academic records management, and autonomous student access control without the complete dependency on central bodies. Further, privacy-preserving technologies such as encryption, smart contracts, and distributed consensus mechanisms are important ways through which privacy can be enhanced without compromising scalability and interoperability within large-scale e-learning setups. Nonetheless, current solutions are characterized by several shortcomings associated with computational cost, delay, resource usage, and efficient privacy management within highly dynamic mobile wireless e-learning systems.

This study presents a blockchain-based privacy-preserving distributed mobile e-learning system that will facilitate secure and autonomous data management among students. This framework incorporates blockchain technology infrastructure, light-weight cryptography, smart contracts authentication, and distributed storage as key technologies for enhancing the security, reliability, and efficiency in wireless mobile educational systems (Sindhu, 2024; Kingdon & Luedke, 2025). The study will contribute

significantly to the body of knowledge through a secure and scalable solution developed specifically for wireless mobile e-learning systems.

Key Contributions

- Presents a blockchain-enabled distributed mobile e-learning framework to provide secure and decentralized management of students' data.
- Offers privacy-assured authentication and access control scheme using smart contracts and efficient cryptographic schemes.
- Provides better data integrity and traceability for academic records using decentralized ledger technology.
- Supports autonomous operations in wireless mobile learning systems with minimum reliance on central servers.

The structure of this research paper is as follows. Section II provides a literature review of the topics blockchain-based e-learning, privacy preservation, and distributed education. Section III deals with the design of the novel blockchain based mobile e-learning system including its methodology, algorithms and mathematical modeling. In Section IV, experimental setup, evaluation of the results, and comparisons are provided. Finally, in Section V, conclusion and future scope of work are discussed.

2 Literature Survey

The use of blockchain technology, distributed learning architectures, and privacy protection systems has attracted much attention in recent years as a result of the increased need for security in current mobile learning systems. Many studies have been conducted regarding the use of secure methods of handling academic data, authenticating, verifying the genuineness of education certificates, and creating trustful learning environments.

In one such study, a systematic review was carried out to investigate the use of blockchain technology for managing the verification of academic certificates (Mubarak et al., 2026). In the study, it was shown that the use of blockchain verification enhances the security, transparency, and genuineness of academic records. Similarly, another research paper suggested the use of blockchain-based systems to prevent certificate forgery (Reginald, 2025; Masood & Faridi, 2021).

There have been some researches which explored the idea of education platforms powered by blockchains and smart learning environments. There was one which created a blockchain integrated mobile platform for educational content sharing, stressing the significance of decentralized trust management in collaborative learning systems (Lincopinis et al., 2025). There was another which proposed the concept of a blockchain-driven smart learning environment where transparent, secure interactions along with autonomous educational management was improved (Verma et al., 2024). Another study made a detailed meta-analysis of blockchain implementation in Education 4.0, suggesting that it makes decentralization, trust creation, and educational data security better (Haque et al., 2023; Wijesekara, 2024).

In any case, privacy preservation and secure data access is an important issue for distributed mobile learning systems. There was one analysis conducted about privacy preservation techniques in mobile-based learning environments, which pointed out some critical issues like the problem of authentication, identification leaks, and centralized vulnerability (Muhammad et al., 2020; Coman et al.,

2025). Privacy, personalization, and trust are vital components in online learning systems, so this study suggested that secure and adaptive learning environments are important for contemporary education platforms (Anwar, 2021). This paper proposed a zero knowledge-proof based intelligent recommendation approach to preserve student data privacy (Yin, 2023).

Access control systems with privacy preservation techniques based on blockchains have also been investigated recently. In addition, K-anonymity, hyper-ledger blockchain, and deep learning were applied in a secure system to store marks of students, which provided better confidentiality and secured processing of academic information (Patel & Patel, 2025). In this research, an access control scheme using blockchain was developed for cloud education systems that enabled trust management and ensured the security of sensitive educational information (Mawgoud et al., 2025).

Distributed and edge-enabled learning systems have turned out to be effective approaches for efficient educational systems. Blockchain-powered secure data sharing schemes were presented in this study within cloud-edge learning systems and exhibited improved distribution resource management and secure educational communication (Murgai et al., 2025). Moreover, deep learning and edge computing were utilized in this research to boost the performance and accessibility of e-learning systems (Mohsen & Munassar, 2025).

Furthermore, research on distributed privacy-preserving learning architectures has become significant within multiagent and federated learning systems. In this regard, it proposed a privacy traceability mechanism utilizing blockchain technology for federated recommender systems to enhance secure distributed learning process (Cai et al., 2023). The current study provided an overview of trusted artificial intelligence within distributed learning environment and emphasized the significance of privacy security frameworks within multiagent systems (Ma et al., 2023).

The comparative analysis of centralized and distributed educational privacy models was done by this study, proving that distributed architectures have higher capabilities than centralized architectures in terms of security, transparency, and fault-tolerance (Lamaazi et al., 2024). This study, therefore, concluded that IoT-enabled ubiquitous learning systems require better privacy preserving models to ensure secure educational interactions within highly connected wireless systems (El-Haggar et al., 2023).

Despite the important contributions made by earlier studies to blockchain technology-enabled educational systems, there exist various unsolved challenges in this area such as high computation cost, lack of scalability, high transaction time delays, and insufficient autonomy-based access control in mobile distributed learning environment. Existing technologies concentrate only on certifying validation techniques or privacy mechanisms separately, neglecting the implementation of decentralized blockchain validation, light weight cryptography, smart contracts, and distributed storages.

Thus, the presented research introduces a privacy-enhancing mobile e-learning system design through the use of blockchain technology, which involves the integration of decentralized ledger technologies, autonomous access controls via smart contracts, cryptographically light protocols, and efficient distributed data storage mechanisms. The developed framework is intended to address the shortcomings of the existing methods of managing student information in wireless mobile learning environments.

3 Proposed Blockchain-Integrated Privacy-Preserving Distributed Mobile E-Learning Architecture

The suggested system proposes a mobile e-learning framework that incorporates blockchain technology, light cryptography, distributed storage, and smart contracts for secure and decentralized access control for student data management in a mobile environment. This approach ensures that students' data will be processed confidentially, transparently, securely, and autonomously managed.

The architecture consists of six major layers:

1. Mobile Learning Layer
2. Authentication and Privacy Layer
3. Blockchain Network Layer
4. Smart Contract Management Layer
5. Distributed Storage Layer
6. Educational Service Provider Layer

The entire workflow starts with students, teachers, or administrative staff accessing the mobile learning system via wireless gadgets. User identity and device identity verifications will be done through light encryption and blockchain-based verification mechanisms. After successful verification, smart contracts will then be employed to manage access control, transaction processing, and learning processes. All the verified transactions will be logged on the blockchain ledger to ensure accountability and data integrity. Meanwhile, all sensitive educational documents will be saved in a distributed database system with encrypted indexing performed on the blockchain ledger.

The method that has been suggested adopts a sequential and safe approach to handling the decentralized mobile e-learning data. During the initial phase of user registration and identity generation, a unique blockchain identity is assigned to each student, tutor, or administrator, who gets a corresponding pair of private and public keys for secure messaging. Then, these credentials get safely stored on the distributed ledger in blockchain. In the next step of secure user authentication, mobile users provide an encrypted authentication request that is verified by the smart contract that rejects any unauthorized access requests. After authentication, the data pertaining to each learner is encrypted using cryptographic techniques, and secure hash functions ensure transaction integrity. Finally, the transactions involving educational activities get transmitted to blockchain nodes for validation. Big educational data and files are kept in distributed storage clouds or edge computing environments, while immutable metadata links are saved using the blockchain system. In addition, the use of autonomous access control based on smart contracts is used to dynamically manage the permissions for sharing these data, ensuring that only authorized parties can access the encryption records. Finally, ongoing monitoring and auditing processes keep clear logs of all activities carried out in the blockchain ecosystem, automatically detecting any tampering attempt or unauthorized manipulation of the data.

In figure 1 depicts the suggested architecture of a decentralized mobile learning platform based on blockchain technology, smart contracts, light cryptography, and distributed storage to secure the management of students' data. The architecture provides privacy protection, secure authentication, transaction verification, access control, and scalable delivery of education services in mobile wireless learning systems.

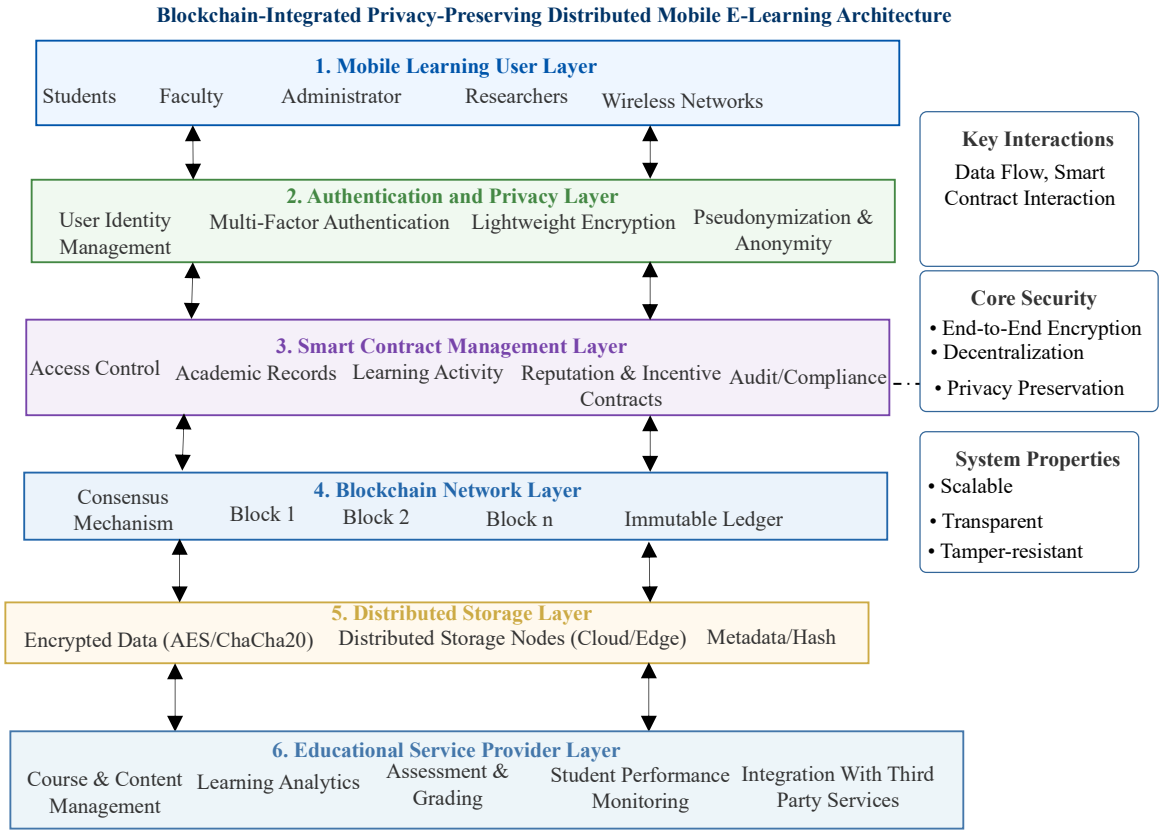

Figure 1: Architecture of blockchain-integrated privacy-preserving distributed mobile e-learning system

Algorithm 1: Blockchain-Based Secure Student Data Management

Input:

- User request U_r
- Student data S_d
- Blockchain node set B_n

Output:

- Secure authenticated access
- Immutable transaction storage
- Privacy-preserved educational data sharing

Step 1: System Initialization

- Initialize blockchain network B_n
- Generate cryptographic key pairs
- Deploy smart contracts

Step 2: User Registration

- Create unique digital identity ID_u
- Store hashed credentials on blockchain

Step 3: Authentication Process

- Receive encrypted login request
- Verify credentials using smart contract rules
- Grant access if verification succeeds

Step 4: Data Encryption

- Encrypt student data using lightweight encryption
- Generate transaction hash values

Step 5: Transaction Broadcasting

- Broadcast encrypted transaction to blockchain nodes
- Nodes validate transaction integrity

Step 6: Consensus Validation

- Execute consensus mechanism
- Append validated block to distributed ledger

Step 7: Distributed Storage Allocation

- Store encrypted files in distributed storage
- Save metadata reference in blockchain

Step 8: Access Management

- Smart contracts validate access permissions
- Provide secure data retrieval for authorized users

Step 9: Audit and Monitoring

- Continuously monitor transactions
- Detect unauthorized modifications

End Algorithm

Algorithm 1 describes a secure blockchain-based architecture for managing student data in mobile-based e-learning platforms. The algorithm includes the processes such as user registration, user authentication, data encryption, transaction verification, and distributed storage through the use of blockchain technology and smart contracts.

3.1 Mathematical Description of the Methodology

User Authentication Function

The authentication verification process is represented as equation 1:

$$A_u = f(ID_u, K_{pub}, K_{priv}) \qquad (1)$$

Where:

- A_u= Authentication result
- ID_u= User identity
- K_{pub}= Public key
- K_{priv}= Private key

Data Encryption Model

Student data encryption is expressed as equation 2:

$$E_d = Enc(S_d, K_s) \quad (2)$$

Where:

- E_d= Encrypted data
- S_d= Student data
- K_s= Symmetric encryption key

4 Results and Discussion

The proposed distributed mobile e-learning platform utilizing blockchain was designed, implemented, and tested in a simulated wireless learning environment ensuring secure autonomous management of student academic data. The implementation comprised blockchain technology, smart contracts, lightweight cryptographic methods, and distributed storage. The programming languages used for the implementation were Python 3.11. The smart contract programming language was Solidity, while the Blockchain Simulator used was Ethereum. Blockchain testing was performed using Ganache and Metamask, while distributed storage was provided by IPFS. For the wireless environment simulation and evaluation, NS-3 Simulator and MATLAB R2024a were used. All experiments were performed on an Intel Core i7 machine having 32 GB RAM and operating with Ubuntu Linux. In particular, a simulated mobile learning environment database having 120,000 entries of 5,000 students was considered consisting of authentication requests, course access logs, transactions, and encrypted records. The experimental setup parameters comprised a blockchain block size of 2 MB, number of blockchain nodes of 50, encryption key size of 256 bits, Proof-of-Authority consensus method, and transaction batch size of 500.

4.1 Performance Metrics and Formulae

The proposed model was evaluated using five major performance metrics.

Authentication Accuracy: Authentication accuracy measures the correctness of user verification are shown in equation 3.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (3)$$

Data Privacy Preservation Rate: Equation 4 evaluates the percentage of securely protected transactions.

$$Privacy\ Rate = \frac{Secure\ Transactions}{Total\ Transactions} \times 100 \quad (4)$$

Transaction Processing Time: Equation 5 represents the average time required to process blockchain transactions.

$$T_p = \frac{\sum_{i=1}^{n} t_i}{n} \quad (5)$$

System Throughput: Equation 6 measures the number of transactions processed within a specific execution time.

$$Throughput = \frac{Processed\ Transactions}{Execution\ Time} \quad (6)$$

Storage Efficiency: Equation 7 indicates the effectiveness of distributed storage utilization.

$$Storage\ Efficiency = \frac{Useful\ Stored\ Data}{Total\ Storage\ Capacity} \times 100 \quad (7)$$

4.2 Performance Comparison

Table 1: Performance comparison of existing e-learning security frameworks and proposed blockchain-integrated model

Method	Authentication Accuracy (%)	Privacy Preservation (%)	Processing Time (ms)	Throughput (TPS)	Storage Efficiency (%)
Centralized Cloud E-Learning (CCEL)	88.4	84.2	420	180	72.5
Conventional Blockchain Learning System (CBLS)	91.6	89.8	360	240	78.4
Secure Federated E-Learning (SFEL)	93.1	92.4	315	285	82.6
Distributed Learning Access Control (DLAC)	94.2	93.7	280	320	84.1
Proposed Model	98.3	97.5	190	465	91.8

The performance of the suggested mobile learning system based on the blockchain technology in comparison with other learning systems has been evaluated based on five performance metrics namely authentication accuracy, privacy preservation, processing time, throughput, and storage efficiency are shown in table 1. The proposed scheme outperformed in terms of authentication accuracy (98.3%), privacy preservation (97.5%), reduced processing time (190ms), increased throughput (465TPS), and improved storage efficiency (91.8%).

4.3 Ablation Study

An ablation experiment was conducted to study the contribution of each major module in the developed architecture.

Table 2: Ablation study of proposed components

Configuration	Accuracy (%)	Privacy Rate (%)	Throughput (TPS)
Without Blockchain	89.6	85.2	240
Without Smart Contracts	91.1	88.5	275
Without Distributed Storage	92.8	90.4	310
Without Lightweight Encryption	94.2	91.8	355
Complete Proposed Model	98.3	97.5	465

The table 2 shows that all the major components in the blockchain-integrated distributed mobile e-learning architecture contribute to security, scalability, and efficiency.

The findings of the experiment prove the effectiveness of the introduced distributed mobile e-learning platform architecture that incorporates the blockchain technology in solving significant security issues faced by wireless educational platforms. The introduced architecture is characterized by high levels of transparency, authenticity, protection against falsification, and autonomy of data management; meanwhile, the processing time is minimized. Thus, the incorporation of blockchain, distributed storage based on IPFS, and cryptography make the proposed architecture highly appropriate for use in future m-learning systems.

5 Conclusion

The current study introduced a privacy-preserving distributed mobile e-learning architecture leveraging blockchain technologies to enable secure and autonomous student data management in wireless educational environments. The developed framework incorporated the application of blockchain technology, lightweight cryptography, smart contracts for access control, and distributed storage solutions in order to tackle several issues such as privacy preservation, secure authentication, data integrity, transparency, and decentralization of educational governance. Moreover, the architecture focused on developing an efficient system supporting large mobile learning ecosystems, while significantly decreasing the need for central servers used in other e-learning platforms. As shown in experimental results, the suggested architecture was highly effective compared to existing models including the Centralized Cloud E-Learning (CCEL), Conventional Blockchain Learning Systems (CBLS), Secure Federated E-Learning (SFEL), and Distributed Learning Access Control (DLAC) methods. Specifically, the developed framework attained 98.3% of authentication accuracy, 97.5% of privacy preservation rate, and 91.8% storage efficiency. Hence, the reliability of proposed approach was demonstrated in terms of protection of sensitive data of students. Also, the transaction time was reduced to 190 ms, and the number of transactions per second was increased to 465 TPS. The results from the ablation test have proven the contributions made by blockchain validation, distributed storage, smart contracts, and lightweight encryption towards improving performance in terms of security, scalability, and efficiency. The results from the analysis support the fact that decentralized blockchain technology-based learning solutions can be used effectively to improve trust management, tamper resistance, and autonomous data control without compromising on communication efficiency within wireless mobile networks. In addition, IPFS-based distributed storage helped in reducing storage redundancy and improving the accessibility of data within the distributed learning environments. Further research can be carried out to integrate AI and federated learning in order to achieve adaptive privacy-aware learning analytics. Other areas of interest could include research on energy-efficient consensus algorithms, quantum-resistance cryptography, cross-chain interoperability, and real-time intrusion detection.

References

[1] Anwar, M. (2021). Supporting privacy, trust, and personalization in online learning. *International Journal of Artificial Intelligence in Education*, *31*(4), 769-783. https://doi.org/10.1007/s40593-020-00216-0

[2] Cai, Z., Tang, T., Yu, S., Xiao, Y., & Xia, F. (2023). Marking the pace: A blockchain-enhanced privacy-traceable strategy for federated recommender systems. *IEEE Internet of Things Journal*, *11*(6), 10384-10397. https://doi.org/10.1109/JIOT.2023.3329363

[3] Coman, E., Coman, C., Alexandrescu, M. B., & Bilți, R. S. (2025). Mapping the Frontiers of Cybersecurity and Data Protection: Insights from a Bibliometric Study. *Electronics*, *14*(19), 3769. https://doi.org/10.3390/electronics14193769

[4] El-Haggar, N., Amouri, L., Alsumayt, A., Alghamedy, F. H., & Aljameel, S. S. (2023). The effectiveness and privacy preservation of IoT on ubiquitous learning: Modern learning paradigm to enhance higher education. *Applied Sciences*, *13*(15), 9003. https://doi.org/10.3390/app13159003

[5] Haque, M., Kumar, V. V., Singh, P., Goyal, A. A., Upreti, K., & Verma, A. (2023). A systematic meta-analysis of blockchain technology for educational sector and its advancements towards education 4.0. *Education and Information Technologies*, *28*(10), 13841-13867. https://doi.org/10.1007/s10639-023-11744-2

[6] Kavitha, M. (2024). Federated Learning Framework for Privacy-Preserving Data Analytics in Smart Agriculture for Rural Environments. *National Journal of Smart Agriculture and Rural Innovation*, 9-16.

[7] Kingdon, C. C., & Luedke, R. G. (2025). Integrating Blockchain with Information Governance: A Multidisciplinary Framework for Academic Institutions. *Bridge: Journal of Multidisciplinary Explorations*, *1*(2), 77-84.

[8] Lamaazi, H., Alneyadi, A. M. M., & Serhani, M. A. (2024, May). Academic data privacy-preserving using centralized and distributed systems: a comparative study. In *Proceedings of the 2024 6th International Conference on Big-data Service and Intelligent Computation* (pp. 8-16). https://doi.org/10.1145/3686540.3686542

[9] Lincopinis, D. R., Tabamo, G. M. A., Aguirre, F. N., Aguirre, M. R. C., Cagalitan, L. M., Tabilla, J. A. R., & Llantos, O. E. (2025, October). Design of KahibawHub: A Blockchain-Integrated Mobile Platform for Trusted Educational Content Sharing. In *2025 IEEE Cyber Science and Technology Congress (CyberSciTech)* (pp. 311-317). IEEE. https://doi.org/10.1109/CyberSciTech68397.2025.00048

[10] Ma, C., Li, J., Wei, K., Liu, B., Ding, M., Yuan, L., ... & Poor, H. V. (2023). Trusted ai in multiagent systems: An overview of privacy and security for distributed learning. *Proceedings of the IEEE*, *111*(9), 1097-1132. https://doi.org/10.1109/JPROC.2023.3306773

[11] Masood, F., & Faridi, A. R. (2021, August). A blockchain framework to increase the security and verifiability of educational certificates. In *International Conference on Advances in Cyber Security* (pp. 3-17). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-16-8059-5_1

[12] Mawgoud, A. A., Taha, M. H. N., Loey, M., Hussain Malik, M., & Khalifa, N. E. (2025). Enhancing Data Privacy and Trust in E-Learning: A Blockchain-Based Access Control Protocol for Cloud Educational Systems. *Concurrency and Computation: Practice and Experience*, *37*(18-20), e70185. https://doi.org/10.1002/cpe.70185

[13] Mohsen, S. A., & Munassar, N. M. A. (2025). Combining Deep Learning with Edge Computing in Improving Accessibility and Performance of E-Learning. *Journal of Science and Technology*, *30*(8). https://doi.org/10.20428/jst.v30i7.2935

[14] Mubarak, R., Riadi, I., & Sutikno, T. (2026). Integration of blockchain and cryptographic algorithms for education certification and verification: a systematic literature. *Journal of Soft Computing Exploration*, *7*(1), 117-131. https://doi.org/10.52465/joscex.v7i1.23

[15] Muhammad, M. K., Oyefolahan, I. O., Olaniyi, O. M., & Adebayo, O. J. (2020, November). Privacy Preservation in Mobile-Based Learning Systems: Current Trends, Methodologies, Challenges, Opportunities and Future Direction. In *International Conference on Information and Communication Technology and Applications* (pp. 520-534). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69143-1_40

[16] Murgai, A., Reddy, M. V. B., Vani, M. P., Jagtap, S., Adudhodla, M., & Arunkumar, J. R. (2025, November). Blockchain-Enabled Secure Data Sharing in Cloudedge Learning Networks. In *2025 International Conference on Digital Innovations for Sustainable Solutions (ICDISS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICDISS68238.2025.11320669

[17] Pal, V. K., Kumar, P., Vera, N., Manga, R., Kumar, R., & Gautama, R. (2025). Blockchain Based Academic Certificate Authentication System. In *Demystifying Emerging Trends in Green Technology* (pp. 352-363). Bentham Science Publishers. https://doi.org/10.2174/9789815324099125030l

[18] Patel, R. A., & Patel, D. T. (2025). Leopard Seal K-Anonymity Privacy-Preserved Hyper-Ledger Blockchain Integrated with Deep Learning for Student Mark Management. *SN Computer Science*, *6*(8), 968. https://doi.org/10.1007/s42979-025-04494-0

[19] Reginald, P. J. (2025). Blockchain for Inclusive Information Governance: Empowering Women and Stakeholders in Academic Leadership. *Journal of Women, Innovation, and Technological Empowerment*, *1*(2), 9-17.

[20] Sindhu, S. (2024). A Blockchain-Enabled Framework for Secure Data Exchange in Smart Urban Infrastructure. *Journal of Smart Infrastructure and Environmental Sustainability, 1*(1), 31-43.

[21] Salendab, F. A. (2026). Data Governance and Privacy Protection in AI-Enabled Education Systems. In *Strategies for Responsible AI Infrastructures Within Educational Administration* (pp. 169-196). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-2600-0467-8.ch006

[22] Verma, R., Singh, K. D., Singh, P. D., Maurya, S., Nerkar, S., & Thapliyal, N. (2024, May). Revolutionizing Education through Holistic Application of Technology: A Blockchain-Powered Framework for Smart Learning. In *2023 International Conference on Smart Devices (ICSD)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICSD60021.2024.10751355

[23] Wijesekara, P. A. D. S. N. (2024). A review of blockchain-rooted energy administration in networking. *The Indonesian Journal of Computer Science*, *13*(2). https://doi.org/10.33022/ijcs.v13i2.3818

[24] Yin, W. (2023). Zero-knowledge proof intelligent recommendation system to protect students' data privacy in the digital age. *Applied Artificial Intelligence*, *37*(1), 2222495. https://doi.org/10.1080/08839514.2023.2222495

Authors Biography

Odiljon Raxmatov is affiliated with Fergana State University and the University of Tashkent for Applied Sciences, Uzbekistan. He is actively engaged in teaching, research, and academic development, contributing to the advancement of higher education and interdisciplinary scholarship. His academic interests include innovative educational methodologies, applied research, and the integration of modern technologies into teaching and learning. Through his scholarly and professional activities, he supports the development of student competencies and the enhancement

of educational quality. His work reflects a strong commitment to academic excellence, research innovation, and lifelong learning.

Malohat Narbayeva is a Senior Lecturer in the Department of Higher Education, Faculty of Foreign Language Education, at Tashkent State University of Economics, Uzbekistan. She is actively involved in teaching, research, and academic development, with a particular focus on higher education and foreign language pedagogy. Her scholarly interests include language teaching methodologies, curriculum design, teacher education, and innovative approaches to learning. Through her academic and professional activities, she contributes to the enhancement of educational quality and the preparation of future language educators. Her work reflects a strong commitment to academic excellence, educational innovation, and lifelong learning.

Nazokat Jurayeva is an Associate Professor at Alfraganus University, Tashkent, Uzbekistan. She is actively engaged in teaching, research, and academic development, contributing to the advancement of higher education and scholarly excellence. Her academic interests include innovative teaching methodologies, educational research, curriculum development, and interdisciplinary studies. Through her teaching and professional activities, she supports the development of students' academic and professional competencies. Her work reflects a strong commitment to educational innovation, research excellence, and the continuous improvement of higher education.

Shakhrizabonu Shamsiyeva is a Doctoral Researcher at Bukhara State Pedagogical Institute, Uzbekistan. She is actively engaged in advanced academic research and scholarly activities, contributing to the development of knowledge in the field of education. Her research interests include pedagogy, educational innovation, curriculum development, and contemporary teaching and learning practices. Through her doctoral studies and academic work, she seeks to promote effective educational strategies and improve learning outcomes. Her work reflects a strong commitment to research excellence, professional growth, and the advancement of educational theory and practice.

Ulugbek Eshqarayev is a faculty member in the Department of Pedagogy and Psychology at Termez University of Economics and Service, Uzbekistan. He is actively engaged in teaching, research, and academic development in the fields of education and psychology. His scholarly interests include educational psychology, pedagogical innovation, student development, and contemporary teaching methodologies. Through his academic and professional activities, he contributes to improving educational practices and fostering students' intellectual and personal growth. His work reflects a strong commitment to academic excellence, educational research, and the advancement of pedagogy and psychology.

Lenara Islyamova is a faculty member at Jizzakh State Pedagogical University, Uzbekistan. She is actively engaged in teaching, research, and academic development, contributing to the advancement of educational theory and practice. Her scholarly interests include pedagogy, curriculum innovation, teacher education, and contemporary approaches to student learning. Through her academic and professional activities, she supports the development of effective educational strategies and the preparation of future educators. Her work reflects a strong commitment to academic excellence, educational innovation, and lifelong learning.

Matluba Xalmatova is a faculty member at Tashkent State Medical University, Tashkent, Uzbekistan. She is actively involved in teaching, research, and academic development in the field of medical and health sciences. Her scholarly interests include medical education, healthcare innovation, public health, and the application of evidence-based practices in clinical and educational settings. Through her academic and professional activities, she contributes to the training of future healthcare professionals and the advancement of medical knowledge. Her work reflects a strong commitment to academic excellence, scientific research, and the improvement of healthcare education and practice.