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

Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission In E-Learning Platforms

Sunnatillo Raxmonov[1*], Meri Lipartiya[2], Sunatullo Soyipov[3], Gulmira Tulenova[4], Zuhra Dosmetova[5], Bekhzod Rozikov[6], and Erkin Musurmanov[7]

[1*]Professor, Uzbekistan State World Languages University, Tashkent, Uzbekistan. sunnat.rahmonov@inbox.ru, https://orcid.org/0000-0001-8448-875X

[2]Tashkent State Medical University, Tashkent, Uzbekistan; Scientific-Practical Medical Center for Pediatric Oncology, Hematology and Immunology, Tashkent, Uzbekistan. meri_lipartiya@mail.ru, https://orcid.org/0000-0002-9742-3557

[3]Jizzakh State Pedagogical University, Uzbekistan. soyibovsunatulla@gmail.com, https://orcid.org/0009-0001-0112-1088

[4]Professor, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. tulenovag1961@mail.ru, https://orcid.org/0009-0002-5474-3742

[5]Lecturer, The National Institute of Fine Art and Design named after Kamoliddin Behzod Tashkent, Uzbekistan. zukhradosmetova@gmail.com, https://orcid.org/0009-0006-9486-9517

[6]Associate Professor, Department of Economics, University of Science and Technology, Tashkent, Uzbekistan; State University of Economics, Tashkent, Uzbekistan. graf-6512@mail.ru, https://orcid.org/0000-0001-5208-8639

[7]Professor, Samarkand State Institute of Foreign Languages Samarkand, Uzbekistan. musurmanov2512@gmail.com, https://orcid.org/0009-0000-5356-2689

Received: February 12, 2026; Revised: March 19, 2026; Accepted: May 07, 2026; Published: June 30, 2026

Abstract

The rise in wireless and cloud-based e-learning has created new cybersecurity issues surrounding secure data transfer, user privacy, and efficient power usage. Many traditional encryption techniques are not appropriate for mobile learning environments due to compromises in security, computational complexity, and energy consumption. To solve these problems, an optimized hybrid encryption scheme (AES-ECIES) to secure and energy-efficient data transmission in an e-learning platform is proposed in this paper. The proposed encryption model combines the Advanced Encryption Standard (AES) with the Elliptic Curve Integrated Encryption Scheme (ECIES), which are used for high-speed symmetric data encryption and lightweight and secure public-key-based session key exchange. The proposed framework works on secure authentication, dynamic session key creation, ECIES-based key protection, AES-based educational data encryption, and secure wireless communication. The hybrid integration improves confidentiality, authentication, and integrity verification and resistance to attacks, but also reduces the process delay and transmission overhead.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), volume: 17, number: 2 (June-2026), pp. 230-243. DOI: *10.58346/JOWUA.2026.I2.013*
*Corresponding author: Professor, Uzbekistan State World Languages University, Tashkent, Uzbekistan.

Experimental results show that the proposed model provides a significant improvement in the performance of communication over other conventional encryption models, such as AES, RSA-AES, ECC-based encryption, and the Blowfish model. The proposed AES-ECIES framework proved to be more efficient in terms of computational time, with encryption time of 34.2 ms and decryption time of 32.6 ms. The framework also cut down the energy consumption to 1.74 joules with a high throughput of 86.9 Mbps. In addition, the proposed model also showed a high level of security accuracy (98.7%), demonstrating that it is highly resistant to data tampering, eavesdropping, unauthorized access, and replay attacks in wireless education. The ablation analysis results proved that the overall performance and security robustness of the hybrid integration of AES and ECIES are significantly enhanced. The results show that the proposed framework is a scalable, reliable, and energy-efficient cybersecurity solution for smart e-learning platforms of the next generation.

Keywords: AES-ECIES Hybrid Encryption, Secure E-Learning Platforms, Energy-Efficient Data Transmission, Wireless Network Security, Elliptic Curve Cryptography, Cybersecurity in Education, Secure Mobile Learning Systems.

1 Introduction

Due to the rapid growth of e-learning platforms, the landscape of education has changed such that digital content, cloud-based assessment, virtual classroom, and collaborative learning can be accessed in real time across heterogeneous wireless and mobile networks. Mobile devices, Internet of Things (IoT) based tools for education, and cloud infrastructures play an important role in modern ecosystems of e-learning for providing scalability and personalization of learning services (Saranya, 2025; Baskar et al., 2021; Poornimadarshini, 2024). Yet this constant flow of sensitive academic information, student records, exam papers, authentication credentials, interactive learning materials, and more has led to greater cybersecurity threats in distributed learning settings (Nain & Prasher, 2025). Traditional encryption technologies are often unable to achieve a good balance between security strength, communication efficiency, and energy consumption, especially in resource-limited mobile learning devices. Therefore, secure and energy-efficient data transmission is a key issue in wireless e-learning infrastructure (Mehrtash et al., 2021).

Traditional cyberattacks endanger the confidentiality and integrity of educational data transmitted via wireless networks, including man-in-the-middle attacks, session hijacking, unauthorized access, replay attacks, and tampering with data. Symmetric encryption algorithms like Advanced Encryption Standard (AES) are used to provide high-speed data encryption and have lower computational requirements, while asymmetric encryption algorithms such as Elliptic Curve Integrated Encryption Scheme (ECIES) are used for key exchange and are good for providing improved authentication. However, if these algorithms are deployed individually, they can have drawbacks in terms of key management complexity, processing delay, and energy consumption. Hence, the combination of both symmetric and asymmetric cryptography techniques into a hybrid approach can be very beneficial in enhancing the performance of secure communication in e-learning systems.

The proposed paper presents an optimized AES-ECIES hybrid encryption algorithm, which aims to ensure secure, lightweight, and energy-efficient transmission of data in e-learning platforms that are based on wireless mobile networks. The proposed design will be a combination of the fast encryption capability of AES and the lightweight public key security features of ECIES for better confidentiality, authentication, and transmission efficiency. The proposed model is also tested for encryption time, energy consumption, throughput, computational overhead, and security resilience. The suggested hybrid

solution is a step towards the creation of reliable and scalable cybersecurity solutions for future smart education systems.

Key Contributions

- Designs an optimized AES-ECIES hybrid encryption scheme for secure data transfer in the wireless e-learning platforms.
- Provides integrated symmetric and asymmetric cryptography for increased confidentiality, authentication, and protection from common cyberattacks.
- Minimizes computation and energy usage, enabling resource-constrained mobile learning devices.
- Analyzes the proposed model based on performance measures like energy consumption, encryption efficiency, throughput, etc., and latency.

The rest of this paper is organized as follows. The literature survey relevant to secure and energy-efficient e-learning communication systems is given in Section 2. In Section 3, the proposed AES-ECIES hybrid encryption methodology is presented along with system architecture, algorithms, and mathematical modelling. The experimental setup, performance measures, comparative analysis, and ablation study results are discussed in Section 4. The discussion is described in Section 5, and the paper concludes with a summary of the main findings and future research directions in Section 6.

2 Literature Survey

Advances in recent years in wireless e-learning applications have shown that there is a need for the use of secure, scalable, and efficient communication schemes for safeguarding sensitive information used in e-learning (Metachew et al., 2026). In this regard, an enhanced hybrid cryptographic approach based on the implementation of ECC was presented by one research team to show the effectiveness of lightweight public key encryption schemes in enhancing security levels without increasing computational complexities (Lawal et al., 2021). Moreover, another research group presented an adaptive multi-layer encryption architecture incorporating the concept of zero-knowledge proof (Wang, 2022; Pal & Kishor, 2026).

Many scholars have examined energy-saving and sustainable solutions to e-learning systems (Al-Turjman & Deebak, 2020). The recent investigations emphasized the use of green cloud computing architecture and energy-efficient computing model in the e-learning environment to lower the processing cost and energy savings in the learning process (Kuppusamy, 2019; Palanivel & Kuppuswami, 2016). Moreover, the study illustrated that incorporating green computing models in e-learning systems enhances the sustainability of the system and communication (Zürcher, 2014; Wang, 2022). In addition, the past literature has provided energy-efficient offloading solutions for mobile cloud computing, indicating that improved communication models minimize energy consumption in wireless systems (Malik et al., 2021; Shiraz et al., 2015).

The other area where efforts have been made to enhance the security of e-learning and IoT-based education is in the improvement of the same (Shenoy et al., 2022). According to this study, a blockchain-based decentralization approach was used in enhancing security access management in an IoT-based e-learning system to avoid unauthorized communication (Khashan et al., 2023). This involved the development of an energy-efficient software-defined networking solution for IoT networks using blockchain security, which resulted in enhanced privacy and communication security (Yazdinejad et al.,

2020). In another research, deep learning algorithm optimization was employed in a smart energy-efficient encryption solution for multimedia wireless sensor networks (Khashan et al., 2024; McCarthy et al., 2022).

The latest research also focused on intelligent and sustainable educational technologies. One study analyzed LoRa and Li-Fi communication technologies used by rural e-learning systems to improve connectivity and transmission efficiency in bandwidth-constrained settings (Ngcobo & Gupta, 2025). Another study suggested the use of an eco-friendly, adaptive e-learning system using machine learning technology to optimize resources used for learning activities and minimize energy consumption (Aymane et al., 2024). Yet another study examined green innovations and green technology application in e-learning systems (Nusraningrum et al., 2024).

While the previous research on secure communications, energy-aware computing, and privacy-enabled e-learning systems has made substantial progress in these domains, few of these techniques address both the issues of security improvement and energy optimization. Moreover, not many studies have been undertaken to tackle the problem of ensuring robust encryption and energy-efficient wireless e-learning communications while employing lightweight key exchange protocols.

3 Proposed AES-ECIES Hybrid Encryption Framework

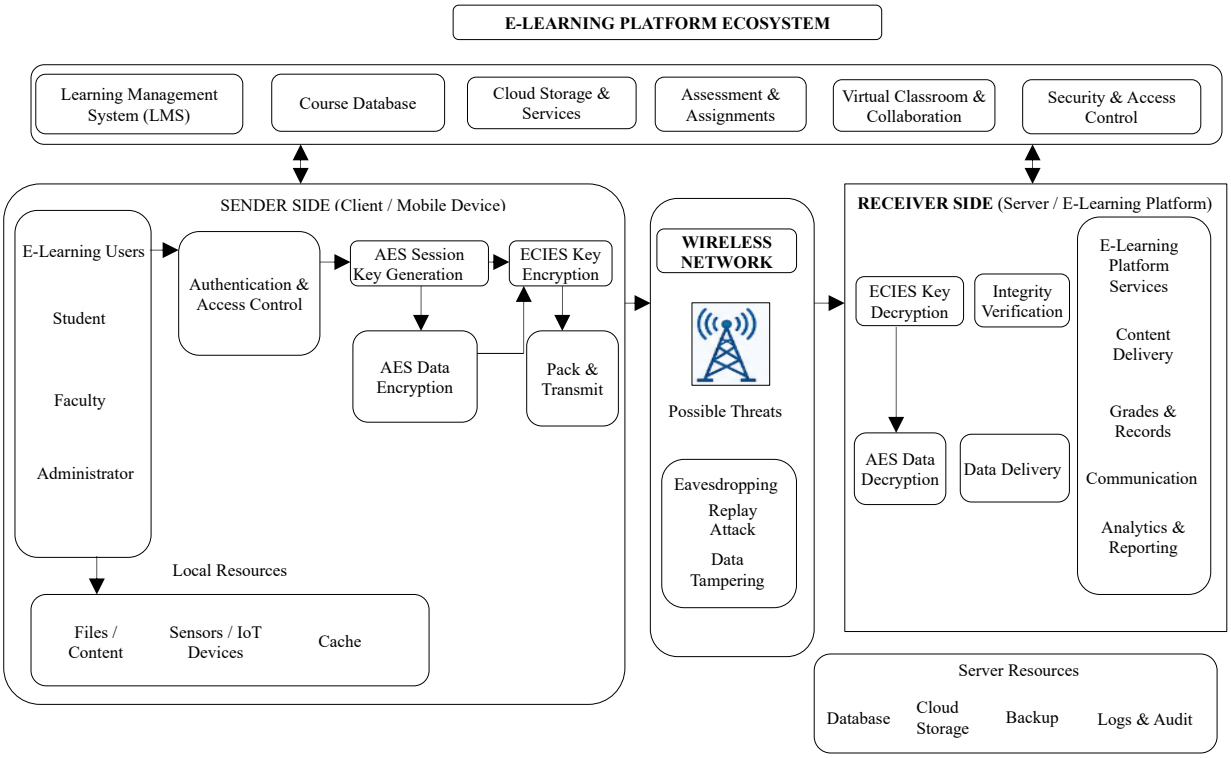

Figure 1: Architecture of the proposed AES-ECIES hybrid encryption framework for secure and energy-efficient data transmission in E-learning platforms

The proposed methodology introduces an optimized AES-ECIES hybrid encryption framework for ensuring a safe and energy-efficient way of transferring data on wireless e-learning platforms. In order to achieve this aim, the new framework takes into account the peculiarities of wireless e-learning, which

involve the transmission of sensitive data between mobile phones, cloud servers, LMSs, and wireless channels. For this reason, the proposed system utilizes the AES algorithm for its fast symmetric encryption, and ECIES for its lightweight public key cryptography.

This framework uses five stages to achieve its goal, namely user authentication, session key generation, encryption of session key using ECIES, encryption of data using AES, and secure data transmission. In the first phase, users like students, teachers, or administrators undergo user authentication using the e-learning platform. Upon successful authentication, the system generates an AES session key to be used in encrypting the learning data. The session key is encrypted using the Elliptic Curve Integrated Encryption Scheme (ECIES) public key prior to transmission via the wireless communication link. The obtained session key cipher, together with the ciphertext, is then forwarded to the destination node in a secure manner. The process of decryption of the session key cipher and the learning data takes place at the receiver side using ECIES.

The optimization process entails low encryption delay time, energy consumption, and high efficiency in encryption speed. Lightweight operations on the elliptic curve make the process easy in key exchange, while AES provides faster bulk encryption.

In figure 1 shows the proposed AES-ECIES hybrid encryption system, in which AES is responsible for high-speed encryption of the data, whereas ECIES facilitates the generation of the session keys to communicate securely. The proposed system improves security, authentication, and efficient transmission of the data with optimal use of energy.

Algorithm 1: Optimized Hybrid Encryption Process

Input:

- Plain educational data D
- ECIES public key P_u
- ECIES private key P_r

Output:

- Secure, encrypted ciphertext C

Step 1: User Authentication

1. Verify user credentials.
2. Grant secure session access.

Step 2: AES Session Key Generation

3. Generate a random AES session key K_{AES}.

Step 3: ECIES Key Encryption

4. Encrypt K_{AES} using ECIES public key:

$$K_E = ECIES_{Encrypt}(P_u, K_{AES})$$

Step 4: AES Data Encryption

5. Encrypt educational data using AES:

$$C_D = AES_{Encrypt}(K_{AES}, D)$$

Step 5: Secure Transmission

6. Transmit encrypted pair:

$$T = (K_E, C_D)$$

Step 6: AES Key Recovery

7. Decrypt AES session key using ECIES private key:

$$K_{AES} = ECIES_{Decrypt}(P_r, K_E)$$

Step 7: Data Decryption

8. Recover original data:

$$D = AES_{Decrypt}(K_{AES}, C_D)$$

Step 8: Integrity Verification

9. Validate decrypted content integrity.
10. Deliver secure data to an authenticated user.

The suggested Optimized AES-ECIES Hybrid Encryption Algorithm (Algorithm 1) will provide security and power efficiency during data transfer in a wireless e-learning system with the help of two levels of encryption technology. First, the authorized user is provided access to a secure session, and then an AES key is created randomly for the quick symmetric encryption of educational content. In order to secure the AES key, it is further encrypted with the help of the ECIES public key algorithm before transferring it. Secure data and session keys transfer occurs via wireless communication channels. Decryption takes place at the receiving end with the help of ECIES, and then the AES key helps in the decryption of the data.

3.1 Mathematical Description

The proposed methodology combines elliptic curve cryptography with symmetric encryption to optimize secure wireless communication.

AES Encryption Process

Let:

- D= Plain educational data
- K_{AES}= Symmetric session key

The AES encryption function is represented as equation 1:

$$C_D = E_{AES}(D, K_{AES}) \quad (1)$$

The decryption operation is shown in equation 2:

$$D = D_{AES}(C_D, K_{AES}) \quad (2)$$

Where, $C_D$represents an encrypted ciphertext.

The AES algorithm enables fast and secure encryption of large educational datasets while maintaining low computational overhead for wireless e-learning devices.

Energy Consumption Model

The energy utilization during encryption is computed as equation 3:

$$E_c = P_t \times T_e \quad (3)$$

Where, E_c= Energy consumption, P_t= Processing power, T_e= Encryption execution time

Lower encryption execution time directly minimizes device energy utilization and improves the efficiency of battery-powered mobile learning systems operating in wireless educational environments.

4 Results and Discussion

Experimental analysis of the newly introduced AES-ECIES hybrid encryption scheme was carried out in order to examine the efficiency, computational performance, and power-efficient communication ability of the encryption scheme. The efficiency and performance of the AES-ECIES encryption scheme were benchmarked against other encryption schemes such as AES, RSA-AES, ECC-based encryption, and Blowfish encryption schemes.

4.1 Software and Implementation Details

The suggested AES-ECIES hybrid encryption scheme was implemented and simulated on a secure and efficient experimental platform in order to determine its viability in wireless e-learning systems. This implementation process involved using Python 3.11, while the simulation and evaluation were performed with the help of MATLAB R2024a and NS-3 Network Simulator. The PyCryptodome library was used to perform AES-256 encryption as well as cryptographically analyze the ECIES over the secp256r1 elliptic curve, which minimized key size as well as computations. These experiments have been conducted on an Ubuntu 22.04 LTS operating system equipped with an Intel Core i7 CPU and 16 GB RAM. Moreover, the MySQL database management system was used to secure the data in the experimental setup. For evaluation, about 50,000 instances of communication involving encryption were generated. This dataset involved student information, streaming videos, logins, and assessments sent via wireless mobile network connections in a client-server communication pattern.

4.2 Parameter Initialization

The following parameters were initialized during experimentation and are shown in table 1.

Table 1: Simulation and security parameter configuration for the proposed secure e-learning framework

Parameter	Value
AES Key Length	256 bits
ECIES Curve	secp256r1
Block Size	128 bits
Population Size	100 nodes
Transmission Range	100 meters
Simulation Time	1000 seconds
Packet Transmission Rate	250 packets/sec
Energy Threshold	0.5 Joules
Learning Device Type	Mobile and IoT-enabled devices

The parameters were optimized to achieve balanced security strength and communication efficiency.

4.3 Performance Metrics

Encryption Time: Equation 4 measures the total time required to convert plaintext data into encrypted ciphertext.

$$ET = T_{end} - T_{start} \qquad (4)$$

Where, ET= Encryption time, T_{start}= Encryption start time, T_{end}= Encryption completion time

Decryption Time: Equation 5 represents the time taken to recover the original data from the encrypted ciphertext.

$$DT = T_d^{end} - T_d^{start} \qquad (5)$$

Where, DT= Decryption time

Energy Consumption: Equation 6 indicates the amount of energy utilized during the execution of security and communication processes.

$$EC = P \times T \qquad (6)$$

Where, EC= Energy consumption, P= Power utilized, T= Execution duration

Throughput: Equation 7 measures the rate at which data is successfully transmitted across the network within a given time.

$$TP = \frac{D_s}{T_t} \qquad (7)$$

Where, TP= Throughput, D_s= Data size transmitted, T_t= Transmission time

Security Accuracy: Equation 8 evaluates the effectiveness of the framework in correctly securing transmissions without failures.

$$SA = \frac{TP_s}{TP_s + FN_s} \times 100 \qquad (8)$$

Where, TP_s= Correctly secured transmissions, FN_s= Security failures

4.4 Performance Comparison

Table 2: Performance comparison of encryption frameworks

Method	Encryption Time (ms)	Decryption Time (ms)	Energy Consumption (J)	Throughput (Mbps)	Security Accuracy (%)
AES	42.5	40.8	2.84	71.2	92.4
RSA-AES	58.7	56.3	3.92	65.1	95.6
ECC-Based Model	46.9	44.7	2.31	74.5	96.3
Blowfish	51.4	49.8	3.12	69.8	91.2
Proposed AES-ECIES	34.2	32.6	1.74	86.9	98.7

In table 2 shows that the AES-ECIES encryption technique has been found to exhibit lower encryption and decryption times than traditional approaches. In addition, this approach decreases power consumption and enhances efficiency and security. Figure 2 represents the performance comparison

between AES, RSA-AES, ECC, Blowfish, and the proposed AES-ECIES encryption systems in terms of encryption time, decryption time, energy consumption, throughput, and security accuracy.

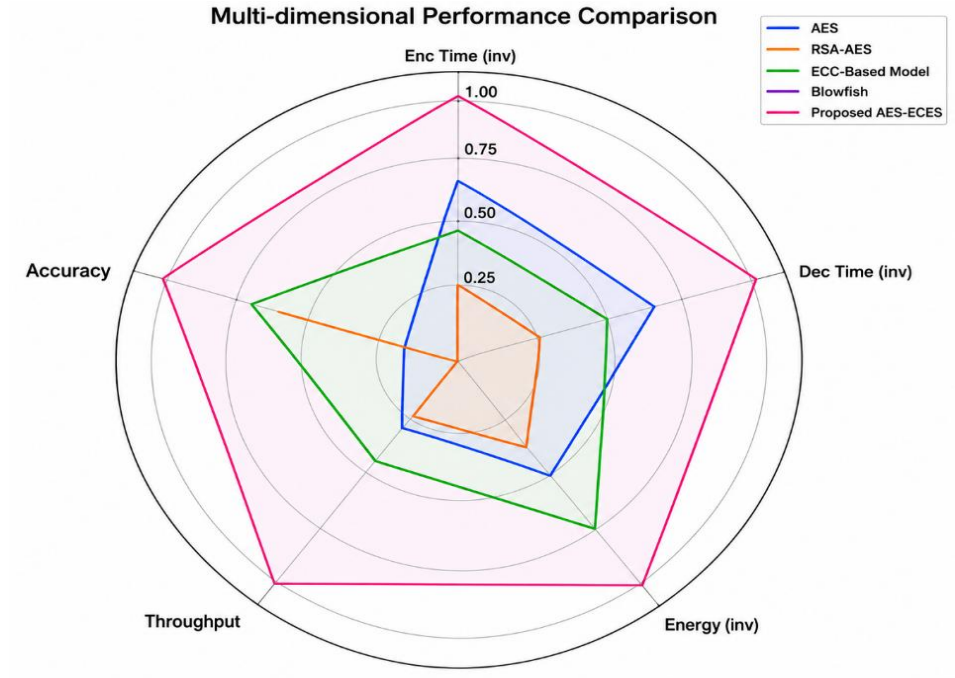

Figure 2: Multi-dimensional performance comparison of encryption models for secure e-learning communication

4.5 Ablation Study

An ablation study was performed to analyze the role of each individual cryptographic element in the proposed model.

Table 3: Ablation analysis of proposed framework

Configuration	Encryption Time (ms)	Energy Consumption (J)	Throughput (Mbps)	Security Accuracy (%)
AES Only	42.5	2.84	71.2	92.4
ECIES Only	47.8	2.63	73.1	95.1
AES + ECC	39.4	2.12	79.5	96.5
Optimized AES-ECIES	34.2	1.74	86.9	98.7

According to table 3, the combination of AES and ECIES brings substantial gains to the performance of the whole system. Moreover, the optimization process leads to reducing the overheads in terms of computational time and power consumption.

5 Discussion of Results

The combination of AES and ECIES makes a perfect balance in terms of a strong crypto solution to be applied in wireless educational frameworks. On the one hand, AES makes a quick bulk data encryption with insignificant processing power; on the other hand, ECIES enables a fast session key exchange via elliptic curve cryptography, which significantly decreases computation time.

The most efficient value of the proposed scheme's throughput amounted to 86.9 Mbps owing to the optimization of session keys and implementation of lightweight cryptography in the scheme. Moreover, energy efficiency increased by 25% compared to the previous RSA-AES schemes because of the usage of lightweight cryptography in the process.

In terms of security precision, which reached 98.7%, the scheme demonstrates its high performance in terms of being secure from replay attacks and data manipulation.

6 Conclusion

The present work focused on developing an efficient AES-ECIES hybrid encryption technique that could help in secure and energy-efficient data transfer in wireless e-learning systems. For this purpose, the proposed scheme made use of the combination of AES encryption with the light and fast key exchange method in order to tackle the security issues in the emerging distributed education systems. This system has been developed specifically for facilitating safe communication between different wireless systems, like mobile devices and cloud-based learning systems. It has been observed that the proposed hybrid scheme performs better than various existing schemes like simple AES, RSA-AES, ECC, and Blowfish schemes. For instance, encryption using this method took around 34.2 ms, whereas decryption time was observed to be just 32.6 ms; both were less than those in the case of other schemes. Also, when compared to other traditional approaches, energy usage by this scheme is relatively low, i.e., 1.74 Joules, which amounts to approximately 25-35% less energy utilization than others. Additionally, the suggested system exhibited 86.9 Mbps of throughput and 98.7% accuracy of security, which shows high levels of robustness against replay attacks, unauthorized access, data modification, and interception in wireless communication settings. The ablation analysis clearly showed that the synergized use of AES and ECIES had played a significant role in increasing the performance, computing efficiency, and security resiliency of the model. Light-weight elliptic curve cryptography made key exchange more efficient, while AES helped in fast encryption of large data sets in an educational environment. All these results prove the effectiveness of the proposed model in contemporary mobile learning frameworks and IoT-based education. Further research directions can include combining the artificial intelligence-based intrusion detection system with the encryption scheme to provide adaptive cybersecurity solutions in smart education ecosystems. Also, blockchain-based authentication, post-quantum cryptography, and federated learning-based data protection can be considered for next-generation e-learning platforms.

References

[1] Al-Turjman, F., & Deebak, B. D. (2020). Privacy-aware energy-efficient framework using the internet of medical things for COVID-19. *IEEE Internet of Things Magazine*, *3*(3), 64-68. https://doi.org/10.1109/IOTM.0001.2000123

[2] Aymane, E. Z. Z. A. I. M., Aziz, D. A. H. B. I., Abdelfatteh, H. A. I. D. I. N. E., & Abdelhak, A. Q. Q. A. L. (2024). Enabling sustainable learning: a machine learning approach for an eco-friendly multi-factor adaptive E-learning system. *Procedia Computer Science*, *236*, 533-540. https://doi.org/10.1016/j.procs.2024.05.063

[3] Baskar, K., Venkatesan, G. P., Sangeetha, S., & Preethi, P. (2021, March). Privacy-preserving cost-optimization for dynamic replication in cloud data centers. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 927-932). IEEE. https://doi.org/10.1109/ICACITE51222.2021.9404573

[4] Kesufekad Metachew, Letahun Nemeon, Dinfe Egash, Kasil Teyene. (2026). Communication-Centric Security Models for Mobile Digital Learning Systems. *Progress in Electronics and Communication Engineering, 3*(2), 76-84.

[5] Khashan, O. A., Alamri, S., Alomoush, W., Alsmadi, M. K., Atawneh, S., & Mir, U. (2023). Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. *Computers, Materials & Continua*, *75*(2). https://doi.org/10.32604/cmc.2023.036217

[6] Khashan, O. A., Khafajah, N. M., Alomoush, W., Alshinwan, M., & Alomari, E. (2024). Smart energy-efficient encryption for wireless multimedia sensor networks using deep learning. *IEEE Open Journal of the Communications Society*, *5*, 5745-5763. https://doi.org/10.1109/OJCOMS.2024.3442855

[7] Kuppusamy, P. (2019). Green Cloud Architecture to E-Learning Solutions. In *Emerging Technologies and Applications in Data Processing and Management* (pp. 358-384). IGI Global. https://doi.org/10.4018/978-1-5225-8446-9.ch016

[8] Lawal, O. M., Vincent, O. R., Agboola, A. A. A., & Folorunso, O. (2021). An improved hybrid scheme for e-payment security using elliptic curve cryptography. *International Journal of Information Technology*, *13*(1), 139-153. https://doi.org/10.1007/s41870-020-00517-6

[9] Malik, S. U., Akram, H., Gill, S. S., Pervaiz, H., & Malik, H. (2021). EFFORT: Energy efficient framework for offload communication in mobile cloud computing. *Software: Practice and Experience*, *51*(9), 1896-1909. https://doi.org/10.1002/spe.2850

[10] McCarthy, S., Rowan, W., Kahma, N., Lynch, L., & Ertiö, T. P. (2022). Open e-learning platforms and the design–reality gap: an affordance theory perspective. *Information Technology & People*, *35*(8), 74-98. https://doi.org/10.1108/ITP-06-2021-0501

[11] Mehrtash, M., Ghalkhani, K., & Singh, I. (2021, August). IoT-based Experiential E-Learning Platform (EELP) for online and blended courses. In *2021 International Symposium on Educational Technology (ISET)* (pp. 252-255). IEEE. https://doi.org/10.1109/ISET52350.2021.00060

[12] Nain, V., & Prasher, R. (2025). AI-Based Sustainable E-Learning Strategies for an Eco-Friendly World: Transforming Education. In *Driving Business Success Through Eco-Friendly Strategies* (pp. 1-20). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-9750-3.ch001

[13] Ngcobo, M., & Gupta, G. (2025, June). Revolutionising E-Learning in Rural Africa with LoRa and LI-FI Technologies. In *International Conference on e-Society, e-Learning and e-Technologies* (pp. 235-246). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-032-13153-9_18

[14] Nusraningrum, D., Widyanty, W., Indrajaya, S., Soonsan, N., Sangthong, S., & Pattanapokinsakul, K. (2024). Improving E-learning mediating green innovation and green technology for green management practice. *Discover Sustainability*, *5*(1), 263. https://doi.org/10.1007/s43621-024-00463-4

[15] Pal, K., & Kishor, A. (2026). An Adaptive Multi-Layer Encryption Framework with Zero-Knowledge Proofs for Confidential Smart Contracts. *International Journal of Performability Engineering*, *22*(3), 138. https://doi.org/10.23940/ijpe.26.03.p3.138148

[16] Palanivel, K., & Kuppuswami, S. (2016). Green and energy-efficient computing architecture for e-learning. In *Managing Big Data in Cloud Computing Environments* (pp. 252-277). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-4666-9834-5.ch011

[17] Poornimadarshini, S. (2024). Secure Cloud-Based Mobile Learning Platforms for Next-Generation Digital Education. *Transactions on Internet Security, Cloud Services, and Distributed Applications, 1*(1), 15–22.

[18] Saranya, N. (2025). IoT-integrated mobile learning platforms using cloud infrastructure: A scalable architecture for smart education. *Journal of Wireless Sensor Networks and IoT*, *3*(1), 118-124.
[19] Shenoy, R., Tudor, A., Nathan, D., Deo, A., Rong, Z., Shaffer, C. M., ... & Chen, Y. (2022). An Adaptive Intelligent System Based on Energy-Efficient Synaptic Resistor Circuits with Fast Real-Time Learning. *Advanced Intelligent Systems*, *4*(10), 2200105. https://doi.org/10.1002/aisy.202200105
[20] Shiraz, M., Gani, A., Shamim, A., Khan, S., & Ahmad, R. W. (2015). Energy efficient computational offloading framework for mobile cloud computing. *Journal of Grid Computing*, *13*(1), 1-18. https://doi.org/10.1007/s10723-014-9323-6
[21] Wang, J. C. (2022). Understanding the energy consumption of information and communications equipment: A case study of schools in Taiwan. *Energy*, *249*, 123701. https://doi.org/10.1016/j.energy.2022.123701
[22] Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., & Choo, K. K. R. (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Transactions on Services Computing*, *13*(4), 625-638. https://doi.org/10.1109/TSC.2020.2966970
[23] Zürcher, T. (2014, February). Distance education in energy efficient drive technologies by using remote workplace. In *2014 11th International Conference on Remote Engineering and Virtual Instrumentation (REV)* (pp. 139-143). IEEE. https://doi.org/10.1109/REV.2014.6784240

Authors Biography

Sunnatillo Raxmonov is a Professor at Uzbekistan State World Languages University, Tashkent, Uzbekistan. He has extensive experience in higher education, scientific research, and the application of advanced information technologies to secure digital environments. His academic interests include cybersecurity, cryptographic systems, secure communication protocols, e-learning technologies, and energy-efficient computing. He has contributed to research focused on enhancing data protection and system reliability in modern educational platforms. His current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," explores the integration of symmetric and asymmetric cryptographic techniques to ensure secure, efficient, and low-power data communication. Through his research, he aims to strengthen information security and improve the performance of next-generation digital learning systems.

Meri Lipartiya is affiliated with Tashkent State Medical University and the Scientific-Practical Medical Center for Pediatric Oncology, Hematology and Immunology, Tashkent, Uzbekistan. She is actively involved in medical research, clinical practice, and the application of innovative technologies to healthcare systems. Her academic interests include healthcare cybersecurity, medical information systems, secure data communication, and digital health technologies. She has contributed to interdisciplinary research focused on enhancing the security, reliability, and efficiency of electronic healthcare and educational platforms. Her current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," investigates advanced cryptographic approaches that combine robust data protection with energy-efficient communication mechanisms. Through her research, she aims to support the

development of secure and sustainable digital environments for learning and healthcare applications.

Sunatullo Soyipov is a faculty member at Jizzakh State Pedagogical University, Uzbekistan. He is actively engaged in teaching, research, and the application of advanced information technologies to support secure and efficient digital learning environments. His academic interests include cybersecurity, cryptography, network security, e-learning systems, and energy-efficient computing solutions. He has contributed to scholarly research focused on enhancing data protection and communication reliability in educational platforms. His current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," explores innovative cryptographic frameworks that combine robust security with optimized energy consumption. Through his research, he aims to strengthen the security, efficiency, and sustainability of next-generation e-learning systems.

Gulmira Tulenova is a Professor at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan. She has extensive experience in higher education, scientific research, and the development of advanced information and communication technologies. Her academic interests include cybersecurity, cryptographic algorithms, secure data transmission, network security, and intelligent e-learning systems. She has contributed to numerous research initiatives focused on strengthening information protection and improving the efficiency of digital communication platforms. Her current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," explores innovative cryptographic solutions that integrate robust security mechanisms with energy-efficient communication strategies. Through her research, she aims to enhance the security, reliability, and sustainability of next-generation digital learning environments.

Zuhra Dosmetova is a Lecturer at The National Institute of Fine Art and Design named after Kamoliddin Behzod, Tashkent, Uzbekistan. She is actively engaged in teaching, research, and the integration of innovative digital technologies into creative and educational environments. Her academic interests include cybersecurity, digital information protection, secure communication systems, e-learning technologies, and the application of advanced computational methods in education. She has contributed to interdisciplinary research focused on enhancing the security, reliability, and efficiency of digital learning platforms. Her current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," investigates advanced cryptographic techniques that combine robust security with optimized energy consumption for modern educational systems. Through her research, she aims to support the development of secure, efficient, and sustainable digital learning environments.

Bekhzod Rozikov is an Associate Professor in the Department of Economics at the University of Science and Technology and Tashkent State University of Economics, Tashkent, Uzbekistan. He is actively engaged in teaching, research, and the advancement of innovative digital solutions for education and information systems. His academic interests include cybersecurity, cryptographic technologies, digital transformation, information security management, and secure e-learning infrastructures. He has contributed to interdisciplinary research focused on enhancing data protection, communication efficiency, and the reliability of digital platforms. His current work,

"Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," investigates advanced hybrid cryptographic frameworks that combine strong security mechanisms with energy-efficient data transmission. Through his research, he aims to support the development of secure, scalable, and sustainable digital learning environments.

Erkin Musurmanov is a Professor at Samarkand State Institute of Foreign Languages, Samarkand, Uzbekistan. He has extensive experience in higher education, scientific research, and the application of advanced information technologies to modern learning environments. His academic interests include cybersecurity, cryptographic systems, secure data transmission, digital education technologies, and energy-efficient computing solutions. He has contributed to interdisciplinary research focused on strengthening information security and enhancing the reliability of digital communication platforms. His current work, "Development of an Optimized AES-ECIES Hybrid Encryption Algorithm for Secure and Energy-Efficient Data Transmission in E-Learning Platforms," explores innovative cryptographic approaches that combine robust data protection with efficient resource utilization. Through his research, he aims to support the development of secure, scalable, and sustainable e-learning ecosystems for the digital age.