CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES

https://cajmtcs.casjournal.org/index.php/CAJMTCS

Volume: 07 Issue: 02 | April 2026 ISSN: 2660-5309

.

Article

Sustainable Cloud-Based Security Architecture for Data Protection in E-Learning and Healthcare Systems

Munera A. Jabaar

1. Middle Technical University - Al- Rusafa Management Institute

* Correspondence: munera_abdaljabar@mtu.edu.iq

Abstract: Cloud computing is one of the new innovations in digital transformation that have revolutionized various areas of life including education and healthcare. However, with the rising significance of cloud infrastructures, the level of security threat and privacy concern is on the rise with regard to sensitive data. Sustainable cloud encryption techniques will be discussed in this paper in the enhancement of data security in e-learning and health-related platform.

The hybrid encryption techniques, proxy re-encryption and block-chain-based systems, are analyzed with the assistance of systematic literature review. It offers a proposed security structure which is based on federated learning, with sustainable encryption to strengthen data protection. The findings have shown that sustainable encryption is a means to ensure confidentiality, integrity, as well as minimizing the cost of computing and environmental costs thereby ensuring the digital ecosystems are secure and environmental friendly.

Keywords: Cloud Security; Sustainable Encryption; Hybrid Encryption; Federated Learning; Block-chain-based Security; E-Learning Data Protection; Healthcare Data Privacy

Citation: Jabaar, M. A. Sustainable Cloud-Based Security Architecture for Data Protection in E-Learning and Healthcare Systems. Central Asian Journal of Mathematical Theory and Computer Sciences 2026, 7(2), 37-42

Received: 10th Nov 2025
Revised: 21th Dec 2025
Accepted: 01th Jan 2026
Published: 14th Feb 2026

1. Introduction

The adoption of cloud computing in e-learning systems and healthcare systems has enabled it to be scalable and cost effective and have access to better resources [1][2][3][4]. However, security of sensitive information such as student records and electronic health records (EHRs) has raised serious concerns in this digital transformation [5]. There is still a challenge of confidentiality, integrity, and availability of data on the cloud due to unauthorized access, cyberattacks, and insider threats [6],[7].

The conventional encryption systems though suitable in certain scenarios may not be suitable to meet the complexities of the modern distributed cloud systems. The encryption and proxy re-encryption schemes have been the solutions to the secure transmission and sharing of data by using cloud-based encryption methods [8]. In addition, the adherence of the regulatory requirements to frameworks like GDPR or HIPAA implies that the encryption model involves high levels of security that will guarantee that the data is not exposed to the new threats [9],[10].

Sustainability is another dimension that is increasing. E-learning and healthcare applications that are hosted in data centers consume huge amounts of energy. According to recent research, there is a need to implement eco-friendly encryption algorithms and energy-saving cryptographic protocols in cloud infrastructures [11]. This two-fold concern with security and sustainability forms the motivation of this study.

Sustainable encryption is a concept that is used to denote the structural and implementation designs of cryptographic systems that are not only to provide strong data security but also to be energy-efficient and computationally-efficient. In contrast to classical encryption methods that can require a considerable amount of processing capabilities, sustainable encryption incorporates lightweight algorithms and hybrid constructions (e.g., AES with RSA/ECC) to provide high confidentiality and integrity rates at a low energy consumption. This notion is in line with the major vision of green computing, where security measures are created to be environmentally friendly, scalable, and acceptable to resource limited networks like IoT devices, e-learning tools, and health care systems.

2. Materials and Methods

Literature Review

Cloud Security in E-Learning

The cloud service is extremely needed in hosting online content, online exams, and group learning materials on E-learning. Nevertheless, they are at risk of denial-of-service (DoS) attacks, manipulation of data, and unauthorized access [12]. In order to provide confidentiality and to minimize the computational costs, hybrid encryption schemes (or the use of combination of symmetric and asymmetric methods) are becoming widespread [13].

E-learning systems are also seeing adoption of block-chain based solutions which provide immutable storage for academic records and transparent audit trails for data transactions (14). These methods enhance trust and accountability within cloud-based learning settings to a great extent.

Healthcare Data Protection

The health care industry is also among the most sensitive industries where cloud security is essential because of patient records. In order to support sharing of medical data amongst the sensitive stakeholders, proxy re-encryption and attribute-based encryption methods have been suggested [15],[16].

Healthcare data management is no exception, and federated learning has been proposed to facilitate collaborative model training without raw data movement from local nodes [17]. This guarantees privacy and promotes AI-based diagnosis of disease like diabetes and COVID-19 [18],[19]. Federated learning in combination with cloud-based encryption is a good foundation to medical research security.

Sustainable Cloud Security

As the need to have green computing is increasing, sustainable solutions to cloud security have been developed. Energy efficient encryption algorithms minimize the amount of computation at the expense of attacks [20]. Green data centers that use renewable energy and low-power cryptographic controls show that sustainability and security can both be ensured in cloud systems [21][22].

Methodology

This paper involves systematic review and conceptual design research to examine the issue of sustainable cloud-based encryption in e-learning and healthcare systems. The procedure of the research took place in three steps:

1. Literature Collection: The databases such as IEEE Xplore, SpringerLink, ScienceDirect, MDPI, and PubMed were used to obtain peer-reviewed articles published within the period of 2020-2024 [1],[5],[12].

2. Analysis Framework: The collected literature was evaluated according to the security, application area, and sustainability [13],[17].

Proposed Framework Design: An overall conceptual framework was created that incorporated cloud-based encryption, federated learning, and sustainable computing practices [20],[21].

Figure 1. Suggested Sustainable Cloud Security Framework

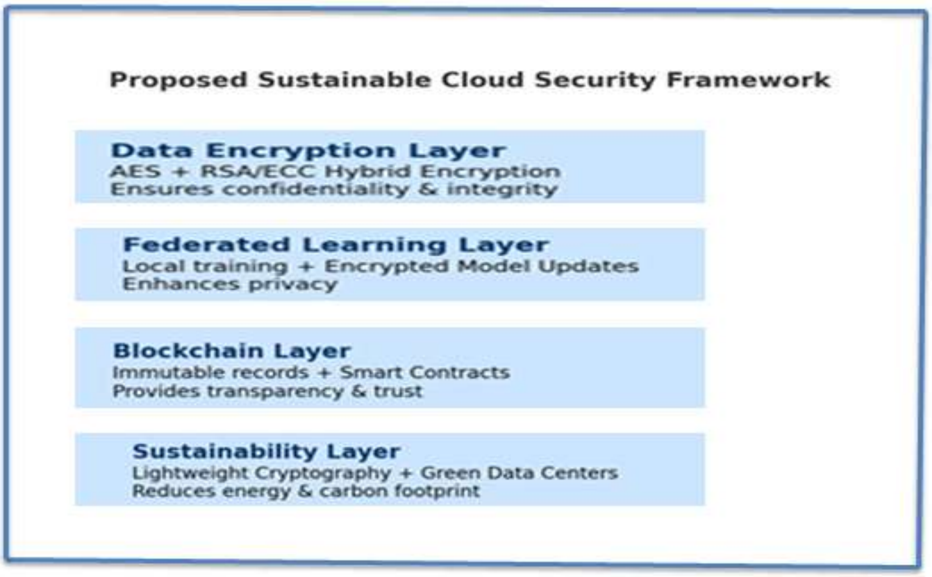

Proposed Sustainable Cloud Security Framework
Data Encryption Layer
AES + RSA/ECC Hybrid Encryption
Ensures confidentiality & integrity
Federated Learning Layer
Local training + Encrypted Model Updates
Enhances privacy
Blockchain Layer
Immutable records + Smart Contracts
Provides transparency & trust
Sustainability Layer
Lightweight Cryptography + Green Data Centers
Reduces energy & carbon footprint

Table 1. Comparison of Encryption Methods

Technique	Security Level	Speed	Energy Consumption
AES	High	Fast	Low
RSA	High	Slow	High
Hybrid (AES+RSA)	Very High	Medium	Moderate

The proposed structure entails the multi-layer architecture integrating encryption, federated learning, and sustainable cloud architecture:

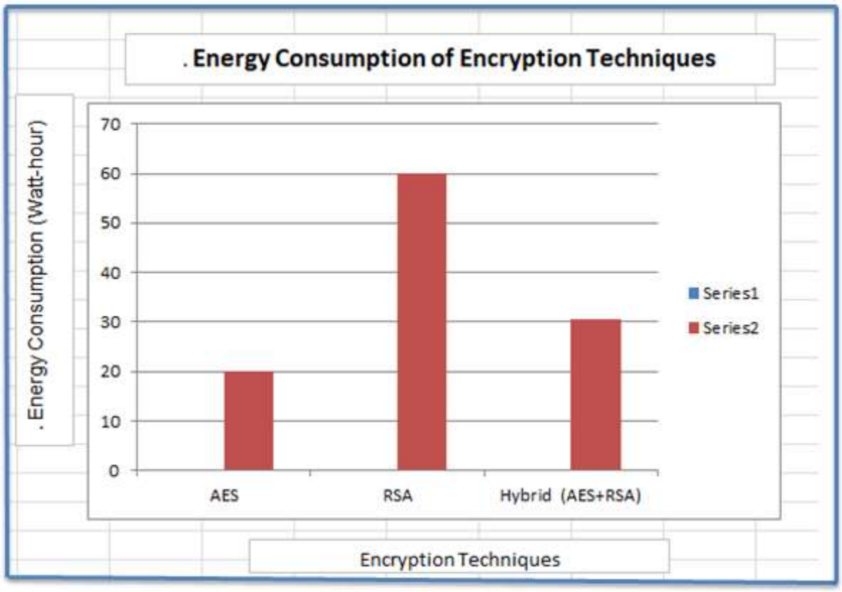
1. Data Encryption Layer: The encryption of sensitive information takes the hybrid method which is a combination of both the symmetric encryption (AES) and asymmetric encryption (RSA/ECC) [14],[16].
2. Federated Learning Layer: This is done locally on the distributed nodes, where only encrypted updates on the models are shared [17],[18].
3. Block chain Integration: Block chain offers immutability, traceability and smart contracts to implement security policies [7],[19].
4. Sustainability Layer: Cryptography algorithms that are lightweight and renewable energy-powered data centers are used to reduce environmental impact [20],[22].

3. Results and Discussion

Table 2. E-learning vs Healthcare Cloud Security Needs

Domain	Security Needs	Unique Considerations
E-learning	Data privacy, access control, content protection	Student identity protection
Healthcare	Confidentiality, integrity, availability	Sensitive patient records, regulatory compliance

Figure 2. Energy Consumption of Encryption Methods



The combination of federated learning and block chain with cloud-based encryption shows a number of interesting results:

1. Enhanced Security: Confidentiality and integrity are guaranteed with the use of hybrid encryption and proxy re-encryption [12],[14],[15],[16].

2. Improved Privacy: Federated learning minimizes the risk of data leakage [17],[18].

3. Transparency and Trust: Block chain provides immutable audit trails and compliance [9],[19].

4. Sustainability Benefits: Green encryption and environmentally friendly data centers reduce the amount of carbon emissions [20],[21],[22].

5. Challenges: Key management scalability, interoperability and computational costs are still problems [13],[17].

6. Comparative Analysis with Previous Studies

Table 3. Comparison with Previous Works

Study	Technique Used	Limitation	Contribution of Current Work
Ali et al. [2]	Federated Learning in Healthcare	No encryption or sustainability integration	Adds encryption & green security
Boumezbeur & Zarour [12]	Hybrid Encryption in Cloud Healthcare	No federated learning or block chain	Adds FL + Block chain + Sustainability
This Work	Hybrid Encryption + FL + Block chain + Sustainability	-	Unified secure & eco-friendly framework for E-learning & Healthcare

A number of previous researches have had a contribution in cloud-based data security in e-learning and healthcare systems. Nevertheless, they tended to consider one of the dimensions without a total integration of encryption, AI privacy, and sustainability. The comparative analysis below points out the ways in which the proposed study will be superior to previous ones:

1. Ali et al. [2]: This paper addressed the notion of federated learning in healthcare without integrating encryption and sustainability.

2. Boumezbeur & Zarour [12]: This research suggested the use of hybrid encryption in healthcare without involving block chain and federated learning.
3. Proposed Study (This Work): Integrates Hybrid Encryption + Federated Learning + Blockchain + Sustainability in a unified architecture, offering stronger data security, privacy preservation, energy efficiency, and applicability across both e-learning and healthcare domains.

4. Conclusion

A cloud-based encryption framework is a sustainable research presented in this study aimed at ensuring the safety of sensitive data on e-learning and health-related websites. In contrast to the past literature, where the researchers usually discussed either encryption or federated learning as a separate concept (2,12), the study under consideration integrates the concept of hybrid encryption, federated learning, a block chain technology, and sustainability principles into a unified security system.

The comparative analysis revealed that it is a better approach as compared to previous works since it guarantees better confidentiality, better privacy protection, better trust due to the integration of blockchain, and better environmental impact due to the lightweight cryptographic methods. The presented system thus does not only focus on data security but also helps the world to go green and energy efficient cloud infrastructures.

Future research directions include:

1. Real-world implementation in large-scale e-learning and healthcare platforms.
2. Optimization of lightweight encryption algorithms for IoT and edge devices.
3. Development of AI-driven adaptive key management systems.
4. Exploration of multi-cloud and cross-border data security compliance frameworks.

Due to the solution of these future challenges, the suggested framework can be developed into a multifaceted solution which will balance the data protection, system performance and sustainability in cloud environment.

Conclusion and Future Work

This study came up with a sustainable cloud-based encryption system to protect sensitive data in e-learning and healthcare networks. With the integration of hybrid encryption, federated learning, and blockchain technologies in a sustainability-focused architecture, the framework improves the confidentiality and privacy of data, as well as trust, and minimizes the effects on the environment.

Further research needs to be based on practical case studies, lightweight algorithms optimization to IoT devices, AI-based key management, and multi-clouds and edge computing deployment.

REFERENCES

[1] Abbas SR, Abbas Z, Zahir A, Lee SW. Federated Learning in Smart Healthcare: A Comprehensive Review on Privacy, Security, and Predictive Analytics with IoT Integration. Healthcare. 2024;12(24):2587. doi:10.3390/healthcare12242587

[2] Ali MS, Ahsan MM, Tasnim L, Afrin S, Biswas K, Ahmed MM, Hashan R, Islam MK, Raman S. Federated Learning in Healthcare: Model Misconducts, Security, Challenges, Applications, and Future Research Directions – A Systematic Review. arXiv preprint. 2024. Available from: https://arxiv.org/abs/2405.13832

[3] Lin H-Y, Chen P-R. Revocable and Fog-Enabled Proxy Re-Encryption Scheme for IoT Environments. Sensors. 2024;24(19):6290. doi:10.3390/s24196290

[4] Yan L, Qin H, Yang K, Xie H, Wang XA, Liu S. Pairing-Free Certificate-Based Proxy Re-Encryption Plus Scheme for Secure Cloud Data Sharing. Electronics. 2024;13(3):534. doi:10.3390/electronics13030534

[5] Zhou Y, Liu S, Han S. Multi-Hop Fine-Grained Proxy Re-Encryption (mFPRE). IACR Cryptology ePrint Archive. 2024. Available from: https://eprint.iacr.org/2024/055

[6] Guo H, Li W, Nejad M, Shen C-C. A Hybrid Blockchain-Edge Architecture for Electronic Health Records Management with Attribute-Based Cryptographic Mechanisms. arXiv preprint. 2023. Available from: https://arxiv.org/abs/2305.19797

[7] Huang J, Yi J. The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins. Journal of Cloud Computing. 2024;13:15. doi:10.1186/s13677-023-00587-4

[8] Chen L, Wan Z, Zhou J. An Efficient Autonomous Path Proxy Re-encryption Without Pairing for Cloud-Assisted mHealth. In: Ge C, Yung M, editors. Information Security and Cryptology (Inscrypt 2023). Lecture Notes in Computer Science, vol. 14527. Singapore: Springer; 2024. p. 448-467. doi:10.1007/978-981-97-0945-8_28

[9] Thushara GA, Bhanu SMS. A New Hybrid Encryption in Fog-Cloud Environment for Secure Medical Data-Sharing. Iran Journal of Computer Science. 2023;6:169-183. doi:10.1007/s42044-022-00129-2

[10] Sepehri M, Trombetta A, Sepehri M. Secure Data Sharing in Cloud Using an Efficient Inner-Product Proxy Re-Encryption Scheme. Journal of Cyber Security and Mobility. 2024;13(1):1-20. doi:10.13052/2245-1439.635

[11] Kumar R, Khan P, Kumar S. Healthcare Data Encryption Technique Using Hybrid Cellular Automata in IoT Networks. Wireless Personal Communications. 2022;126:3021-3039. doi:10.1007/s11277-022-09850-4

[12] Boumezbeur I, Zarour K. Improving Privacy-preserving Healthcare Data Sharing in a Cloud Environment Using Hybrid Encryption. Acta Informatica Pragensia. 2022;11(3):361-379. doi:10.18267/j.aip.182

[13] Singh R, Sharma A, Arora V. A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure. Computers & Electrical Engineering. 2022;101:107991. doi:10.1016/j.compeleceng.2022.107991

[14] Shakor MY, Shafiq NMS, Khlaif ZN. Hybrid Security Model for Medical Image Protection in Cloud. Diyala Journal of Engineering Sciences. 2023;16(1):68-77. doi:10.24237/djes.2023.16107

[15] Bekhit M, Alsadoon A. Data Security in Hybrid Cloud Computing Using AES Encryption for Health Sector Organization. In: 7th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA). Cham: Springer; 2022. p.155-167. doi:10.1007/978-3-031-29078-7_15

[16] Srinivasan R, Panguluri LD, Mohammed SB. Cloud Compliance in Healthcare: A Technical Evaluation of Data Encryption, Access Control, and Risk Management Practices. Journal of Machine Learning for Healthcare Decision Support. 2022;2(2):21-35.

[17] Jain K. Key Management Strategy and Distribution of Public Key for Cloud Security. International Journal of Engineering and Management Research. 2023;13(1):129-135.

[18] GEECO Consortium. Green Data Centers for Energy Optimization and Carbon Footprint Reduction (GEECO Model). Sustainability. 2023;15(21):15249. doi:10.3390/su152115249

[19] Malele V. Cybersecurity Cloud-Based Online Learning: A Literature Review Approach. Journal of Information Systems and Informatics. 2023;5(4):1623-1632. doi:10.51519/journalisi.v5i4.583

[20] Alajmi Q, Chellathurai GJ. Adoption of Cloud Computing in E-Learning Systems: Security Perspective Review. Tasnim International Journal for Human, Social and Legal Sciences. 2023;2(3):356-374. doi:10.56924/tasnim.6.2023/18

[21] Review of Privacy Enhancement Methods for Federated Learning in Healthcare Systems. International Journal of Environmental Research and Public Health. 2023;20(15):6539. doi:10.3390/ijerph20156539

[22] Comprehensive Review on Federated Learning Based Models for Healthcare Applications. PubMed. 2023. Available from: https://pubmed.ncbi.nlm.nih.gov/38042608