Media Elektrik
Teknik Elektro Universitas Negeri Makassar
e-ISSN 2721-9100

Letter of Acceptance
Nomor: LOA202601282575

Dear Sir.

M. Zian Al Farisi. Bz
Universitas Islam Negeri Ar-Raniry

Thank you for submitting a scientific article to be published in **Media Elektrik** (E-ISSN: 2721-9100) published by the Department of Electrical Engineering Education, Faculty of Engineering, Universitas Negeri Makassar with the title:

BLOCKCHAIN FOR SECURITY AND PRIVACY IN AI-BASED EDUCATION: A SYSTEMATIC LITERATURE REVIEW

Based on the results of the review team's examination, the article was declared ACCEPTED, with revisions to be published in Volume 23, Number 2, April, 2026. This information has been conveyed, and for his attention, thank you. We will provide you with information regarding the publication of your journal via email.

Makassar, 28 Januari 2026
Editor in Chief

The authenticity of the LOA can be checked by scanning the QR code on the side!

LOA202601282575

Muhammad Yusuf Mappeasse

BLOCKCHAIN FOR SECURITY AND PRIVACY IN AI-BASED EDUCATION: A SYSTEMATIC LITERATURE REVIEW

[1]M. Zian Al Farisi. Bz [2]Khairan AR [3]Malahayati [4]Hendri Ahmadian
[1]Department of Information Technology, UIN Ar-Raniry, Banda Aceh, Indonesia
[2]Department of Information Technology, UIN Ar-Raniry, Banda Aceh, Indonesia
[3]Department of Information Technology, UIN Ar-Raniry, Banda Aceh, Indonesia
[4]Department of Information Technology, UIN Ar-Raniry, Banda Aceh, Indonesia

ARTICLE INFO

Article history:

Keywords:
Blockchain, Artificial Intelligence, Education, Data Privacy, PRISMA, Self-Sovereign Identity.

ABSTRACT

The transformation of education driven by artificial intelligence (AI) requires massive data flows, which poses serious challenges to student privacy if stored on centralized infrastructure. This study is a Systematic Literature Review (SLR) aimed at evaluating the effectiveness of blockchain technology in mitigating AI data security risks (RQ1) and analyzing the role of data sovereignty mechanisms in protecting student privacy (RQ2). Following the PRISMA guidelines, a literature search was conducted in the DOAJ and IEEE Xplore databases (2021–2026). From the initial 873 articles, 20 high-quality articles were selected through a quality assessment procedure and analyzed using the Narrative Synthesis Analysis method. The results of the empirical analysis show that centralized databases are highly vulnerable to Single Points of Failure (SPOF). As a solution, blockchain integration mitigates this risk through the implementation of Self-Sovereign Identity (SSI) and Zero-Knowledge Proofs (ZKP), which enable AI models (Federated Learning) to verify data without compromising Layer-2 scalability (zk-Rollups), which have been shown to reduce transaction costs by up to 90%, as well as agent-centric protocols (Holochain) for ecological efficiency. Practically, this study recommends that educational institutions and Ed-Tech developers transition to a hybrid storage architecture. Limitations of this study include the niche nature of the literature sample and the scope limitations of the database. Future research should focus on testing the latency of real-time prototypes in academic environments.

DOI:

Introduction

Digital transformation through artificial intelligence (AI) has opened up significant opportunities for the creation of a more personalized, flexible, and adaptive education system[1], [2]. The integration of AI into the curriculum and learning processes enables learning experiences tailored to individual students' needs, which serves as a cornerstone of future educational innovation [1]. However, the effectiveness of AI systems heavily relies on the collection and processing of massive amounts of big data, ranging from learning profiles to other sensitive data. The current reliance on centralized database architectures poses serious challenges regarding data privacy and security [3]. Bibliometric analysis of AI trends indicates that while scientific productivity is growing rapidly, issues of ethics, trust, and data privacy remain major unresolved obstacles in the literature [4]. Traditional centralized models are highly vulnerable to cyberattacks and single points of failure, where a single breach can expose an entire institution's data—a risk similar to data vulnerabilities in digital health systems [5], [6].

Blockchain technology has emerged as a potential solution to mitigate these risks through decentralized mechanisms that ensure data integrity and immutability [7]. Practical implementations are beginning to demonstrate the effectiveness of combining AI and blockchain, as seen in the BANFES system for non-formal education, which protects the learning rights of marginalized groups [8]. Additionally, modern scholarship management platforms now use AI to provide recommendations while leveraging blockchain to secure students' digital identities through the principle of data sovereignty or Self-Sovereign Identity [9]. The integration of these two technologies enables the creation of an inclusive educational ecosystem that remains secure from the threat of data manipulation [10], [11]. Although Web3 technologies like blockchain offer high security, new challenges persist regarding scalability and environmental impact, leading some researchers to suggest alternatives such as Holochain for a more sustainable educational context [12].

Although the potential for this integration is significant, previous systematic literature reviews (SLR) indicate that research on blockchain in the education sector remains focused on the issues of digital diploma certification and credential management [13]. There remains a significant literature gap specifically evaluating the comparative effectiveness of decentralized architectures versus centralized models in protecting the dynamic data streams required

by educational AI [3], [4]. Most current data security studies remain focused on the medical domain [14], [15], while the need for a comprehensive security framework within the evolving educational AI ecosystem has not yet been clearly mapped out. Therefore, a systematic review is needed to analyze recent developments and validate how blockchain can address privacy vulnerabilities in AI-based educational systems.

This study aims to conduct a systematic literature review to analyze the role of blockchain in enhancing data privacy and security in AI-based education. To achieve this objective, the study is guided by the following two research questions:

1. RQ1: How effective is the integration of blockchain technology compared to centralized database architectures in mitigating data security risks in AI-based education systems?
2. RQ2: How can the decentralization and data sovereignty mechanisms of blockchain protect student privacy while still facilitating the data requirements needed for AI-based personalized learning?

Materials and Methods

A. Literatur Review

1. Pedagogical Transformation in the Age of Artificial Intelligence

The application of Artificial Intelligence (AI) in education has extended far beyond the mere digitization of instructional materials, evolving toward a model of radical personalization. Jung [1] highlights that within open university environments, AI plays a crucial role in delivering customized learning pathways for thousands of students simultaneously. In the context of vocational education, Ghosh and Ravichandran [16] emphasize that immersive technologies combined with AI are essential for achieving precision in competency-based skills training. Furthermore, contemporary Outcome-Based Education (OBE) models increasingly depend on data analytics to monitor and evaluate student performance in real time [7]. However, the effectiveness of these AI-driven pedagogical systems fundamentally depends on a critical prerequisite: the integrity, accessibility, and availability of large-scale student data.

2. Privacy Vulnerabilities and the Centralization Dilemma

Dependence on Big Data introduces unprecedented inherent risks within AI-driven educational systems. Rahmatika and Sulasmi [2] emphasize that adaptive curricula require extensive access to student profiles—including learning pace and emotional responses—which, when stored within centralized architectures, become high-value targets for cyberattacks. Zou et al. [3] caution that in the absence of robust encryption mechanisms, such technological innovations may inadvertently expose students to privacy violations and commercial exploitation of personal data. Furthermore, Kaya [4], through a bibliometric analysis, confirms the presence of a persistent trust gap: despite a substantial increase in the volume of AI-related educational research, practical and comprehensive solutions for data security continue to lag behind advancements in algorithmic innovation.

3. Digital Blockchain as a Digital Trust Infrastructure

Blockchain represents a paradigm shift from traditional perimeter-based security models, such as firewalls, toward consensus-based security mechanisms. Fundamentally, blockchain functions as an immutable distributed ledger that enhances data integrity and resilience. Nazari et al. [8] explain that within non-formal education systems, particularly the Blockchain and Artificial Intelligence Non-Formal Education System (BANFES), this decentralized structure ensures that educational records cannot be altered or manipulated by either corrupt administrators or external attackers. Samuels and Singh [11] further conceptualize blockchain as a technological catalyst for developing countries, enabling them to leapfrog conventional infrastructures by establishing robust educational systems without reliance on costly and vulnerable centralized server architectures. Moreover, the implementation of smart contracts facilitates the automation of administrative processes—such as diploma issuance—in a manner that is transparent, verifiable, and less susceptible to human bias [7].

4. Ethical Convergence: Data Sovereignty and Sustainability

Contemporary scholarly discourse increasingly extends beyond technical considerations to encompass ethical and sustainability dimensions. The concept of Self-Sovereign Identity (SSI) has emerged as a prominent solution to persistent privacy challenges in digital education systems. Ahmad et al. [10] argue that within inclusive educational environments, students must retain full control over their digital identities in order to prevent discrimination and ensure equitable access to learning opportunities. Concurrently, the environmental implications of blockchain technology have begun to attract significant academic attention. Kıyak [12] critically examines the substantial carbon footprint associated with conventional blockchain protocols and proposes Holochain as a more environmentally sustainable alternative, particularly within medical education and planetary health contexts. This growing body of literature reflects an increasing technological maturity, suggesting that advancements in data security and digital trust infrastructures should no longer come at the expense of ecological sustainability.

B. Research Methodology

1. Research Design

This study uses a Systematic Literature Review (SLR) approach. This method was chosen for its ability to identify, evaluate, and interpret all available research on a particular topic objectively and transparently [11]. This approach allows researchers to map the latest developments in the integration of Blockchain and AI, as well as identify gaps in the existing literature. The reporting protocol in this study was compiled following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure the validity and reproducibility of the selection process.

2. Literature Search Strategy

The literature search process was guided by the PICO (Population, Intervention, Comparison, Outcome) framework to formulate specific and focused research questions.

Table 1. PICO Framework

Component	Specifications
Population (P)	AI-based Education Systems
Intervention (I)	Blockchain Technology Integration
Comparison (C)	Centralized Database Architecture
Outcomes (O)	Improved Student Data Privacy and Security

3. Data Sources and Selection Process

The search was conducted electronically through the Directory of Open Access Journals (DOAJ) and IEEE Xplore. This database was selected based on the principles of accessibility and transparency in global research. The search string used was a combination of Boolean operators: (blockchain AND "artificial intelligence" AND "education").

To ensure the quality and relevance of the studies, strict inclusion and exclusion criteria were applied:

Table 2. Selection Criteria (Inclusion and Exclusion)

Criteria	Inclusion	Exclusion
Time Range	Last 5 Years (2021–2026)	Articles published before 2021
Language	English	Languages other than English
Publication Type	Scientific Journal Articles (Peer-reviewed)	Conference proceedings, theses, book chapters, editorials
Subject	Education	Purely technical without an educational context
Relevance	Focus on security, privacy, or data architecture	Does not discuss technology integration or data security

4. Data Collection and Analysis Procedures

The selection process was conducted through multi-stage screening following the PRISMA flow diagram:

a. Identification: The initial search yielded 873 articles. DOAJ (186) and IEEE Xplore (687).
b. For IEEE Xplore: When only open access documents are included, 61 remain; the total number of documents is 247.
c. Initial Screening (Year): Restricting the time range (2021–2026) left 236 articles.
d. Quality Screening (Source Type): Elimination of non-journal articles to ensure peer-review standards, leaving 209 articles.
e. Relevance Screening (Subject & Abstract): Manual review of titles and abstracts to ensure suitability for the context of education and data security. This stage left 23 articles.

f. Feasibility (Language): Final selection of English resulted in 20 final articles.

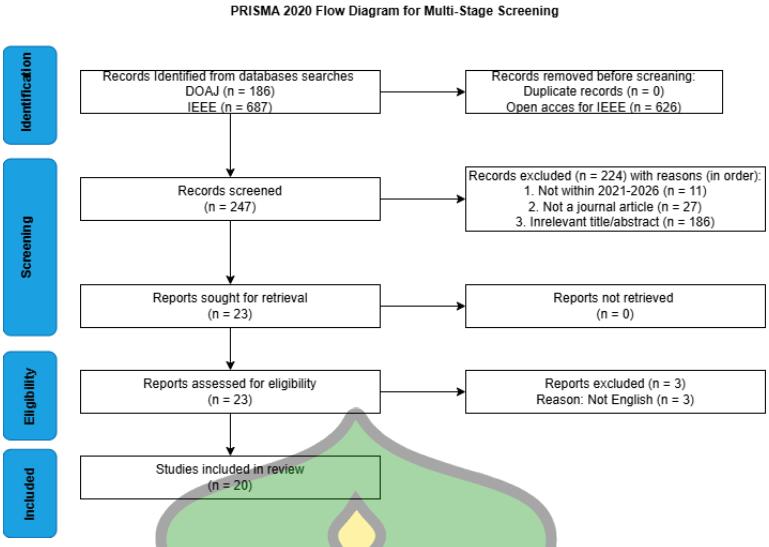

Figure 1. Prisma Flow

5. Quality Assessment Procedure

In accordance with the need for methodological transparency, all articles that pass the initial screening stage undergo a quality evaluation using a critical assessment instrument. Each study is evaluated based on three main parameters:

a. Clarity of the research objectives and appropriateness of the methodology used.
b. Depth of analysis regarding data vulnerabilities in centralized AI systems.
c. Contribution of findings to the development of secure educational architectures. Only articles meeting the minimum score on these criteria proceed to the final synthesis stage, resulting in a total of 20 high-quality articles as the research database.

6. Data Extraction and Synthesis Analysis

Data from the selected literature was processed using Narrative Synthesis Analysis techniques. This process began by extracting crucial information—such as the proposed system architecture, tested security parameters, and integration effectiveness results—into a data extraction matrix. Synthesis is then performed deductively to compare blockchain performance against traditional databases in handling AI data loads, without using thematic coding procedures. This approach enables an in-depth analysis of the Self-Sovereign Identity (SSI) concept and decentralized identity management as solutions to data leakage risks in educational environments.

RESULTS

A. Characteristics and Distribution of the Literature (Quantitative Analysis)

Prior to conducting an in-depth synthesis, a descriptive analysis was performed on 20 articles that met the eligibility criteria to identify current research trends. The distribution of publication years was dominated by recent literature, with 7 articles published in 2025, 9 in 2024, 2 in 2023, and 2 in 2022. This trend indicates a significantly increasing urgency regarding the implementation of decentralized technology in the era of artificial intelligence (AI).

From a methodological perspective, the studies fall into three main categories: 30% used Systematic Literature Review (SLR) or Bibliometric Analysis methods [2], [3], [4], [10], [11], [13]. A further 30% proposed new system architectures validated through simulation or network experiments [5], [8], [9], [15], [17], [18], and 40% used conceptual analysis and case studies [1], [6], [7], [12], [14], [16], [19], [20]. To strengthen the validation of blockchain's effectiveness in securing the flow of sensitive data, 25% of the total articles are cross-domain studies from the medical sector, which shares similar data vulnerability characteristics with student records in the education sector [6], [14], [15], [18], [20].

B. Literature Synthesis Matrix

Table 3 presents a comprehensive synthesis of the 20 evaluated articles. This matrix maps the specific methodologies of each study and their direct contributions to the PICO framework parameters (specifically data security and privacy outcomes).

Table 3. Selected Literature Synthesis Matrix

Author (Year)	Research Focus	Methodological Approach	Specific Contribution to Data Security/Privacy (PICO Outcome)
Ahmad et al. (2024)	Inclusive Learning & Industry 4.0	Literature Review	The use of blockchain to ensure transparency in credentialing processes, thereby mitigating bias and ensuring accessibility.
Ali (2024)	*Summative Assessment in Outcome-Based Education*	Framework Development	Blockchain provides an immutable, decentralized ledger for securely recording assessment data.
Ghosh & Ravichandran (2024)	Vocational Education	Conceptual Review	Blockchain improves information management, safeguards data privacy, and facilitates secure digital certification.
Jung (2024)	Personalization at the Open University	Conceptual Analysis	Blockchain provides transparency and tamper-proof records of academic achievements in large-scale education systems.
Kaya (2024)	AI Bibliometric Analysis	Network & Bibliometric Analysis	AI adoption continues to rise, but new infrastructure is needed because ethical and privacy issues have not yet been fully resolved.
Kıyak (2023)	The Carbon Footprint of the Healthcare and Education Systems	A Critical Review	Proposing Holochain, with its agent-centric paradigm, as a far more energy-efficient alternative to conventional blockchains.
Nazari et al. (2024)	Non-Formal Education (BANFES)	Smart Contract Simulation	Securing the integrity of academic records using a decentralized, intermediary-free ecosystem.
Rahmatika & Sulasmi (2025)	Technology-Based Curriculum	Systematic Review	Conclude that student data privacy is a major challenge for personalized curricula, requiring regulatory measures and protective technologies.
Samuels & Singh (2025)	Higher Education in the Fourth Industrial	Literature Review	The use of blockchain and AI is crucial for record-keeping integrity, but faces challenges related to accessibility and infrastructure.

	Revolution		
Wang et al. (2025)	Biotechnology Education (Adaptive Learning)	Architectural Review	Blockchain is recommended for securing micro-credential certifications to verify the authenticity of competencies in a tamper-proof manner.
Zou et al. (2025)	21st-Century Technology Integration	Literature Review	Blockchain provides a secure and tamper-proof record of academic achievements, supporting AI-driven personalized learning.
Yang et al. (2024)	Federated Learning (MS-FL)	Machine Learning Simulation	The aggregation algorithm ensures that participants' data privacy is not compromised while maintaining the model's robustness against poisoning attacks.
Puri et al. (2025)	Decentralized Machine Learning	System Experiments (IPFS & Smart Contracts)	Storing AI models in a decentralized manner mitigates failures and enables secure data sharing without exposing raw data.
Mahmood et al. (2025)	Medical Data Sharing (Watermarking)	Review & Taxonomy	Centralized database architectures are vulnerable to hacking; decentralized systems eliminate single points of failure and protect privacy.
Nguyen-Hoang et al. (2025)	Scholarship Management with zk-Rollups	Network Implementation & Model Evaluation	Self-Sovereign Identity and ZKPs enable private application submission; zk-Rollups reduce transaction times by up to 63.6%
Ullah et al. (2024)	AICyber-Chain for Cybersecurity	System Modeling & Simulation Testnet	Automating real-time responses to AI threats with an immutable, tamper-resistant blockchain audit trail.
Ocheja et al. (2022)	Practical Case Studies on Blockchain in Education	Bibliometric Analysis & Case Studies	Most blockchain systems in education fail to integrate deep learning logs; robust API interoperability is required.
Wazid et al. (2022)	Healthcare 5.0 Security	Security Framework Design	Decentralized blockchain architecture has proven capable of protecting critical data flows from Denial of Service attacks and eavesdropping.
Zhukabayeva et al. (2024)	Post-Quantum Cryptography &	Discrete Event Simulation (DES)	Enhancing data confidentiality using post-quantum cryptography (hash-based) integrated into Hyperledger

	Hyperledger		Fabric.
Murala et al. (2023)	MedMetaverse Architecture	A Proposed Architecture	Integrating Explainable AI and Blockchain Data Records to Ensure the Accuracy and Transparency of Automated Diagnostics.

C. Thematic Synthesis and Connection to the PICO Framework

Rather than merely summarizing the literature descriptively, this analysis synthesizes the findings in depth to compare blockchain infrastructure (Intervention) with centralized databases (Comparison) in achieving privacy and security (Outcome) for AI-based systems (Population). The results of the analysis conceptualize three main dimensions:

1. Addressing the Single Point of Failure Vulnerability Through Decentralized Resilience

Artificial intelligence systems require a massive and constant supply of big data to develop accurate personalization patterns [3]. The literature critically highlights that the centralized database architecture commonly used today is vulnerable to fundamental weaknesses, namely Single Point of Failure (SPOF) and Denial of Service attacks [6], [20]. When a central server is hacked, the entire student data ecosystem can be exposed. As an intervention, blockchain technology distributes the burden of storage and management across various independent nodes [16]. Architectural models such as AICyber-Chain and IPFS storage demonstrate that a decentralized approach successfully secures data flows, prevents unilateral manipulation, and ensures system availability even in the event of a local attack on one of the networks [5], [15].

2. Self-Sovereign Identity as a Privacy Solution

There is a conceptual dilemma between the need for historical data profiles in AI algorithms and users' privacy rights [2]. A synthesis of the latest literature suggests a solution pattern involving the implementation of Self-Sovereign Identity (SSI) supported by Zero-Knowledge Proofs (ZKP) within a blockchain network [9]. Students can verify their academic qualifications for AI-powered automated recommendation systems without having to submit all raw data documents to a central institutional server [9]. On the algorithmic side, innovations such as Federated Learning allow Machine Learning models to be trained directly on each user's device in a distributed manner [17]. Only model parameter updates are sent to the network, which mitigates the risk of raw data breaches and protects the AI system from poisoning attacks that mislead the model [17].

3. Efficiency, Scalability, and Continuous Adaptation

Although decentralized systems have proven to offer significant comparative advantages in terms of security over centralized systems, their mass adoption is often hindered by computational inefficiencies and consensus costs [13]. As a new conceptual adaptation, the literature proposes Layer-2 scalability models such as zk-Rollups, which can bundle thousands of transactions into a single compact cryptographic proof; these have been shown to increase processing speed and reduce transaction costs by nearly 90% without sacrificing decentralization [9]. From an ecological preservation perspective, alternative protocols like Holochain offer an agent-centric architecture that does not require energy-intensive mining processes, as seen in Proof-of-Work consensus [12]. Meanwhile, the integration of Post-Quantum Cryptography (PQC) and Explainable AI (XAI) ensures that the system remains transparent and resilient against future hacking attempts [14], [18]. The synergy between these intelligent, energy-efficient computing models and high-level cryptographic validation forms the foundation for realizing digital education that is not only cutting-edge in AI but also secure and sustainable

DISCUSSION

This study aims to evaluate the effectiveness of blockchain technology as an infrastructure for safeguarding privacy and data integrity in AI-based education systems. Based on a synthesis of 20 recent literature articles, the research results explicitly address this objective by confirming that decentralized architectures offer an absolute advantage in mitigating the inherent security risks of centralized AI systems. A critical analysis of the findings in the results section crystallizes into three main interpretations, along with their implications for the development of educational technology theory and practice.

A. Deconstructing the Single Point of Failure Paradigm in the AI Ecosystem

The literature consistently highlights the vulnerability crisis plaguing educational systems when AI algorithms are forced to rely on centralized data architectures [3]. Interpretation of these findings suggests that the "walled garden" model on institutional servers is no longer a protective mechanism, but rather a major point of failure or Single Point of Failure (SPOF). A failure in a single central server due to a cyberattack (Denial of Service) automatically paralyzes all AI analytical capabilities and exposes students' sensitive data on a massive scale.

Interestingly, validation of blockchain's effectiveness does not stem solely from educational literature but is empirically reinforced by cross-domain studies from the medical sector (Healthcare 5.0) analyzed in this review [6], [20]. The shared vulnerability characteristics between medical records and academic records demonstrate that the transition to a distributed ledger is a fundamental necessity. In decentralized infrastructures such as IPFS and smart contracts, system resilience (survivability) increases drastically due to the distributed nature of the entire database [5], [15]. This revolutionizes how educational institutions view cybersecurity: shifting from a focus on "building higher server walls" to "distributing data so that no single target can be destroyed."

B. Resolving the Personalization vs. Privacy Paradox through Advanced Cryptography

The most critical dilemma in the application of AI in the education sector is the trade-off between personalization and privacy. To develop adaptive curricula, AI algorithms require highly granular predictive data streams, which logically increases the risk of digital surveillance that violates student privacy [2].

This discussion finds that blockchain does not merely operate through data sovereignty or Self-Sovereign Identity (SSI). Instead of submitting raw data to institutional servers, students retain full control over their credentials. Algorithmic findings from the studies by Yang et al. [17] on Federated Learning and Nguyen-Hoang et al. [9] regarding Zero-Knowledge Proofs (ZKP) provide a clear operational foundation: students do not reveal any of their raw data. Interpretation of these findings confirms a paradigm shift in data ownership; institutions can still leverage the precision of AI analytics without triggering risks of privacy breaches or algorithmic bias.

C. Overcoming Ecological and Computational Challenges in Sustainable Infrastructure

Although decentralized interventions have proven superior in terms of security, this analysis rejects the utopian narrative surrounding blockchain. A critical interpretation of the literature's findings indicates that the integration of AI algorithms requiring high-speed computation with conventional blockchain networks (particularly Layer-1) results in cost inefficiencies and extreme scalability barriers [13].

As an architectural evolution aligned with the goals of sustainable education, the literature points to two specific innovations: the adoption of Layer-2 networks (zk-Rollups), which can significantly reduce transaction time and costs [9], and the shift toward agent-centric protocols like Holochain, which have proven to be far more energy-efficient compared to Proof-of -Work mechanisms [12]. This demonstrates that the future of AI and blockchain integration in education cannot be measured solely by its level of cryptographic resilience, but must also be evaluated based on its carbon footprint and operational efficiency.

CONCLUSION

The integration of blockchain technology into artificial intelligence (AI)-based education systems has proven to be not merely a theoretical concept but an empirical architectural solution to address the Single Point of Failure (SPOF) vulnerability in centralized databases. This systematic review confirms that decentralization mechanisms combined with Self-Sovereign Identity (SSI) and Zero-Knowledge Proofs (ZKP) can resolve the privacy paradox. This technology restores data sovereignty to students while still facilitating the need for big data to safely personalize AI algorithms.

This study contributes a conceptual framework that integrates Federated Learning (AI), data sovereignty, and decentralized cryptography, while validating the feasibility of adopting cross-domain security architectures (such as Healthcare 5.0) into the digital education ecosystem. From a practical and policy perspective, these findings urge Ed-Tech developers and educational institutions to transition to hybrid storage models. To address scalability and carbon footprint challenges, future infrastructure policies must prioritize energy-efficient, low-latency decentralized protocols such as Layer-2, zk-Rollups, or Holochain.

This study has several limitations, particularly regarding the scope of the search, which relied solely on the DOAJ and IEEE Xplore databases, as well as the relatively small sample size of the literature (20 articles), given that this topic is still in the early stages of development (niche). To complement these findings, further research is recommended to:

1. Expand the literature search to other global databases such as Scopus or Web of Science to enrich the bibliometric analysis.
2. Conduct empirical testing and real-time simulations of the implementation of a hybrid architecture

prototype (AI and blockchain) in a university or school environment to accurately measure system latency and scalability.

3. Assess the digital literacy readiness of educators and students in using self-sovereign identity (SSI) wallets as data governance tools.

REFERENCES

[1] I. Jung, "Personalized Education for All : The Future of Open Universities," vol. 16, no. 2024, pp. 24–36, doi: 10.55982/openpraxis.16.1.612.

[2] A. Rahmatika and E. Sulasmi, "Primary : Jurnal Pendidikan Guru Sekolah Emilda Dasar," no. 2021, pp. 166–177, 2025.

[3] Y. Zou, F. Kuek, W. Feng, and X. Cheng, "Digital learning in the st century : trends , challenges , and innovations in technology integration," 2023.

[4] D. Kaya, "Sakarya University Journal of Education," vol. 14, no. 3, pp. 447–472, 2024.

[5] Z. I. A. Ullah, A. Waheed, M. I. Mohmand, and S. Basar, "AICyber-Chain : Combining AI and Blockchain for Improved Cybersecurity," vol. 12, no. July, 2024.

[6] S. D. Mahmood, F. Drira, and S. Member, "Secure Medical Image Sharing : Technologies , Watermarking Insights , and Open Issues," no. June, pp. 103995–104026, 2025.

[7] Q. I. Ali, "Towards more effective summative assessment in OBE : a new framework integrating direct measurements and technology," *Discov. Educ.*, 2024, doi: 10.1007/s44217-024-00208-5.

[8] S. Banfes, Z. Nazari, and A. R. Vahidi, "education sciences Blockchain and Artificial Intelligence Non-Formal Education," pp. 1–36, 2024.

[9] N. C. U. Hoang and P. H. U. T. Hua, "Advancing Scholarship Management : A Blockchain-Enhanced Platform With Privacy-Secure Identities and AI-Driven Recommendations," vol. 13, no. November 2024, 2025.

[10] I. Ahmad *et al.*, "Inclusive learning using industry 4 . 0 technologies : addressing student diversity in modern education," *Cogent Educ.*, vol. 11, no. 1, p., 2024, doi: 10.1080/2331186X.2024.2330235.

[11] A. B. Samuels and U. Singh, "Education reimagined : South Africa ' s journey through the 4IR and beyond," pp. 1–13, 2024.

[12] Y. S. Kıyak, "Blockchain and Holochain in Medical Education from Planetary Health and Climate Change Perspectives," pp. 79–85, 2023, doi: 10.6018/edumed.560681.

[13] P. Ocheja, F. J. Agbo, S. S. Oyelere, B. Flanagan, H. Ogata, and S. Member, "Blockchain in Education : A Systematic Review and Practical Case Studies," *IEEE Access*, vol. 10, no. July, pp. 99525–99540, 2022, doi: 10.1109/ACCESS.2022.3206791.

[14] D. K. Murala, S. K. Panda, and S. P. Dash, "MedMetaverse : Medical Care of Chronic Disease Patients and Managing Data Using Artificial Intelligence , Blockchain , and Wearable Devices State-of-the-Art Methodology," vol. 11, no. October, 2023.

[15] V. Puri, I. Priyadarshini, A. Kataria, S. Rani, and H. Min, "Privacy-First ML for Chronic Kidney Disease Prediction : Exploring a Decentralized Approach Using Blockchain and IPFS," *IEEE Access*, vol. 13, no. November 2024, pp. 43178–43189, 2025, doi: 10.1109/ACCESS.2025.3548645.

[16] L. Ghosh and R. Ravichandran, "Emerging Technologies in Vocational Education and Training," vol. 04, no. 1, pp. 41–49, 2024, doi: 10.52562/jdle.v4i1.975.

[17] W. Yang, P. Kang, and C. Wei, "MS-FL : A Federated Learning Framework Based on Multiple Security Strategies," *IEEE Access*, vol. 12, no. November 2023, pp. 8912–8923, 2024, doi: 10.1109/ACCESS.2024.3353131.

[18] T. Zhukabayeva and A. U. R. Rehman, "Hyperledger Fabric-Based Post Quantum Cryptography for Healthcare Application Using Discrete Event Simulation," *IEEE Access*, vol. 12, no. December, pp. 192482–192493, 2024, doi: 10.1109/ACCESS.2024.3513153.

[19] T. Wang and F. R. Trejo-macotela, "Revolutionizing biotech and pharmaceutical education with adaptive learning," no. November, pp. 1–17, 2025, doi: 10.3389/feduc.2025.1679222.

[20] M. Wazid and S. Member, "Healthcare 5 . 0 Security Framework : Applications , Issues and Future Research Directions," *IEEE Access*, vol. 10, no. November, pp. 129429–129442, 2022, doi: 10.1109/ACCESS.2022.3228505.

***M. Zian Al Farisi. Bz (Corresponding Author)**
Department of Information Technology,
UIN Ar-Raniry,
Jl. Syeikh Abdur Rauf, Syiah Kuala, Banda Aceh, Aceh, 23239, Indonesia
Email: 200705049@student.ar-raniry.ac.id

Khairan AR
Department of Information Technology,
UIN Ar-Raniry,
Jl. Syeikh Abdur Rauf, Syiah Kuala, Banda Aceh, Aceh, 23239, Indonesia
Email: khairan.ar@ar-raniry.ac.id

Malahayati
Department of Information Technology,
UIN Ar-Raniry,
Jl. Syeikh Abdur Rauf, Syiah Kuala, Banda Aceh, Aceh, 23239, Indonesia
Email: malahayati_umar@ar-raniry.ac.id

Hendri Ahmadian
Department of Information Technology,
UIN Ar-Raniry,
Jl. Syeikh Abdur Rauf, Syiah Kuala, Banda Aceh, Aceh, 23239, Indonesia
Email: hendri@ar-raniry.ac.id

Media Elektrik
Teknik Elektro Universitas Negeri Makassar
e-ISSN 2721-9100

Letter of Acceptance
Nomor: LOA202601282575

Dear Sir.

M. Zian Al Farisi. Bz
Universitas Islam Negeri Ar-Raniry

Thank you for submitting a scientific article to be published in **Media Elektrik** (E-ISSN: 2721-9100) published by the Department of Electrical Engineering Education, Faculty of Engineering, Universitas Negeri Makassar with the title:

BLOCKCHAIN FOR SECURITY AND PRIVACY IN AI-BASED EDUCATION: A SYSTEMATIC LITERATURE REVIEW

Based on the results of the review team's examination, the article was declared ACCEPTED, with revisions to be published in Volume 23, Number 2, April, 2026. This information has been conveyed, and for his attention, thank you. We will provide you with information regarding the publication of your journal via email.

The authenticity of the LOA can be checked by scanning the QR code on the side!

LOA202601282575

Makassar, 28 Januari 2026
Editor in Chief

Muhammad Yusuf Mappeasse

Media Elektrik

M. Zian Al Farisi. Bz