Suraj Kumar Sahu, et. al. International Journal of Engineering Research and Applications
www.ijera.com
ISSN: 2248-9622, Vol. 16, Issue 8, August 2026, pp 55-64

RESEARCH ARTICLE OPEN ACCESS

Integrating Advanced Encryption Standard and Blockchain Technology for Secure Educational Record Management: A Systematic Literature Review

Suraj Kumar Sahu[1], Aradhana Kumari Singh[2]
[1]*Research Scholar, Department of Computer Science & Engineering, MATS School of Engineering & IT, MATS University, Aarang, Raipur (C.G.), India*
[2]*Associate Professor, Department of Computer Science & Engineering, MATS School of Engineering & IT, MATS University, Aarang, Raipur (C.G.), India*

ABSTRACT—
The digitization of academic record-keeping has increased the exposure of sensitive student data to unauthorized access, tampering, and centralized single points of failure. Advanced Encryption Standard (AES) and blockchain technology have separately been proposed as solutions to the confidentiality and integrity challenges in educational record management, yet a unified understanding of how these two technologies can be combined into a comprehensive privacy-preserving framework remains limited. This paper presents a systematic literature review of research on AES-based encryption, blockchain-based educational record systems, and hybrid AES-blockchain architectures. A structured search of academic databases (IEEE Xplore, Scopus, Web of Science, Springer, MDPI, and ACM Digital Library) combined with backward and forward citation tracing yielded a corpus of sources spanning cryptography, distributed ledger technology, and educational informatics, which were screened, categorized, and synthesized thematically. The review finds that AES-centric studies emphasize confidentiality but rarely provide decentralized validation; blockchain-centric studies ensure immutability and transparency but frequently omit strong encryption layers for the underlying data; and hybrid AES-blockchain approaches are concentrated in the healthcare domain rather than education. Building on these findings, the paper identifies specific research gaps — in particular, the absence of a unified framework combining AES-256 encryption, SHA-256 integrity verification, permissioned blockchain, and smart-contract-based role-based access control across the complete student-record lifecycle — and proposes directions for future research.
Keywords—*Advanced Encryption Standard; Blockchain; Educational Records; Data Privacy; SHA-256; Smart Contracts; Systematic Review; Student Data Security*

Date of Submission: 11-08-2026 Date of acceptance: 23-08-2026

I. Introduction

Educational institutions increasingly rely on digital platforms to store and process academic transcripts, personal information, and certification records. This transition improves accessibility and administrative efficiency but simultaneously exposes student data to cyberattacks, insider misuse, and single points of failure inherent in centralized databases. Reports on cyber-incidents affecting the education sector consistently identify it among the most targeted sectors for data breaches, underscoring the urgency of robust data-protection mechanisms tailored to academic environments.

Two technological approaches have received particular attention in the literature. The first, symmetric cryptography — most notably the Advanced Encryption Standard (AES) — addresses confidentiality by rendering stored and transmitted data unreadable without the correct key. The second, blockchain technology, addresses integrity and trust through a decentralized, append-only ledger that is resistant to unilateral tampering. Each approach, however, is only a partial solution: encryption alone does not prevent a centralized custodian from unilaterally altering or losing records, while blockchain alone does not, by itself, protect the confidentiality of the data referenced by its transactions.

This has motivated a growing body of work exploring hybrid architectures that combine AES-based encryption with blockchain-based integrity verification, typically by storing encrypted data off-chain while anchoring a cryptographic hash of that data on-chain. Such hybrid designs have been explored extensively in healthcare record management but remain comparatively

underexplored for the specific requirements of educational record-keeping, including academic transcripts, certificates, and role-differentiated access among students, faculty, administrators, and verification agencies. This paper systematically reviews the existing literature across these three strands — AES-based security, blockchain-based educational systems, and hybrid architectures — to consolidate the current state of knowledge and to surface concrete research gaps that motivate further work.

1.1 Objectives of the Study

Consistent with the gap identified above, this review is organized around three objectives that also define the scope of the companion design paper by the present authors. These objectives anchor the thematic categorization in Sections 3–7 and the future-research agenda in Section 8:

1. To examine, through the reviewed literature, how a hybrid security architecture combining AES-256 encryption with a permissioned blockchain network can protect sensitive student information against unauthorized access and data breaches, and to identify the design patterns (off-chain encrypted storage, on-chain SHA-256 hash anchoring) that make such integration effective (Section 5).
2. To review existing approaches to smart-contract-based role-based access control (RBAC) for secure, transparent, and auditable sharing of academic records among students, faculty members, administrators, and verification agencies, and to assess how far these approaches achieve privacy-preserving sharing without exposing sensitive student information (Section 6).
3. To consolidate the performance and security evaluation metrics — encryption/decryption time, transaction latency, throughput, storage overhead, scalability, and resistance to data tampering, unauthorized access, and replay attacks — that the literature uses to validate AES-blockchain frameworks, as a benchmark against which the proposed framework will later be evaluated (Section 7).

II. Review Methodology

A structured review process was followed to identify, screen, and synthesize relevant literature. Search queries combining terms such as “AES,” “blockchain,” “education,” “student data,” “credential verification,” “SHA-256,” “smart contract,” “role-based access control,” “attribute-based encryption,” and “zero-knowledge proof” were executed against IEEE Xplore, Scopus, Web of Science, SpringerLink, MDPI, ACM Digital Library, and arXiv. Only sources that directly addressed encryption, blockchain, or hybrid security mechanisms applicable to educational or comparable record-management contexts (e.g., healthcare, personal-data management) were retained. Duplicate records were removed, and the reference lists of highly cited works were examined for additional relevant studies (backward snowballing). Retained sources were then organized into four thematic categories: (i) AES-based confidentiality mechanisms, (ii) blockchain-based integrity and decentralization mechanisms, (iii) hybrid AES-blockchain architectures, and (iv) privacy-preserving access-control mechanisms (attribute-based encryption, zero-knowledge proofs, and smart-contract-based role-based access control).

2.1 Research Questions

This review is guided by four research questions that structure the thematic categories reported in Sections 3–6:

4. RQ1: How effectively does AES-based encryption address confidentiality requirements in educational record management, and what limitations remain?
5. RQ2: How does blockchain technology address integrity, transparency, and decentralization for educational records, and what confidentiality gaps persist in blockchain-centric designs?
6. RQ3: To what extent have hybrid AES-blockchain architectures been explored for record management, and how does adoption in the education domain compare to healthcare?
7. RQ4: What privacy-preserving access-control mechanisms (attribute-based encryption, zero-knowledge proofs, smart-contract RBAC) have been integrated with AES-blockchain designs, and what gaps remain in achieving a unified, education-specific framework covering the complete record lifecycle?

2.2 Inclusion and Exclusion Criteria

Sources were retained if they met all of the following inclusion criteria:

1. Peer-reviewed journal articles, conference papers, or established preprints (e.g., arXiv) with a clear technical treatment of AES encryption, blockchain, or hybrid security architectures in record-management contexts (educational or comparable domains such as healthcare);
2. Published in English and indexed in at least one of IEEE Xplore, Scopus, Web of Science, SpringerLink, MDPI, or ACM Digital Library, or identified

through backward/forward citation snowballing from such sources;

3. Foundational works on AES, blockchain, attribute-based encryption, or zero-knowledge proofs retained for technical grounding regardless of publication year.

Sources were excluded if they duplicated an already-retained study, lacked a clear technical treatment of encryption, blockchain, or access-control mechanisms, or were non-authoritative, non-peer-reviewed general reference material offering no unique technical contribution. The retained corpus spans publications from 2005 to 2026, reflecting both foundational cryptographic and blockchain works and recent (2024–2026) studies specific to educational systems.

2.3 Search, Screening, and Thematic Categorization

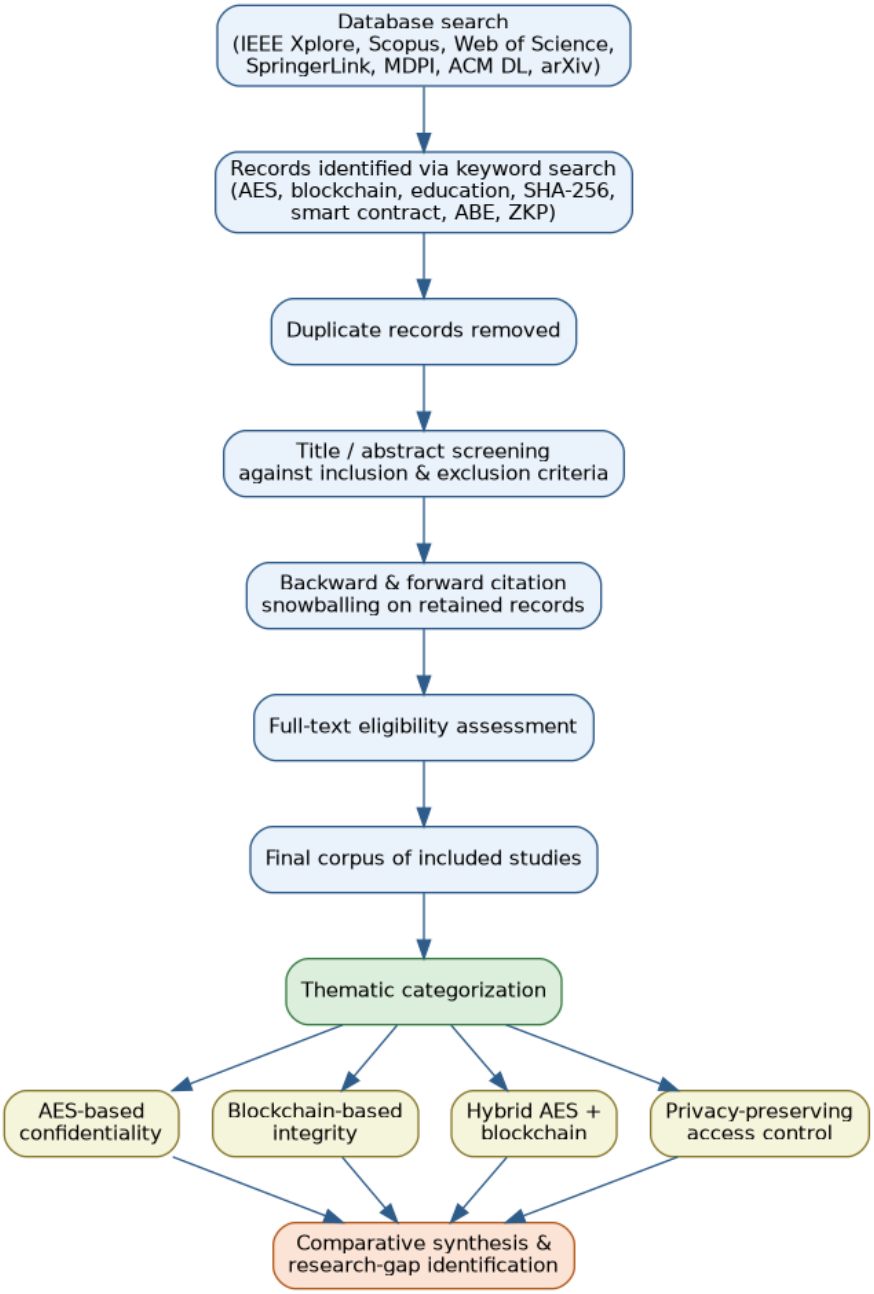

Fig. 1. Systematic review methodology: search, screening, snowballing, and thematic categorization process.

III. AES for Data Confidentiality in Educational Systems

AES was standardized by the U.S. National Institute of Standards and Technology as a symmetric block cipher operating on 128-bit blocks with key lengths of 128, 192, or 256 bits, using a substitution–permutation network [1]. Its computational efficiency and resistance to cryptanalytic attacks such as differential and linear cryptanalysis have made it the de facto standard for protecting data at rest and in transit [1], [2].

Within educational contexts specifically, several studies have applied AES to protect academic information systems, database fields, and file-level student records, reporting favorable trade-offs between security strength and processing overhead for typical institutional workloads [3]–[6]. Cloud-hosted academic information systems have combined AES with complementary mechanisms such as RSA-based key exchange to address the symmetric key-distribution problem inherent to AES-only designs [7], [8]. Across this body of work, a consistent limitation emerges: AES-centric proposals secure the confidentiality of data at the point of storage but do not, on their own, provide a decentralized, tamper-evident record of who accessed or modified that data, nor do they eliminate the single point of failure represented by the centralized database or key-management server.

IV. Blockchain Technology for Integrity and Decentralization in Education

Blockchain is a distributed ledger in which data is organized into cryptographically linked blocks, each referencing the hash of its predecessor, such that any retroactive modification is immediately detectable [9], [10]. Beyond its origin in cryptocurrency, blockchain has been applied to certificate issuance and verification [11]–[16], academic-credential management on Hyperledger Fabric and comparable permissioned platforms [17]–[23], self-sovereign identity for students [24], and broader educational digital-asset management [25]–[27]. Systematic reviews and bibliometric analyses of this literature confirm rapid growth in blockchain-in-education research, with credential verification and academic-record management identified as the dominant application clusters [28]–[31].

A recurring theme across these studies is a preference for permissioned or consortium blockchain architectures — such as Hyperledger Fabric — over public platforms such as Bitcoin or Ethereum, owing to their higher transaction throughput, lower latency, finer-grained access control, and suitability for institutional governance models in which only verified institutions participate in ledger validation [19], [20], [22]. However, the majority of these blockchain-centric proposals focus primarily on credential or certificate verification rather than the confidentiality of the full underlying student record, and few incorporate a strong, explicit encryption layer for the data referenced by blockchain transactions.

V. Hybrid AES + Blockchain Architectures

A smaller set of studies has explored combining AES encryption with blockchain-based integrity verification. The general pattern is to encrypt sensitive data using AES, store the ciphertext in off-chain storage such as a cloud database or the InterPlanetary File System (IPFS), compute a SHA-256 hash of the encrypted data, and record only that hash on the blockchain [32]–[38]. This design keeps blockchain storage requirements manageable while preserving tamper-evidence: any change to the off-chain ciphertext produces a hash mismatch upon recomputation, revealing tampering without requiring the blockchain itself to store bulk data.

Such hybrid designs have been most thoroughly explored in healthcare record management, where AES-encrypted patient data is anchored to a blockchain ledger for tamper-evidence and audit trails [39]. Off-chain storage solutions such as IPFS have themselves been the subject of dedicated performance and scalability studies, examining trade-offs between retrieval latency, data-availability guarantees, and integration complexity relative to conventional cloud storage [40]–[45]. Comparatively few studies, however, adapt this hybrid AES-plus-hash-anchoring pattern specifically to the educational domain, where record types (transcripts, certificates, disciplinary records, personal information) and stakeholder roles (students, faculty, administrators, external verifiers) differ materially from healthcare workflows.

Reframed against Objective 1 of this review, the reviewed hybrid designs converge on a small set of architectural layers that a permissioned-blockchain education framework must instantiate: (a) a symmetric-encryption layer, typically AES-256 in CBC or GCM mode, applied to the raw record before it ever leaves institutional custody; (b) an off-chain storage layer — a managed database or a content-addressed store such as IPFS — that holds the ciphertext and is decoupled from the ledger to avoid on-chain storage-cost and scalability penalties \[39\]–\[45\]; (c) an integrity layer that computes a SHA-256 digest of the ciphertext at write time and re-computes it at read time, so that any unauthorized modification of the off-chain payload is detected by hash mismatch rather than by trusting the storage provider; and (d) a permissioned-ledger layer —

most commonly Hyperledger Fabric in the surveyed studies \[19\], \[20\], \[22\] — that anchors the hash, the record metadata, and the access-transaction history, giving institutional participants a shared, tamper-evident audit trail without exposing plaintext data to the network. None of the reviewed hybrid studies, however, instantiate all four layers together for the specific record types and multi-stakeholder governance model of higher education, which is precisely the gap Objective 1 is intended to close in the companion design paper.

Fig. 2 traces this layered pattern end to end, from the point a raw student record enters institutional custody through to the moment a role-checked requester either receives a decrypted record or triggers a logged tamper alert. The write path (encrypt → store off-chain → hash → anchor on-chain) and the read path (request → retrieve → re-hash → verify → decrypt) are deliberately symmetric: whichever party audits the system can regenerate the write-time hash from the read-time ciphertext and compare it against the immutable on-chain value, which is what gives the architecture its tamper-evidence property without requiring the blockchain to store the record itself.

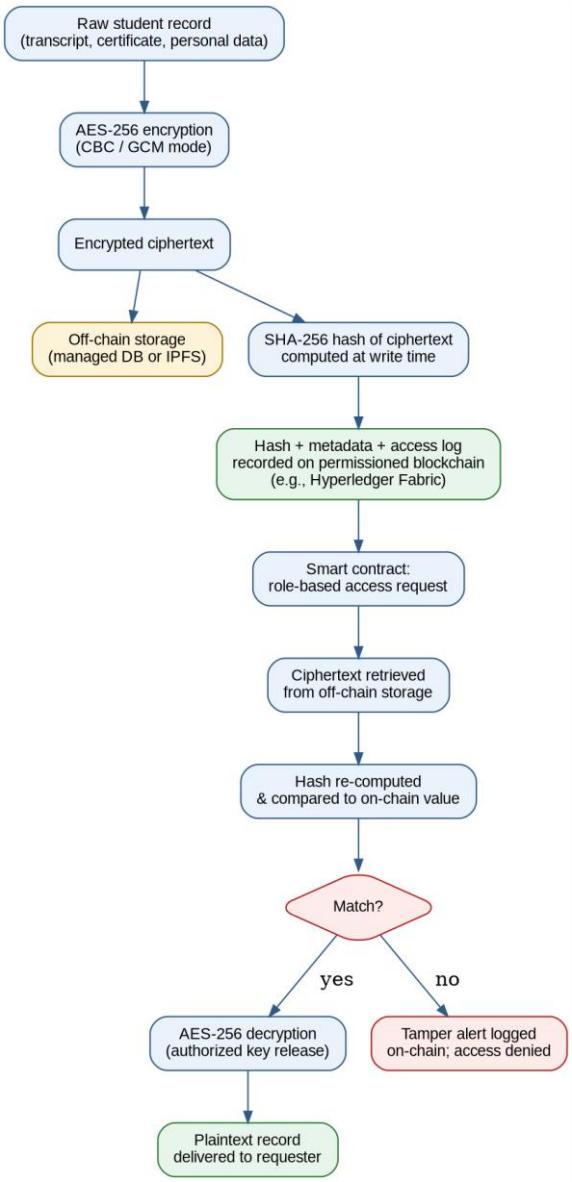

Fig. 2. Hybrid AES-256 + permissioned-blockchain architecture: write path (encrypt, store off-chain, hash, anchor) and read path (request, retrieve, verify, decrypt).

VI. Privacy-Preserving Access Control Mechanisms

Beyond confidentiality and integrity, several studies address controlled, auditable sharing of encrypted records. Attribute-Based Encryption (ABE) enables fine-grained access control by binding decryption capability to attributes rather than fixed identities, allowing flexible policies such as “only faculty of a given department may decrypt” without re-encrypting data for every new recipient [46]–[50]. Zero-Knowledge Proofs (ZKPs) allow a party to prove a credential claim (e.g., degree completion) without revealing the underlying

record, and have been applied to blockchain-based academic-record verification to reconcile transparency with privacy regulations such as the GDPR [51]–[54].

Smart-contract-based Role-Based Access Control (RBAC) has also been proposed as a decentralized alternative to centralized authorization servers, encoding role assignment, grant, and revocation logic directly into blockchain transactions [51]–[54]. The interaction between blockchain immutability and data-protection regulation — particularly the GDPR "right to be forgotten" — has itself become an active research area, generally converging on the same off-chain-storage-with-on-chain-hash pattern discussed in Section 5 as a practical reconciliation mechanism [38], [55], [56].

Mapped onto Objective 2 of this review, the smart-contract RBAC studies surveyed here share a common transaction pattern — a role-assignment transaction issued by an administrator, a role-checked access-request transaction issued by a consumer of the record (faculty, employer, or verification agency), and an on-chain grant/revoke log that makes every access attempt auditable after the fact [51]–[54]. Cruz et al. \[51\] and Kamboj et al. \[52\] demonstrate that encoding this logic in a smart contract removes the need for a trusted centralized authorization server, while Lee and Lee \[53\] and Al Neyadi et al. \[54\] extend the pattern with anonymity and IoT-oriented variants, respectively. For an education-specific deployment, however, this RBAC layer only becomes privacy-preserving in the sense required by Objective 2 — auditable sharing among students, faculty, administrators, and verification agencies without exposing the underlying record — if it is composed with the encryption and hashing layers of Section 5: the smart contract should gate access to the AES-256 decryption key or to a time-boxed, re-encrypted credential rather than to plaintext data, and every grant or revoke transaction should itself be logged as an immutable, hash-anchored event. None of the reviewed RBAC-only studies specify this composition explicitly, which the present review identifies as the second concrete implementation gap for the companion framework.

Fig. 3 illustrates this composed grant/revoke transaction pattern. An administrator's role assignment and every subsequent access decision — grant, denial, expiry, or revocation — is written to the permissioned ledger as its own transaction, so the complete history of who could see a given record, and for how long, is reconstructable after the fact without exposing the record's plaintext content to the chain itself.

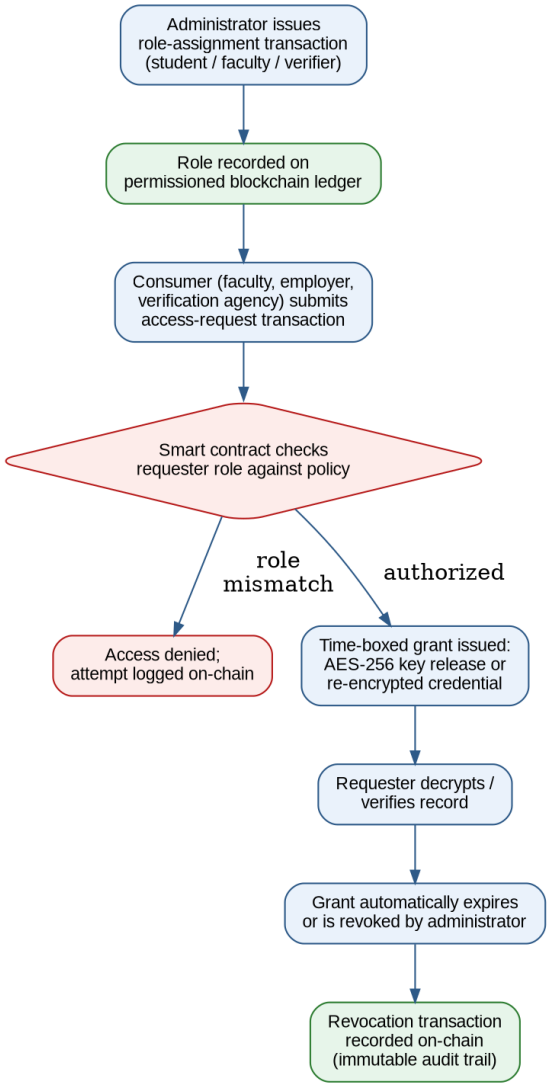

Fig. 3. Smart-contract RBAC flow: role assignment, role-checked access request, time-boxed key/credential grant, and on-chain revocation audit trail.

VII. Comparative Synthesis and Research Gaps

Synthesizing the reviewed literature yields three consistent observations. First, AES-centric studies achieve strong confidentiality guarantees but generally rely on centralized storage and key management, reintroducing single points of failure and offering no independent, tamper-evident audit trail. Second, blockchain-centric studies achieve decentralization, immutability, and transparent audit trails but frequently omit a rigorously specified encryption layer for the sensitive data itself, or store metadata on-chain without addressing confidentiality end-to-end. Third, hybrid AES-blockchain approaches that address both concerns simultaneously exist predominantly in the healthcare

domain; comparatively few studies adapt this pattern to the specific record types, stakeholder roles, and regulatory context of higher education.

Thematic Category	Representative Refs.	Core Strength	Key Limitation
AES-centric encryption	[3]–[8]	Strong data confidentiality at rest/in transit; efficient for institutional workloads	No decentralized integrity verification; centralized DB/key server remains a single point of failure
Blockchain-centric education systems	[11]–[31]	Immutability, transparency, decentralized trust for credential/certificate verification	Encryption layer for underlying record data is weak or absent
Hybrid AES + Blockchain (mostly healthcare)	[32]–[45]	Combines confidentiality and tamper-evidence via off-chain encryption + on-chain hash anchoring	Rarely adapted to education-specific record types and stakeholder roles
Access-control layers (ABE / ZKP / RBAC)	[46]–[56]	Fine-grained, auditable, privacy-preserving sharing and verification	Rarely integrated into a single unified AES + blockchain + RBAC lifecycle framework

Table 1. Comparative synthesis of the four reviewed thematic categories.

A further gap concerns the integration depth of access-control mechanisms. While ABE, ZKP, and smart-contract RBAC have each been studied individually, few reviewed works combine AES-256 encryption, SHA-256 integrity anchoring, permissioned blockchain governance, and smart-contract-based RBAC within a single, unified architecture covering the complete student-record lifecycle — from creation and encryption, through storage and sharing, to verification and revocation. This gap motivates the design of an integrated framework, which is the subject of a companion paper by the present authors.

7.1 Evaluation Metrics for Hybrid AES-Blockchain Frameworks

Addressing Objective 3, the hybrid and blockchain-centric studies reviewed in Sections 4–6 evaluate their designs against a recurring set of metrics, even though few studies report all of them together. Consolidating these into a single benchmark set gives a concrete basis for evaluating the companion framework:

8. Encryption/decryption time — the processing overhead AES-256 adds per record, typically reported in milliseconds for varying file sizes; studies in the AES-centric cluster \[3\]–\[8\] report this most consistently, but rarely alongside blockchain-side costs.
9. Transaction latency and throughput — the time to commit a hash-anchoring or access-control transaction and the sustained transactions-per-second the permissioned ledger supports; consistently favors Hyperledger Fabric over public-chain designs in the reviewed comparisons \[19\], \[20\], \[22\].
10. Storage overhead — the on-chain footprint of a SHA-256 hash and transaction metadata relative to the off-chain ciphertext, and the retrieval latency of the off-chain store (cloud database versus IPFS) \[39\]–\[45\].
11. Scalability — how latency, throughput, and storage overhead behave as the number of records, participating institutions, or concurrent access requests grows, a dimension the reviewed studies treat least rigorously.
12. Resistance to data tampering, unauthorized access, and replay attacks — evaluated through hash-mismatch detection tests, unauthorized-decryption attempts, and re-submission of previously valid transactions; reported qualitatively more often than through reproducible attack simulations across the reviewed corpus.

No single reviewed study reports results across all five dimensions for an education-specific deployment, which is the third concrete gap this review identifies and the benchmark set the companion framework is designed to be evaluated against.

VIII. Conclusion and Future Research Directions

This review has synthesized the literature on AES-based encryption, blockchain-based educational record systems, and hybrid AES-

blockchain architectures. The evidence indicates strong, independently mature foundations in each constituent technology, but a persistent gap in unified architectures tailored to the educational domain that combine confidentiality, integrity, decentralized governance, and fine-grained, auditable access control. Future research should prioritize the three objectives set out in Section 1.1: (i) empirical, education-domain-specific implementations of a hybrid AES-256-plus-permissioned-blockchain architecture, instantiating the four layers identified in Section 5 and reporting performance benchmarks (encryption/decryption latency, transaction throughput, storage overhead); (ii) smart-contract RBAC implementations that gate keys or re-encrypted credentials rather than plaintext, composed with the encryption and hashing layers as outlined in Section 6, and evaluated for auditable, privacy-preserving sharing among students, faculty, administrators, and verification agencies; and (iii) systematic evaluation against the five-dimension benchmark set proposed in Section 7.1 (encryption/decryption time, transaction latency, throughput, storage overhead, scalability, and resistance to tampering, unauthorized access, and replay attacks), alongside regulatory-alignment studies examining how such architectures can satisfy data-protection requirements such as the GDPR without compromising blockchain immutability guarantees.

IX. Limitations of This Review

This review followed a structured but not formally registered PRISMA protocol; exact counts of records identified, screened, and excluded at each stage were not tracked during the original search and are not reported here, which limits full methodological transparency and reproducibility. Because this narrows the review to a thematic, snowball-assisted synthesis rather than a fully auditable systematic review in the PRISMA sense, the title and Section 2 should be read with that scope in mind; a future revision that repeats the search while logging per-database and per-stage counts could add a PRISMA-style flow diagram and justify the "systematic" label more rigorously. The search was limited to six databases plus citation snowballing and did not employ a formal multi-rater screening reliability check. Grey literature and non-English-language sources were not systematically searched, which may introduce publication and language bias. A citation and reference-list audit conducted for this revision corrected two mis-numbered in-text citation ranges (Section 6) that had pointed past the end of the reference list, removed one duplicated reference entry, and independently verified the author list for one previously unverified source (Ref. [24]); one reference (Ref. [3]) still has its authorship unconfirmed against the publisher record and should be checked before submission or indexing.

References

[1] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard. Berlin, Germany: Springer, 2002.
[2] N. Ferguson and B. Schneier, Practical Cryptography. Indianapolis, IN, USA: Wiley Publishing, 2007.
[3] "Field level encryption implementation using AES-256 for secure academic information systems," JIKO (Jurnal Informatika dan Komputer), vol. 9, no. 1, 2026, doi: 10.33387/jiko.v9i1.10859. [Author names to be confirmed from the publisher page at https://ejournal.unkhair.ac.id/index.php/jiko before submission.]
[4] "Securing sensitive digital data in educational institutions using encryption technology," 2018.
[5] "Student data security optimization using multiple cryptography (AES and RSA) for e-Campus services," J. Ilmu Bersama, 2025.
[6] "Data security in cloud using AES," 2020.
[7] "Ensuring data storage security in cloud computing with Advanced Encryption Standard (AES) and authentication scheme," 2016.
[8] S. K. Waybhase and P. Adakane, "Data security using Advanced Encryption Standard (AES)," Int. J. Eng. Res. Technol., 2022.
[9] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Decentralized Business Review, p. 21260, 2008.
[10] N. Kshetri, "Block chain's roles in strengthening cybersecurity and protecting privacy," Telecommun. Policy, vol. 41, no. 10, pp. 1027–1038, 2017.
[11] M. Sharples and J. Domingue, "The blockchain and kudos: A distributed system for educational record, reputation and reward," in Proc. 11th Eur. Conf. Technology Enhanced Learning (EC-TEL), 2016, pp. 490–496.
[12] J. Domingue, J. M. F. López, and L. Farquhar, "Blockchain learning: Credentialing and open badges," Open University Knowledge Media Institute, 2017.
[13] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain-based accreditation and degree verification system," 2019.
[14] Y. Liu et al., "EduChain: A blockchain-based education data management system," 2023.
[15] S. Mahajan and A. Sachdeva, "Blockchain-based framework for validation and authentication of academic certificates," 2022.

[16] T. Hidayat and R. Mahardiko, "Data encryption algorithm AES by using blockchain technology: A review," BACA Journal, 2021.
[17] "A new privacy preserving protocol for academic certificates based on Hyperledger Fabric (DCVPC)," Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 14, no. 2, 2023.
[18] "A Hyperledger-based secure framework for academic certificate authentication using blockchain," Int. J. Saf. Secur. Eng. (IJSSE), vol. 15, no. 6, 2025.
[19] R. F. Ghani et al., "Blockchain-based student certificate management and system sharing using Hyperledger Fabric platform," 2022.
[20] "Enhancing academic certificate privacy with a Hyperledger Fabric blockchain-based access control approach (HLFeCERT)," 2023.
[21] "A blockchain framework for academic certificates using Hyperledger Fabric," Int. J. Adv. Comput. Sci. Appl. (IJACSA), vol. 15, no. 7, 2024.
[22] "A blockchain-based certificate management system using the Hyperledger Fabric platform," Thang Long J. Sci., 2023.
[23] "Conceptual design of a permissioned blockchain-based asset management system in higher education using Hyperledger Fabric," J. Inf. Syst. Informatics, 2026.
[24] W. Chan, K. Gai, J. Yu, and L. Zhu, "Blockchain-assisted self-sovereign identities on education: A survey," Blockchains, vol. 3, no. 1, art. no. 3, 2025, doi: 10.3390/blockchains3010003.
[25] J. Li, M. Lan, Y. Tang, S. Chen, F. Y. Wang, and W. Wei, "A blockchain-based educational digital assets management system," IFAC-PapersOnLine, vol. 53, no. 5, pp. 47–52, 2020.
[26] A. Panwar et al., "Enhancing trust and transparency in education using blockchain: A Hyperledger Fabric-based framework," Artif. Intell. Appl., 2025.
[27] "P. Chinnasamy et al., "Blockchain based electronic educational document management with role-based access control using machine learning model," Sci. Rep., vol. 15, art. no. 18828, 2025.
[28] "A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions," MDPI, 2025.
[29] "Blockchain in education: A bibliometric study and future research agenda," Cogent Educ., 2025.
[30] "Analyzing functional, technical and bibliometric trends of blockchain applications in education: A systematic review," Multimed. Tools Appl., 2024.
[31] "Blockchain-driven academic learning record management in higher education: A comprehensive review of methodologies, applications, benefits, and challenges," SN Comput. Sci., 2025.
[32] K. Yuan and F.-Y. Wang, "Blockchain and cryptography-based secure data sharing for healthcare systems," IEEE Access, vol. 6, pp. 1789–1799, 2018.
[33] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in Proc. IEEE Security and Privacy Workshops, San Jose, CA, USA, 2015, pp. 180–184.
[34] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, 2015.
[35] X. Li, M. Tan, and W. Tian, "A secure and efficient sharing framework for student electronic academic records: Integrating zero-knowledge proof and proxy re-encryption," Future Internet, vol. 18, no. 1, art. no. 47, 2026.
[36] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A zero-knowledge proof-enabled blockchain-based academic record verification system (ZKBAR-V)," Sensors, vol. 25, no. 11, art. no. 3450, 2025, doi: 10.3390/s25113450.
[37] "VeriZKP: A privacy-preserving, gas-less, and granular educational credential verification system on Ethereum using zero-knowledge proofs," 2026.
[38] M. Godyn, M. Kedziora, Y. Ren, Y. Liu, and H. H. Song, "Analysis of solutions for a blockchain compliance with GDPR," Sci. Rep., vol. 12, art. no. 15021, 2022, doi: 10.1038/s41598-022-19341-y.
[39] N. Nizamuddin et al., "IPFS: An off-chain storage solution for blockchain," in Proc. Int. Conf., Springer, 2023.
[40] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy," J. Parallel Distrib. Comput., vol. 164, pp. 152–167, 2022.
[41] M. Alizadeh, K. Andersson, and O. Schélen, "Efficient decentralized data storage based on public blockchain and IPFS," in Proc. IEEE Asia-Pacific Conf. Computer Science and Data Engineering (CSDE), 2020.
[42] S. Lamichhane and P. Herbke, "Verifiable decentralized IPFS cluster: Unlocking trustworthy data permanency for off-chain storage," arXiv:2408.07023, 2024.
[43] "Comparative security and performance evaluation of IPFS and Filecoin for off-chain blockchain storage," Indonesian J. Comput. Sci., 2025.
[44] M. Kaur, S. Gupta, D. Kumar, C. Verma, B.-C. Neagu, and M. S. Raboaca, "Delegated proof of accessibility (DPoAC): A novel consensus protocol for blockchain systems," Mathematics, vol. 10, no. 13, p. 2336, 2022.
[45] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. 13th ACM Conf.

Computer and Communications Security (CCS), 2006, pp. 89–98.
[46] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology – EUROCRYPT 2005, LNCS vol. 3494, Springer, 2005, pp. 457–473.
[47] "Implementation of Ciphertext Policy-Attribute Based Encryption (CP-ABE) for fine grained access control of university data," in Proc. IEEE Conf., 2017.
[48] G. Mahmoud et al., "Attribute-based encryption mechanisms for secure educational credentialing systems," 2020.
[49] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, "Attribute-based encryption for cloud computing access control: A survey," ACM Comput. Surv., vol. 53, no. 4, pp. 1–41, 2020, doi: 10.1145/3398036.
[50] "A formal architecture for privacy-preserving credential verification using blockchain and zero-knowledge proofs," ResearchGate preprint, 2025.
[51] J. P. Cruz, Y. Kaji, and N. Yanai, "RBAC-SC: Role-based access control using smart contract," IEEE Access, vol. 6, pp. 12240–12251, 2018.
[52] P. Kamboj, S. Khare, and S. Pal, "User authentication using blockchain based smart contract in role-based access control," Peer-to-Peer Netw. Appl., vol. 14, no. 5, pp. 2961–2976, 2021.
[53] Y. Lee and K. M. Lee, "Blockchain-based RBAC for user authentication with anonymity," in Proc. Conf. Research in Adaptive and Convergent Systems, ACM, 2019.
[54] D. Al Neyadi, D. Puthal, J. Dutta, and E. Damiani, "Role-based access control in private blockchain for IoT integrated smart contract," in Proc. 6th IFIP Int. Internet of Things Conf. (IFIPIoT), 2023.
[55] "Blockchain, personal data and the GDPR right to be forgotten," Nat. Law Rev., 2018.
[56] N. R. Veeraragavan and K. Zhang, "A position paper on GDPR compliance in sharded blockchains: Rehash of old ideas or new interesting challenges?" arXiv:2011.01367, 2020, doi: 10.48550/arXiv.2011.01367.