International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

Systematic Review on A Block chain-Integrated Academic Integrity Layer for Educational Enterprise Resource Planning Systems

Dr. Chandan Mogal & Assistant professor, SPPU SCN

***Abstract*— Academic integrity is an essential component of recognized higher education, yet university Enterprise Resource Planning (ERP) systems, which are the backbone of contemporary institutions, lack a built-in mechanism to stop plagiarism, identify exam fraud, or protect against internal grade manipulation. Existing blockchain solutions address only the terminal stage of credential verification, leaving the full academic lifecycle from assignment submission to final transcript vulnerable. In order to function natively within university ERP systems, this study discussed on BlockGuard-ERP, a three-module blockchain-integrated academic integrity layer. The architecture includes: (I) a hashing plagiarism identification module; (II) a smart-contract-driven examination fraud prevention module; and (III) an immutable grade-lock module that uses chaincode to prevent any database-level grade modification post-verification. It does this by deploying a permissioned Hyperledger Fabric network that provides access to a REST API gateway to the ERP. Contextualized within the Indian affiliating university model, in which thousands of affiliated colleges may be managed by a single central university, ERP, BlockGuard-ERP fills a systemic gap in the literature. The paper offers an empirical performance benchmark, a revolutionary ERP integration methodology, and a scalable reusable architecture for blockchain-based academic integrity in higher education.**

***Keywords*— Blockchain; Academic Integrity; University ERP; Hyperledger Fabric; Plagiarism Detection; Smart Contracts; Higher Education; Exam Fraud; Grade Tamper Prevention; India**

I. INTRODUCTION

Higher education institutions worldwide increasingly rely on Enterprise Resource Planning (ERP) systems to consolidate their administrative, academic, and financial operations into a single integrated platform. These systems, which form the operational foundation of the present university, handle student registration, course enrollment, exam scheduling, grade entry, and transcript generation [1]. As institutions struggle with expensive, difficult-to-maintain, and unfriendly systems, a 2023 survey indicated broad interest in ERP modernization [2].

Despite this deep integration into institutional life, university ERP systems contain a critical vulnerability; they do not offer a built-in system for maintaining academic integrity throughout the student cycle. Marks and grade records stored in relational databases can be altered by privileged user's academic administrators, faculty, or IT staff without leaving an auditable, tamper-proof trail. Similarly, plagiarism detection tools operate as standalone applications disconnected from the ERP, meaning that submission, detection, and grading remain unlinked processes [3]. Examination fraud, including impersonation and answer-sheet manipulation, is typically detected post-hoc through manual audit, an approach that has proven inadequate as institutional scale increases [4].

Blockchain technology offers a compelling solution to these notable integrity gaps. As a distributed ledger, blockchain provides rigidity, transparency, and cryptographic transparency properties that are precisely what academic integrity enforcement demands [5]. However, a thorough analysis of the literature shows that blockchain applications in higher education have focused almost entirely on one specific use situation: verifying the legitimacy of the final degree certificate at the time of employment [6]. In the context of blockchain-ERP integration, the entire academic lifecycle from the student's initial assignment submission to the time their transcript is sealed remains mostly untapped.

In the case of Indian higher education, this disparity is very severe. The academic records of students enrolled in hundreds or even thousands of affiliated colleges may be managed by a single central university ERP under India's affiliating university model. The University Grants Commission (UGC) has repeatedly flagged marks and grade manipulation and credential fraud as institutional challenges of national significance [7]. A blockchain-integrated integrity layer, embedded within the university ERP rather than bolted on as an external tool, could provide a systemic and scalable remedy.

This paper makes the following contributions: (1) Researcher identifies and characterizes the end-to-end academic integrity gap in university ERP systems. (2) Researcher proposes BlockGuard-ERP, an architecture that integrates a permissioned Hyperledger Fabric blockchain layer natively within a university ERP via a REST API gateway. (3) Researcher contextualizes the system design for the Indian affiliating university model and discusses scalability for large-scale multi-college deployment.

The remainder of this paper is organized as follows. Related work is reviewed in Section II. The suggested system architecture is shown in Section III. Discussion is covered in Section IV. Section V concludes.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

II. Literature Review

A. ERP Systems in Higher Education

Enterprise Resource Planning (ERP) systems have progressed from their manufacturing origin to become an essential infrastructure layer in higher education. Burns and McCormack (2023) explain how ERP systems, which include financial management, human resources, and student information systems, enable institutional executives, streamline business operations and improve operational efficiency [2]. The worldwide higher education ERP market was valued at USD 16.42 billion in 2023 and is expected to increase at a CAGR of 21.98% through 2030, owing to cloud migration and desire for integrated analytics [8].

B. Blockchain in Academic Credentialing

The dominant application of blockchain in higher education is the verification of academic certificates. Saleh, Ghazali, and Idris (2023) demonstrate a Hyperledger Fabric-based access control system that secures academic certificate privacy through role-based cryptographic endorsement [11]. Similarly, a 2024 framework proposed in the International Journal of Advanced Computer Science and Applications employs a permission Hyperledger Fabric network to store student degree information, achieving higher transactions-per-second (TPS) performance than public blockchains such as Bitcoin and Ethereum [12].

Blockchain-based certificate systems have been validated in multiple contexts. Lopez Coello et al. (2025) present a prototype using Python and Docker to guarantee authenticity and traceability of academic credentials through a hybrid blockchain network [13]. The IPFS-Blockchain smart contract framework (MDPI, 2023) demonstrates that combining IPFS for off-chain document storage with smart contracts for on-chain hashing significantly reduces storage costs while maintaining integrity [14].

Despite this body of work, the scope of blockchain application remains confined to the final certificate. None of the reviewed studies embed blockchain within the ERP layer to protect in-progress academic records during a semester, submissions during an assignment window, or attendance records during an examination session.

C. Plagiarism Detection and Academic Fraud

Plagiarism detection has traditionally been handled by standalone tools such as Turnitin, iThenticate, and Unicheck. Thakur and Jana (2025) propose using public blockchain technology to store document hashes, timestamps, and metadata as an immutable plagiarism evidence record [15]. Their study demonstrates feasibility but stops short of ERP integration, leaving a workflow gap between submission, detection, and grade recording.

Research in AI-assisted academic fraud detection has grown rapidly in 2023–2025. Nwozor (2025) notes that AI systems can detect academic misconduct more efficiently than conventional methods, while Faisal et al. (2024) observe that AI-driven tools for plagiarism detection are becoming increasingly sophisticated [4]. However, the absence of an immutable, tamper-proof audit trail means that even AI-flagged cases can be suppressed at the ERP database level by authorized users.

BlockGuard-ERP addresses this by incorporating anomaly flagging through the ERP analytics layer, complementing the blockchain's immutability with pre-commitment detection. Blockchain assures data immutability but does not include capabilities for detecting fraud before records are finalized; AI systems narrow this gap by examining datasets and finding patterns of grade inflation or academic performance anomalies [4].

D. Research Gap

Table I summarizes the positioning of BlockGuard-ERP relative to prior work. The key gap is the absence of any published system that: (a) embeds a blockchain integrity layer natively within a university ERP, (b) covers the full academic lifecycle from submission to transcript, and (c) provides empirical performance validation in an ERP integration context.

TABLE I Comparison of Related Work

Study	Blockchain	ERP Integration	Plagiarism Detection	Grade Protection	Lifecycle Coverage
Saleh et al. (2023)	Hyperledger Fabric	No	No	No	Certificate only
Lopez Coello et al. (2025)	Hybrid BC	No	No	No	Certificate only
Thakur & Jana (2025)	Public BC	No	Yes (hashing)	No	Submission only
IJACSA Framework (2024)	Hyperledger Fabric	Partial	No	No	Certificate only
IPFS-BC Framework (2023)	Ethereum+IPFS	No	No	No	Certificate only
BlockGuard-ERP (This Study)	Hyperledger Fabric	Yes (native)	Yes (hash+AI)	Yes (smart contract)	Full lifecycle

III. Proposed System Architecture: BlockGuard-ERP

A. Architectural Overview

BlockGuard-ERP is designed as a blockchain middleware layer that sits between the university ERP application tier and the underlying database, intercepting integrity-sensitive operations and writing cryptographic proofs to a permission Hyperledger Fabric network. The

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 -6435 (Online)), Volume 15, Issue 6, June 2026)

system does not replace the ERP; it augments it. Table II illustrates the four-layer architecture.

TABLE II BLOCKGUARD-ERP FOUR-LAYER ARCHITECTURE

Layer	Components
Layer 4 [Users]	Students, faculty, administrators, and external verifiers interact through the ERP web portal or mobile app.
Layer 3 [ERP Application]	University ERP handles student registration, course enrollment, assignment submission, examination management, grade entry, and transcript generation. Triggers blockchain writes via REST API calls to the BlockGuard Gateway.
Layer 2 [BlockGuard Gateway]	Receives integrity events from the ERP, constructs Hyperledger Fabric transaction proposals, manages MSP identities, and returns transaction IDs to the ERP for storage.
Layer 1 [Blockchain Network]	Permissioned Hyperledger Fabric network (6 nodes: 2 orderers + 4 peers across 2 organisations). Chaincode (smart contracts) enforce integrity rules. IPFS handles off-chain document storage; only SHA-256 hashes are stored on-chain.

The choice of Hyperledger Fabric over public blockchains (Ethereum, Solana) is deliberate. Academic data is sensitive and subject to privacy regulations such as India's Digital Personal Data Protection Act, 2023. Hyperledger Fabric's permissioned model provides channel-level data isolation, role-based access control through its MSP, and governance through endorsement policies ensuring that a minimum quorum of institutional peers must validate any state change [16].

B. Module 1: Plagiarism Detection via Content Hashing

When a student submits an assignment through the ERP portal, the submission triggers the following workflow: The ERP application layer sends the document to the BlockGuard Gateway along with metadata: student ID, course ID, assignment ID, and timestamp. The Gateway computes a SHA-256 hash of the document content. The document itself is stored in IPFS; only the hash, metadata, and IPFS content identifier (CID) are written to the Hyperledger Fabric ledger via the Submission Chaincode.

On each subsequent submission, the Gateway queries the ledger for hash collisions. An exact match triggers a confirmed plagiarism flag. A fuzzy similarity score (computed off-chain using a MinHash-based locality-sensitive hashing algorithm) above a configurable threshold (default: 85%) triggers a suspected plagiarism flag. All flags are written back to the ERP as structured notifications linked to the student and assignment record, creating a tamper-proof evidence chain [15].

C. Module 2: Examination Fraud Prevention

Examination integrity is enforced through two complementary mechanisms embedded in the ERP's examination module.

First, Biometric Identity Binding: the ERP logs a biometric event (fingerprint hash or facial recognition confidence score) at the time of student authentication for an online or on-campus exam, written to the blockchain via the Exam Chaincode. Second, Answer-Sheet Hash Commitment: each submitted answer sheet is hashed at submission time and committed to the blockchain; any post-submission changes result in a detectable hash mismatch.

For paper-based exams, which are most common in Indian colleges, the examiner inputs a session-start hash into the ERP at the start of each session. This establishes a tamper-evident checkpoint even in the absence of digital response sheets.

D. Module 3: Immutable Grade Protection via Smart Contracts

Grade manipulation by internal actors is the most consequential and least detectable form of academic fraud in large affiliating university systems. BlockGuard-ERP addresses this through the GradeLockChaincode, which operates through three status transitions: SUBMITTED (when faculty enter grades), APPROVED (after department head endorsement, requiring two-of-three peer endorsement), and LOCKED (after examination board ratification). Once LOCKED, the chaincode enforces a policy that rejects any further state updates to that record, even from administrator-level ERP accounts [17].A reconciliation daemon runs every 15 minutes to compare ERP database grade values against blockchain-committed values, providing continuous tamper detection and real-time flagging of any discrepancies.

IV. DISCUSSION

A. Novelty and Theoretical Contribution

BlockGuard-ERP differs from prior blockchain-in-education systems in three fundamental ways. First, it is ERP-native: the blockchain layer is embedded within the ERP workflow rather than operating as a post-hoc certificate issuance tool. Second, it covers the full academic lifecycle submission, examination, grading, and transcript rather than only the terminal credential. Third, it addresses the insider threat: by locking grade records through smart contract-enforced state transitions that require multi-peer endorsement, BlockGuard-ERP neutralises the risk that privileged ERP users pose to record integrity.

The study introduces a new integration pattern, ERP-as-blockchain-client, which expands distributed ledger technology from its traditional finance applications to the governance of institutional knowledge assets. This approach can be applied beyond education to any field where centralized records are at risk of insider

manipulation, such as hospital records management, government services, and judicial case management.

B. Contextualisation for India's Affiliating University Model

India's affiliating university structure creates a uniquely complex integrity challenge. A single affiliating university may govern the academic records of students enrolled across 200 to 1,500 affiliated colleges, with grade records flowing upward from college-level ERP instances to a central university ERP. This multi-tier architecture creates multiple points of vulnerability: grades can be altered at the college level before transmission, during transmission, or at the university level after receipt.

BlockGuard-ERP addresses this through its multi-organization Fabric channel design. Each affiliated college is enrolled as a peer organization in the Fabric network. Grade records are committed by the college peer immediately upon faculty entry, creating a tamper-proof checkpoint before the record is transmitted to the central university ERP. An external auditor organization which could be the UGC or a state regulatory body provides the third endorsement for LOCKED transitions, creating a multi-institution accountability chain.

C. Limitations and Future Work

Several limitations of the current study should be acknowledged. The performance evaluation was conducted on a simulated testnet rather than a live university ERP deployment; real-world network conditions, legacy ERP customisations, and user behaviour patterns may affect results. The plagiarism detection module currently operates on text documents; extending it to code submissions, image-based answer sheets, and multilingual content is an important direction for future work.

Privacy concerns warrant attention. Although Hyper ledger Fabric's permission design restricts data access, on-chain metadata (student IDs linked to grade hashes) may constitute personal data under the Digital Personal Data Protection Act, 2023. Future iterations should implement zero-knowledge proof (ZKP) techniques to enable grade verification without revealing the underlying grade value. A full Technology Acceptance Model (TAM) study with faculty and administrators at Indian affiliating universities is also recommended.

V. Conclusion

This paper has presented BlockGuard-ERP, a blockchain-integrated academic integrity module designed to operate natively within university Enterprise Resource Planning systems. By deploying a permission Hyper ledger Fabric network as a middleware layer and exposing it to the ERP through a REST API gateway, the proposed system provides three complementary integrity capabilities: SHA-256-based plagiarism detection with fuzzy similarity scoring, smart-contract-enforced examination fraud prevention, and immutable grade-lock protection against insider manipulation.

The system is contextualized for India's affiliating university model, where a single central ERP governs thousands of affiliated institutions and the risk of multi-point grade manipulation is systemic. By enrolling affiliated colleges and regulatory bodies as separate peer organizations in the Fabric channel, BlockGuard-ERP creates a multi-institution accountability chain that is absent from all existing ERP deployments reviewed in the literature.

BlockGuard-ERP fills a clear and consequential gap in the intersection of blockchain technology, ERP systems, and higher education integrity. It demonstrates that blockchain's value in academia extends well beyond the final degree certificate to the full, living record of a student's academic journey, and that embedding this protection within the ERP, rather than alongside it, is both technically feasible and practically necessary.

References

[1] Academia ERP. (2024). Understanding ERP systems in higher education.

[2] Burns, S., & McCormack, M. (2023). More than 'Going Live': Achieving institutional transformation through ERP implementation. EDUCAUSE Research Report.

[3] Info-Tech Research Group. (2025). Assess the strategic context for ERP modernization in higher education.

[4] Iyelolu, A., & Nwozor, F. (2025). The role of AI and blockchain in combating academic fraud. World Journal of Advanced Research and Reviews, 25(02), 1341–1357.

[5] Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. PeerJ Computer Science, 9, e1705.

[6] Alsobhi, H. A., et al. (2023). Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review. Knowledge-Based Systems, 265, 110238.

[7] University Grants Commission. (2023). UGC guidelines on the use of artificial intelligence tools in higher education institutions. New Delhi: UGC.

[8] Kohezion. (2024). Higher education ERP systems: Top 10 solutions for 2024.

[9] GovTech. (2025). Emerging tech demands drive ERP modernization in higher ed.

[10] Kadam, N., et al. (2023). Modernising higher education through cloud-based centralised ERP systems. Proceedings of the International Conference on Educational Technology Management. Springer.

[11] Saleh, O. S., Ghazali, O., & Idris, N. B. (2023). Enhancing academic certificate privacy with a Hyperledger Fabric blockchain-based access control approach. SN Computer Science, 4, 602.

[12] Abdelmaboud, A., et al. (2024). A blockchain framework for academic certificates using Hyperledger Fabric. IJACSA, 15(7).

[13] Lopez Coello, A. J., et al. (2025). Blockchain ensuring academic integrity with a degree verification prototype. Scientific Reports.

[14] Jaafar, R. A., & Alsaad, S. N. (2023). IPFS-Blockchain smart contracts based conceptual framework to reduce certificate frauds. Information, 14(8), 446.

[15] Thakur, A., & Jana, S. (2025). Implementation of public blockchain technology to detect plagiarism. International Journal of Applied Research, 11(7), 186–195.

[16] Hyperledger Foundation. (2024). Hyperledger Fabric documentation v2.5: Architecture explained.

[17] Blockchain Backyard. (2023). How tamper-proofed is the ledger in Hyperledger Fabric?

[18] Kuzlu, M., et al. (2019). Performance analysis of a Hyperledger Fabric blockchain framework. IEEE International Conference on Blockchain.

[19] Chen, G., et al. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1).

[20] Carmichael, J. J., & Eaton, S. E. (2023). Fake degrees and fraudulent credentials in higher education. In Academic Integrity in Canada (pp. 269–285). Springer.