IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

Secure Students Records in Block-chain Technology Using Role-Based Access Control Model

Dr. Shilpa B. Sarvaiya[1] and Neha Ravindra Deshmukh[2]
Head, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati, Maharashtra, India[1]
Student, Department of MCA, Vidya Bharati Mahavidyalaya, Amravati, Maharashtra, India[2]
sarvaiya.shilpa@gmail.com and nehadeshmukh242@gmail.com

Abstract: *Student records hold identity details, grades, attendance, disciplinary notes, and certificates, yet most institutions keep them in one central database that a single breach or a single dishonest administrator can compromise. This paper proposes a layered framework that combines a permissioned blockchain with a role-based access control (RBAC) model enforced by smart contracts. The ledger stores only hashes, access policy, student consent, and an append-only audit trail, while the record contents stay encrypted in off-chain storage. Roles such as registrar, faculty, student, and verifier receive narrowly defined permissions, with separation of duty, record ownership, and student consent acting as constraints. Corrections are saved as new linked versions instead of overwriting history, and third parties can check a credential against the ledger without contacting the institution. The work is a design and literature study: it reports no new experimental results, and every statement about earlier work is attributed to its authors. Four figures and six tables summarise the architecture, the role model, the access-check flow, the data placement, the threats, and the limitations.*

Keywords: blockchain, student records, role-based access control, smart contracts, permissioned ledger, data privacy, academic credentials, cybersecurity.

I. INTRODUCTION

Academic records follow a person for decades. A degree certificate or transcript may be requested years after graduation for a job, a visa, or further study, so an institution has to keep it correct, available, and private for a very long time. Students, teachers, office staff, parents, and employers all touch the same data in different ways, which makes the question of who may see or change what a central design problem rather than an afterthought.

Most institutions keep these records in a central student information system. Such a system is easy to run, but it places all trust in one database and a few administrators. A breach or a failed disk can damage every record at once. A privileged insider can alter a grade and also edit the log that would reveal the change. An employer who wants to check a certificate usually has to write to the institution and wait, and students rarely learn who has opened their files.

A blockchain is a shared ledger whose entries are linked by hashes, so altering an old entry breaks every later link [1]. That property suits records, but a ledger alone does not decide who may read or write, and a public chain exposes data too widely for personal information. Role-based access control answers the other half of the problem: permissions belong to roles such as registrar or faculty, and a person receives them by holding a role [5]–[7]. The idea developed here is to place the RBAC rules inside smart contracts on a permissioned blockchain, so that the rules, every change to them, and every access attempt become part of a verifiable record, while the documents themselves remain encrypted outside the chain.

This paper makes three contributions:

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-38877

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

a layered architecture that joins a permissioned blockchain, encrypted off-chain storage, and smart-contract-enforced RBAC;

a role and permission model for educational institutions, with separation of duty and student consent built in as constraints; and a threat analysis, a compliance discussion, and an evaluation plan, together with an honest list of limitations.

No new experimental results are claimed. Findings of earlier researchers are attributed to them, and the proposed design is offered as a blueprint for an independent implementation.

II. RELATED WORK

Earlier research touches this topic from three directions: blockchain for education, access control built on blockchain, and the RBAC model itself. Table I lists the works discussed.

TABLE I: SUMMARY OF REVIEWED WORKS

Work	Year	Contribution relevant here
Nakamoto [1]	2008	Hash-linked blocks as a tamper-evident shared ledger
Ferraiolo et al. [6]	2001	NIST model for RBAC with hierarchy and separation of duty
Zyskind et al. [8]	2015	Blockchain as an access-control manager for personal data kept off-chain
Azaria et al. [9]	2016	MedRec: smart contracts managing permissions over medical records
Grech & Camilleri [10]	2017	Survey of blockchain use cases in education
Turkanovi et al. [11]	2018	EduCTX: blockchain platform for higher-education credits
Gräther et al. [12]	2018	Blockchain-based lifelong learning passport
Androulaki et al. [4]	2018	Hyperledger Fabric: permissioned platform with pluggable consensus and chaincode

A. Blockchain for Education Records

Grech and Camilleri surveyed how blockchain could serve education, including credential issuing and verification [10]. Turkanovi et al. proposed EduCTX, a platform for recording and transferring higher-education credits [11], and Gräther et al. described a blockchain-based learning passport that follows a learner across institutions [12]. These works mainly concern finished results, that is, proving that a credential is genuine. They say less about everyday access to sensitive material such as grades in progress, attendance, or disciplinary notes.

B. Access Control on Blockchain

Zyskind et al. described how a blockchain can act as an automated access-control manager over personal data that is stored elsewhere [8]. Azaria et al. applied smart contracts to permissions over medical records in MedRec [9]. Both follow the pattern adopted here: the ledger holds permissions and evidence, and bulk data stays off-chain. Hyperledger Fabric supports this pattern through authenticated membership, pluggable consensus, certificate-based identities, and chaincode [4].

C. RBAC Foundations

Role-based access control was introduced by Ferraiolo and Kuhn [5] and organised into a family of models by Sandhu et al. [7]. The NIST standard defines core, hierarchical, and constrained RBAC, the last of which adds separation of duty [6]. Universities map naturally onto this model because their staff already work under well-defined roles.

D. Research Gap

The reviewed works either concentrate on certificates or leave access control to an application outside the ledger. What is missing is a design in which the access policy itself is recorded and enforced at ledger level, covers the whole life of a record rather than only the final certificate, and gives the student visible control. That is the gap addressed here.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

III. PROPOSED METHODOLOGY

A. Overview

Fig. 1 shows the five layers of the framework. Users reach the system through portals. Each user holds a certificate-based identity issued by the institution's membership service. Every request is handled by chaincode (a smart contract [2]), which consults the RBAC policy before reading or writing anything. The ledger keeps hashes, policy, consent, and audit entries, and the documents are encrypted in off-chain storage, for example a database or a content-addressed file system such as IPFS [3]. Because all participants are known, a crash-fault-tolerant ordering service is enough inside one institution, whereas a consortium of institutions that do not fully trust one another would prefer a Byzantine-fault-tolerant one.

B. Data Placement

The guiding rule is that personal data is never stored in plaintext on the ledger (Fig. 2). The chain holds a pseudonymous student identifier, the hash of the encrypted document, the record type and version, the issuer and time, a pointer to the stored file, the RBAC policy, consent entries, and audit events. If someone alters a stored document, its recomputed hash no longer matches the ledger and the change is detected. The same split lets an institution delete off-chain data when the law requires it, leaving behind only a hash that reveals nothing.

C. Role Model

Table II lists the roles. Formally, following the NIST reference model [6], the framework has a set of users U, a set of roles R, and a set of permissions P, where each permission pairs an operation with a record type. User-to-role assignment (UA) and permission-to-role assignment (PA) link them, and a role hierarchy lets senior roles inherit the permissions of junior ones (Fig. 3). A request is allowed only when the caller's role holds the permission, directly or by inheritance, and every constraint is satisfied.

TABLE II: ROLES AND RESPONSIBILITIES

Role	Responsibility
Administrator	Manages network and identities; holds no access to record contents
Registrar	Creates student records, issues certificates, approves corrections
Faculty	Enters and reads grades and attendance for assigned courses
Dept. Head	Reviews and approves grade changes in the department
Student	Reads own records; grants and revokes consent
Parent/Guardian	Reads limited records of a linked student, as policy allows
Verifier	Employer or university checking a credential, with student consent
Auditor	Reads audit log and hashes, never personal data

Four constraints refine the model. Separation of duty: the person who enters a grade cannot approve its change, and the administrator never holds a data role. Ownership: faculty act only on courses assigned to them. Consent: a verifier reads only what the student has authorised, for a limited period. Minimal disclosure: a verifier normally receives a match or no-match answer rather than the whole record. Table III summarises the resulting permissions.

TABLE III: PERMISSION MATRIX

Role	Identity	Grades	Cert.	Policy	Audit
Administrator	–	–	–	C*	–
Registrar	C,R,U	R,A	C,R	R	–
Faculty	–	C,R†	–	–	–
Dept. Head	–	R,A	R	–	–
Student	R	R	R	G	R†
Parent	R‡	R‡	–	–	–

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-38877

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

Verifier	–	–	V§	–	–
Auditor	–	H	H	R	R

C create, R read, U update as a new version, A approve, V verify, H hash only, G grant or revoke consent. * needs multi-party endorsement; † own courses or own record only; ‡ limited by policy; § needs student consent.

D. Smart-Contract Functions and Access Check

The chaincode offers functions to register a student, add a grade, request and approve a grade change, issue a certificate, grant and revoke consent, verify a credential, fetch a record, and assign a role. Each begins with the same check, shown in Fig. 4. The caller's role is read from the identity certificate, the permission is looked up in the policy, and the ownership, consent, and separation-of-duty rules are tested in turn. The outcome of every check, including refusals, is appended to the audit log, so failed attempts are as visible to auditors as successful ones.

E. Record Correction

Ledger entries cannot be edited, so a correction becomes a new version linked to the previous one. A faculty member raises a request with a reason, and the department head or registrar approves it. Both identities, the reason, and the times are stored. The earlier version stays available, which supports dispute resolution and removes the possibility of a silent change.

F. Credential Verification

The student grants a time-limited consent that names the verifier and the scope. The verifier submits the hash of the document it holds. The chaincode checks the verifier's role and the consent, compares the hash and the issuer's signature with the ledger, and returns a match or no match. The event is logged and appears in the student's access history. No manual request to the institution is needed.

G. Cryptographic Protection

Every transaction is signed with the submitter's private key, which gives authenticity and non-repudiation. Documents are encrypted with a per-record symmetric key, and that key is wrapped for each authorised role or user. Revoking access stops the release of the key for later requests, and keys are rotated for new versions. Revocation cannot undo a copy that someone has already decrypted and saved, which is a limit of every cryptographic scheme. Private keys should be held in hardware security modules or equivalent protected storage.

IV. SECURITY AND PRIVACY ANALYSIS

A. Threat Analysis

The adversaries considered are outside attackers, malicious insiders with valid accounts, curious verifiers, a compromised node, and forgers of certificates. Table IV pairs each main threat with the countermeasure in the design.

TABLE IV: THREATS AND COUNTERMEASURES

Threat	Countermeasure
Grade tampering by an insider	Hash on ledger exposes edits; changes need two roles and are versioned
Unauthorised reading	RBAC check in chaincode; data encrypted, keys released only to authorised roles
Privilege escalation	Role changes are signed, endorsed transactions; administrator holds no data role
Certificate forgery	Issuer signature and ledger hash show a fake at once
Compromised node	Endorsement by several organisations; fault-tolerant consensus
Verifier over-collection	Scoped, expiring consent; match or no-match answers
Loss of stored files	Redundant encrypted copies; hash confirms integrity after restore

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

Some risks remain. A blockchain guarantees that data has not changed since it was entered, not that it was correct when entered. A stolen faculty credential could still submit false entries, although they would be attributable and detectable. Bugs in the chaincode could undermine enforcement, so independent review and formal verification are advisable. Key management stays the practical weak point.

B. Privacy and Compliance

Student data is regulated by laws such as FERPA in the United States [15], the GDPR in the European Union [14], and the Digital Personal Data Protection Act, 2023 in India [16]. They share a common core: limited collection, purpose and consent, access for the individual, correction, and accountability. The design supports these through hash-only ledger entries, scoped consent, student access to their own records and access history, correction as a new version with deletion of off-chain data when required, and an immutable audit trail. Whether a retained hash is acceptable under an erasure rule differs by jurisdiction, so legal review is advised before deployment.

V. PROPOSED EVALUATION PLAN

A prototype can be built on Hyperledger Fabric with at least three organisations, each running two peers, an ordering service, chaincode, an encrypted off-chain store, and a web interface. Measurements should cover transaction throughput and latency for read, write, and verification calls, the overhead of the RBAC check, storage growth on and off the chain, and behaviour as the number of records and peers grows. Security tests should try every denied cell of Table III, tamper with stored files, attempt privilege escalation, and replay old transactions. A centralised database with application-level RBAC is the natural baseline.

The design suggests stronger integrity and auditability but slower writes than a central database. Because student workloads are read-heavy and grades are entered in batches each term, that trade-off may be acceptable. This expectation is a hypothesis and must be confirmed by measurement.

VI. DISCUSSION

A. Comparison with a Central System

Table V contrasts the proposed design with a conventional central database that applies RBAC inside the application.

TABLE V: CENTRAL DATABASE VERSUS PROPOSED FRAMEWORK

Aspect	Central DB + app RBAC	Blockchain + RBAC
Tamper evidence	Depends on logs the administrator controls	Hash-linked ledger; any change detectable
Single point of failure	Yes	No; replicated nodes
Policy changes	Can be edited silently	Recorded as signed transactions
Third-party check	Manual request	Automated, consent-based
Write speed	Fast	Slower; endorsement and ordering
Cost and effort	Low	Higher

B. Limitations and Mitigations

Table VI lists the main limitations of the approach and practical steps that reduce each one.

TABLE VI: LIMITATIONS AND MITIGATIONS

Limitation	Mitigation
Incorrect data entered in the first place	Two-role approval; validation rules in chaincode; versioned corrections
Lost or stolen keys	Hardware key storage; recovery procedure; multi-factor login
Chaincode defects	Code review, testing, and formal verification
Lower write throughput	Batch grade entry; keep bulk data off-chain
Erasure versus immutability	Hash-only entries; delete off-chain data; legal review

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, October 2026 Impact Factor: 8.2

Legacy system integration	API gateway; phased roll-out
Governance of nodes and policy	Consortium agreement; multi-party endorsement of role changes

C. Practical Deployment

An institution can adopt the framework in stages: first anchor the hashes of issued certificates and the audit log, then bring grades and full RBAC enforcement onto the ledger, and finally join a consortium of institutions for cross-verification. Throughout, the component should work alongside, not replace, normal security controls such as network protection and staff training.

D. Future Scope

Combining RBAC with attribute-based access control [13] would allow rules that depend on course, term, or purpose. Zero-knowledge proofs could let a verifier confirm a claim, such as completion of a degree, without seeing the underlying record. Verifiable credentials and decentralised identifiers would improve interoperability and let students hold their own credentials. Anomaly detection over audit logs, formal verification of chaincode, and a pilot with real users and a usability study are further directions.

VII. CONCLUSION

Central student record systems struggle to offer tamper evidence, fine-grained access control, and trustworthy verification at the same time. This paper described a framework that anchors integrity on a permissioned blockchain, keeps sensitive content encrypted off-chain, and enforces a defined RBAC model through smart contracts, with student consent and separation of duty as built-in constraints. Four figures and six tables set out the architecture, the data split, the role model, the access check, the threats, and the limitations.

The design adds operational complexity and trades some write speed for integrity and accountability. Whether that trade is worthwhile must be shown by an independent implementation that reports its own measurements. Its main strengths are verifiable history, least-privilege access, and student visibility into who uses their data.

ACKNOWLEDGMENT

The authors thank their institution for academic guidance and resources, and acknowledge the researchers whose published work formed the basis of the literature reviewed here.

REFERENCES

[1]S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[2]G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” Ethereum Project Yellow Paper, 2014. [3]J. Benet, “IPFS – Content Addressed, Versioned, P2P File System,” arXiv:1407.3561, 2014.
[4]E. Androulaki et al., “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in Proc. 13th EuroSys Conf., 2018, Art. no. 30. [5]D. Ferraiolo and R. Kuhn, “Role-Based Access Controls,” in Proc. 15th National Computer Security Conf., 1992, pp. 554–563.
[6]D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, “Proposed NIST Standard for Role-Based Access Control,” ACM Trans. Inf. Syst. Secur., vol. 4, no. 3, pp. 224–274, 2001.
[7]R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, “Role-Based Access Control Models,” IEEE Computer, vol. 29, no. 2, pp. 38–47, 1996.
[8]G. Zyskind, O. Nathan, and A. Pentland, “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” in Proc. IEEE Security and Privacy Workshops (SPW), 2015, pp. 180–184.
[9]A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using Blockchain for Medical Data Access and Permission Management,” in Proc. 2nd Int. Conf. Open and Big Data (OBD), 2016, pp. 25–30.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, October 2026
Impact Factor: 8.2

[10]A. Grech and A. F. Camilleri, "Blockchain in Education," European Commission, Joint Research Centre, EUR 28778 EN, 2017.

[11]M. Turkanovi, M. Hölbl, K. Koši, M. Heriko, and A. Kamišali, "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 5112 – 5127, 2018.

[12]W. Gräther et al., "Blockchain for Education: Lifelong Learning Passport," in Proc. 1st ERCIM Blockchain Workshop, 2018.

[13]V. C. Hu et al., "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162, 2014. [14]Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), 2016.

[15]Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g. [16]Digital Personal Data Protection Act, 2023, Government of India.