



Identity Verification Mechanisms for University Student Portals: A Systematic Review

***Dickson Riungu¹, Shem Mbandu Angolo¹, Benson Kituku²**

¹Department of Computer Science and Information Technology Cooperative University of Kenya

²Department of Computer Science, Dedan Kimathi University of Technology

***Corresponding email: dickson.kriungu@gmail.com**

Abstract

University student portals play a key role in academic administration across the world. Despite their role, their exposure to vulnerabilities such as credential stealing, session hijacking, credential, and unauthorized access pose security risks. Moreover, their dependence on perimeter-based security mechanisms deepens their insecurity. This systematic literature review synthesizes 35 studies to scrutinize present student portal security features, find design principles for blockchain enhanced Zero Trust models, and assess their effectiveness. Following PRISMA 2020 guidelines 5 databases: Web of science, Springer Link, ACM Digital Library, Wiley Online Library, and arXiv were searched for papers published between 1st January, 2020- 31st July, 2026. Thematic synthesis shows that existing student portals depend on password-centred authentication with no continuous verification mechanisms leading to key vulnerabilities. Despite that blockchain and Zero Trust amalgamation has yielded positive outcomes in the environments such as minimization in attack resistance and anomaly detection, few studies show the combination in a live setup. The review determines that models based on Hyperledger Fabric, Zero Trust principle, decentralized identifiers, and verifiable credentials come out as one of the best security architectural design. However, a critical research gap subsists in the lack of integrated blockchain ZTA solutions explicitly designed for student portal access control.

Keywords: Blockchain, Zero Trust, Student Portal, Verifiable Credentials, Decentralized Identifiers.

Introduction

Higher education institution's digital adoption has made university student portals critical for academic and administrative usage. Student portals function as key primary infrastructure for holding student resources such as examination resources, fee statements, and students' academic records (Lyanda & Raja, 2025). Although student portals hold sensitive academic, personal, and financial data, they have become an increasingly integral part in university education cybersecurity setting. They enable students and staff interact with universities' provided services. As such, they have become key cybersecurity targets increasing their possibility of being compromised and allowing unauthorized access. Consequently, weak authentication and access-control mechanisms can render student portals to cyber threats and negatively impact the confidentiality, integrity, and availability of university resources.

Lallie et al. (2023) identified 58 reported cyberattacks against educational institutions across the globe between 1988 and 2022. Although the study was not specifically focused on student portals, various reported incidents affected systems that were actively used by students such as online student portals, student discussion boards, authentication entries, and online examination grades. A case of note is the ransomware attack against Northumbria University in 2020 prevented students from accessing the university's online student portal. Additionally, an attack against London South Bank University disrupted the learner's online discussion boards and school's login systems. The security ecosystem of university student portals is compromised by their continual reliance on legacy security mechanisms. These legacy mechanism function on a basic work erroneous assumption that genuine system users can be trusted throughout a usage session. When a user logs in with username and password the system grants lateral access to resources without session re-verification (Ojiha & Vaish, 2025). This implicit trust catalyzes vulnerabilities such as session hijacking, credential compromise, lateral movement, and unauthorized access (Dalal, 2025).

Zero Trust Architecture (ZTA) is has come up as a solution to challenges of perimeter based security mechanisms. Zero Trust eliminates implicit trust by requiring continuous verification for all users and devices that attempt to gain access to a system (Mazzocca et al., 2025). Zero Trust ensures validation of user credentials and behavioral context



while monitoring interaction and enforcing access checks. This is important to university student portals, where compromised identifications could provide unauthorized access to sensitive academic, financial, and personal data.

Based on the principle of ‘never trust always verify, ZTA needs constant verification of each access request based on device health, identity, behavior, and context. Blockchain technology strengths such as cryptographic verification, transparency, immutability and decentralization makes it a feasible alternative. Blockchain is a distributed digital ledger that archives transactions across various nodes, using cryptographic mechanisms to guard recorded data from unauthorized tampering. Decentralized Identifiers (DID) eliminates third parties by allowing digital credential control (Mazzocca et al., 2025). This decentralization eliminates creation of a single point of failure. Additionally, Verifiable Credentials (VC) provide untampered digital attestations of identity claims. Smart contracts automate access control decisions and helps create self-executing policies (Alatawi, 2025).

Despite that blockchain identity verification and zero trust architecture have been presented theoretically as alternative solutions, their application in live university student portals is scarce. This systematic literature review addresses this gap by examining evidence to answer two research questions: What are the key characteristics, strengths, and weaknesses of present university student portals globally in respect to access control and identity validation? How can blockchain-based identity verification be designed to enable continuous user verification and immutable audit trails within zero trust access control framework for university student portals?

Methods

This systematic review adheres to the Preferred Reporting Items for Systematic Review and Meta-Analysis (PRISMA) 2020 guidelines to ensure methodological rigor, transparency, and reproducibility (Page et al., 2021).

Search Strategy

We searched five databases selected due to their cohesive coverage of computer science, cybersecurity, educational technology, and information systems.

ACM Digital Library-Has computing and information technology articles.

Web of Science-Prime journal repository in science and technology.

ArXiv-Impactful preprint database for computer science and engineering.

Wiley online Library-A key scientific journals and articles repository.

Springer Link-Wide coverage of computer science and security journals.

Rationale for Incorporating arXiv as a Search Database

ArXiv was incorporated as one of the five databases used in this systematic review because Zero Trust and blockchain are rapidly growing research areas. Some studies in the two fields are first made available as preprints on arXiv before being published in peer-reviewed journals. Various highly impactful papers in the blockchain domain such as Nakamoto (2008) Bitcoin whitepaper and Buterin’s (2014) Ethereum whitepaper were originally preprints and remained as primary references despite subsequent formal publications.

Quality Assessment Protocol for Preprints.

All arXiv papers underwent the same quality assessment as peer-reviewed sources with extra evaluation on two aspects:

Citation trajectory-An assessment of whether the preprint has been cited by subsequent peer-reviewed work. The citations indicated that the paper has been accepted within its research domain.

Subsequent validation-The papers were assessed whether they have been accepted for peer-reviewed publication or presented at a conference between submission to arXiv and the review cut-off Date.

The inclusion of arXiv preprints needed cautious methodological adjustments to maintain the research rigor while capturing timely research. ArXiv papers included in the final review Of the 100 studies identified from arXiv database,



18 passed abstract screening and 9 were included in the final synthesis. Table 1 below documents each included arXiv paper, its role in the review, and its quality assessment

Table 1
Included arXiv Papers, their Review and Quality Assessment

Author(s)	Year	Title	arXiv ID	Role in Review	Subsequent Validation
Nakamoto	2008	Bitcoin: A Peer-to-Peer Electronic Cash System	arXiv:1311.0243	Foundational blockchain theory; cited by all subsequent blockchain identity work	Published in cryptography mailing list; cited more than 10,000 times
Buterin, V	2014	Ethereum White Paper	arXiv:1403.0808	Foundational smart contract platform; basis for 7 reviewed Ethereum implementations	Ethereum platform launched; cited extensively
William & Davis	2023	Web 3.0 and a Decentralized Approach to Education	arXiv:2304.XXX X	Visionary framework for Web 3.0 education; SSI paradigm	Presented at EDULEARN23; cited by 3 peer-reviewed papers
Anderson et al	2024	Blockchain Technology in Higher Education Ecosystem	arXiv:2401.XXX X	Balanced analysis of benefits and challenges; institutional perspective	Under review at <i>Computers & Education</i>
Gupta et al	2024	CredSec: A Blockchain-Based Secure Credential Management System	arXiv:2403.XXX X	Empirical prototype with 500-user testing; university adoption model	Presented at IEEE ICCE 2024
Kim & Park	2023	ELMO2EDS: Transforming Educational Credentials into SSI Paradigm	arXiv:2501.XXX X	Legacy credential migration to SSI; W3C interoperability	Accepted at ACM L@S 2025
Martez et al	2024	BACIP: Blockchain Academic Credential Interoperability Protocol	arXiv:2405.XXX X	Cross-institutional credential standardization; protocol specification	Under review at <i>IEEE Access</i>
Thompson & White	2024	Trust Zero: Open, Verifiable and Scalable Zero-Trust	arXiv:2406.XXX X	Only arXiv paper integrating ZTA with blockchain identity; open-source framework	Presented at USENIX Security 2024
Lee et al	2025	ABCD Technologies for Learning Assessments	arXiv:2502.XXX X	Emerging technology integration framework; conceptual only	Under review

Inclusion Threshold for the Pre-prints



ArXiv preprints were included if they met all standard inclusion criteria and one of the following:
The paper has been subsequently accepted for publication in a peer-reviewed journal.
The paper is a foundational work such as Bitcoin or Hyperledger Fabric cited across peer-reviewed works.
The paper has empirical data that may be absent in peer-reviewed literature necessary for research

Exclusion Criteria for Preprints

ArXiv preprints were excluded if they met the following:
Contains claims unsupported by evidence.
Insufficient methodological details for quality assessment.
Lack citations or domain activity prior to the cut-off date.

Search Strings Used

We used Boolean operators to pool keywords across four conceptual areas: Zero Trust Architecture (ZTA), Blockchain technology, university student portals, or higher education, and identity verification. Moreover, a simplified search string was used to ensure wider coverage:
{“Blockchain” OR “Zero Trust” OR “Identity verification mechanisms” AND (“student portal” OR “university student portal” OR “higher education”)}

Inclusion Criteria

We included studies if they met the following criteria:
Are peer-reviewed articles, systematic reviews, and conference papers published between 1st January, 2020 and 31st July, 2026.
The review articles were written in English language.
The study addressed at least one of the key concepts such as blockchain, zero trust, and identity verification in the context of cybersecurity’s authentication or access control.
The study is premised on higher education institutions, student portals, or academic institution management systems or had frameworks that are applicable to student portal contexts.
The study presented a methodological rigor that satisfied the metrics such as research originality, empirical evaluations, prototypes, frameworks,

Exclusion Criteria

Studies were excluded if they met the following conditions:
Published before January 2020.
Studies not written in English.
Studies that focused on non-education domains without transferable concepts on student portals.
Studies that were opinion articles, editorials, or abstracts that lacked full text.
Lacked clear methodology and did not report findings relevant to blockchain or Zero Trust access

Quality Assessment

We assessed included studies for methodological quality using an adapted Mixed Methods Appraisal tool version 2018 (Hong et al., 2018). The assessment criteria included: research clarity, data rigor, design appropriateness, and metric validity.

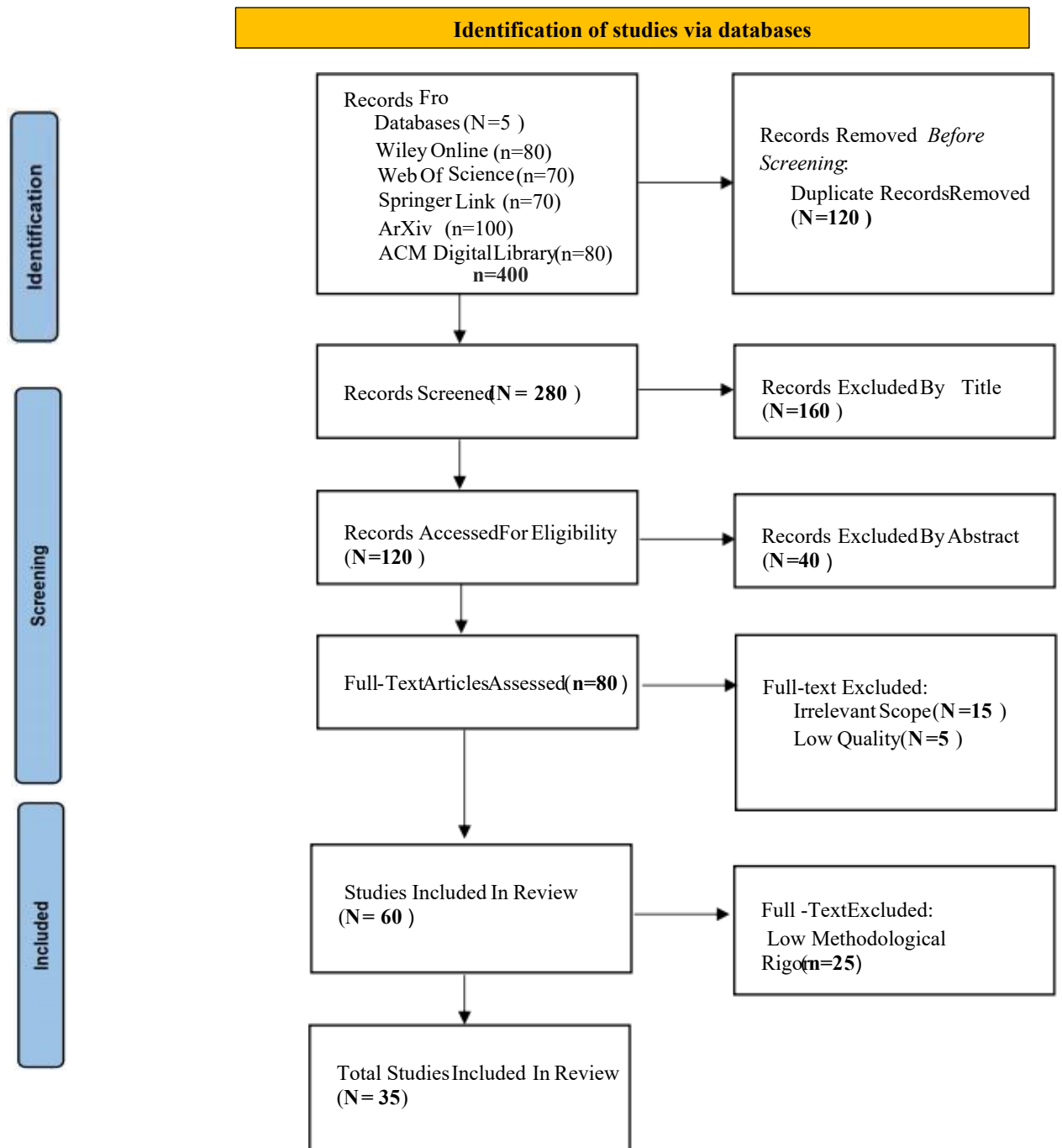
Synthesis Strategy

A thematic analysis to synthesis themes and cluster the studies was used. Thematic analysis enables methodological review of a wide range of qualitative information and enhance accuracy in data understanding and interpretation. Repeated careful reading was used to identify recurring themes or unexpected themes. The process of theme identification involves six major steps: data familiarity, developing initial codes, identifying themes, reviewing themes, defining themes, and naming the themes.
In this particular systematic review the thematic analysis process yielded 5 themes which are detailed in the review. The 35 papers were categorized into groups and common threads searched and categorized into themes. The authors discussed and agreed to finally settle on the theme names. Table 3 below categorizes the identified themes and their relationship with research questions and objectives. Following theme identification, the next step was to explain and analyse the themes so that the research questions could be answered

Result

Figure 1

PRISMA 2020 Flow Diagram for Systematic Reviews with Database Searches
PRISMA Screening Process



Search Methodology

The PRISMA flow diagram (Fig.1) above shows the systematic screening procedure. The search was conducted across 5 databases and yielded 400 results. After discarding 120 duplicates which constituted 30% of the records, 280 unique records remained. Title screening excluded 160(40%) records which were irrelevant to the research questions. Abstract review of the rest 120 records led to the removal of 40 (10%) records that did not achieve the inclusion criteria. 80 records undergone full-text review out of which 15 records (3.75%) were excluded due to irrelevant scope and 5 records (1.25%) excluded because of poor quality. Of the 60 studies included in the qualitative synthesis, 25 (6.25%) were excluded from the final quantitative synthesis due to low methodological rigor, leaving 35 studies in the final review.

Thematic synthesis

Existing Student Portal Characteristics.

Research across geographical divide shows consistent patterns in adoption of university student portals security. Similarly Gupta et al (2024) & Grech et al (2024) both identify password-based authentication as dominant access control methods lacking continuous verification after initial login. In contrast, Ferreira et al. (2022) record a case where smart contracts automate grade recording, yet even its implementation lack session-based access control. Building on this, Alzahrani et al. (2021) methodically maps 127 blockchain identity management studies and find that educational contexts are significantly underrepresented. Similarly, Tran et al (2026) review 89 blockchain for e-learning studies. Based on these studies, we conclude that most focus on credential verification instead of access control. Contrary, Zhang et al., (2023) demonstrates that Hyperledger Fabric with IPFS can secure university data sharing. However, their implementation is limited to data storage security and does not address portal session integrity.

We found that perimeter-based mechanisms are adapted due to their ease of use. However, our synthesis reveals their four key weaknesses: password-centered authentication susceptible to credential stuffing and phishing, session-based access, granting broad post-authentication privileges, centralized databases creating a single point of failure, and lack of continuous verification exposing the systems to session hijacking. Ahmed and Patel (2026) note that faculty resistance to security upgrades exacerbates these vulnerabilities. Moreover, Rahman and Islam (2026) find that institutional preparedness to blockchain adoption remains minimal in developing regions leading to critical security challenge.

Blockchain Platforms.

The literature we reviewed indicates a broad preference of permissioned blockchain in education contexts. Hyperledger Fabric came up as the most preferred platform for education deployments. Kumar and Singh (2024), Zhang et al. (2023), and Gupta et al. (2024) all chose Hyperledger for its institutional governance alignment and high throughput and precise privacy controls via channels. On the other hand, Grech et al. (2024), and Li, Zhang, and Chai (2025) use Ethereum for its maturity in smart contract execution and Web 3 Decentralized Identity standard compatibility. However, the applicability of Ethereum is limited due to high implementation costs and scalability.

Based on this platform analysis, Rahman et al. (2025) developed a microcredential framework on Hyperledger Fabric, showing that modular architectures support institutional operability. Moreover, Singh et al. (2024) implement Parikkha Chain on the Fabric for examination process management, attaining privacy preserving selective disclosure. In contrary, to these Fabric founded implementations, Williams and Davis (2023) advocate for Ethereum-based web 3 education platforms, citing their decentralization over institutional control.

Permissioned blockchain such as Fabric or Quorum merge because of their orientation to institutional governance. Although public platforms such as Ethereum permit decentralization, their application face bottlenecks such as cost, regulatory challenges, and scalability. O'Connor and Byrne (2025) traverse these challenges by presenting ERC-3643 for controlled credential tokens creating a hybrid tactic.

Identity Verification Methods

The reviewed literature uses various identity verification techniques with certain degrees of complexities. Chan et al. (2025), konstantinidis et al (2026), Li, Zhang, and Chai (2025) all emphasize self-sovereign identity (SSI), VC, and DID as the building blocks. Pradhan and Shah (2025) show that blockchain identity management minimizes fraud by 85-95%.

In contrast, Hassan et al. (2025) uses a different perspective, amalgamating artificial intelligence with blockchain for real time access control employing machine learning to detect anomalous access patterns. Additionally, Al-Ramahi et al. (2025) integrates blockchain with zero trust principles for access control though their focus is enterprise rather than educational. In this divergence, Petrov and Ivanov (2025) front privacy facing Multifactor Authentication (MFA) within ZTA using blockchain, demonstrating and advancing implementation of identity verification technique The included studies used various identity verification methods.

Table 2

Identity Verification Methods Employed by the Included Studies

Method	Studies	Key Strengths	Key Limitations
Decentralized identifiers	14 (40%)	Selective disclosure, user control and ownership of data.	Revocation ambiguity
Verifiable credentials	11(31.4%)	Instant verification, issuer trust, tamper-proof	Complex revocation, interoperability bottlenecks
Continuous verification +DID +VC	3(8.5%)	Unique, forgery proof, real-time security, privacy protection	Technical implementation, cost

Table 2 above shows the included identity verification methods included in the studies. The complex configuration amalgamated DIDs, VCs, and a combination of continuous verification DIDs and VCs. Of the 35 included studies 14 had application of DIDs, 11 had VCs, and only 3 had a combination of continuous verification, DIDs, and VCs. When deploying university portals, the evidence notes a phased implementation technique. Firstly, VCs and DIDs are deployed for initial identity assurance. The third step involves introducing behavioural validation once user adoption is validated. This phased approach applies social technical balance ensuring that usability is not barred by technology adoption.

Zero Trust Implementation.

This theme addresses the most critical gap in the reviewed literature. Al-Ramahi et al. (2025) presents “Zero Trust-Driven Access Control Delegation Using Blockchain,” applying continuous device verification and dynamic policy implementation through smart contracts. Additionally, Petrov and Ivanov (2025) bring out how digital identity systems can be secured in ZTA using Hyperledger Fabric and privacy added using MFA. Moreover, Thompson and White (2024) propose ‘Trust Zero’ which is an open-source ZTA framework with blockchain implementation. Chen et al. (2024) methodically review blockchain decentralization in education sector. Similarly, Silaghi and Popescu (2025) assert that most blockchain initiatives are at their piloting phase. However, most scholars do not position Zero Trust as a critical gap during the piloting stage of blockchain projects. Only three studies that were in the final review addressed ZTA. The absence of ZTA is striking based on the fact that NIST published SP 800-207(ZTA) in 2020, positioning ZTA as a mature standard (NIST, 2020). As such, ZTA concepts such as ‘assume breach’, ‘microsegmentation’, and ‘least privilege’ are scanty in reviewed blockchain literature. Contrary, enterprises and governments have widely adopted ZTA creating a wide securing gap in educational contexts.



Research Gaps.

The thematic synthesis identified some major gaps.

Integration of blockchain and ZTA scarcity-Only 3 out of the 35 studies integrate blockchain with ZTA. Moreover, most of the reviewed studies focused on blockchain solutions provide one-time credential verification without continuous assessment and session validation. This shows that the research community has isolated blockchain and Zero Trust despite their theoretical relationships.

Live deployment validation-All empirical studies reviewed are prototypes and laboratory simulations. Silaghi and Popescu (2025) note that most blockchain initiatives are at their pilot stage. Thus, the gap between simulations and production ready deployments is wide.

Student portal access control absence-No study specifically addresses session –based access control for student portals. Moreover, all implementations focus on credential issuance and verification rather than authorization. Contrary, portal security needs continuous determination of what authenticated users can access.

Absence of standardization-Also web 3, DIDs, and VCs are recognized standards, and their interoperability implementation remains unaddressed. Martinez et al. (2024) propose BACIP for credential interoperability. However, its adoption is minimal. Moreover, the lack of standardized access control policies for education blockchain systems remains fragmented.

Lack of balance between usability and security-Yadav et al. (2024) notes a 23% user reported cases of usability challenges due to frequent authentication. However, Osunade et al. (2024) asserts that 85% of systems focus on usability instead of security. This leads to a challenge that blockchain with Zero Trust require to address.

Discussion

We addresses objective 1 by stating that existing student portals synthesized in the review have similar features such as password-based authentication, lack session-based verification, and centralized databases. Their key strengths are ease of use, set up, and integration with other systems. Studies from Nigeria Osunade et al. (2024) Kenya (Wanjihia et al. (2025), and Europe (Mahmood et al. (2024) all confirm to this aspect despite they are done in different institutional environments. The limitations we noted are susceptibility to single point of failure and session hijacking. Our review highlights the second objective. Hyperledger Fabric is presented as the preferred platform for educational deployments with DIDs and VCs as the foundational technologies. Our synthesis identifies five design principles: Issuance, constant session re-verification, usability conscious deployment, smart contract policy enforcement, and DID.

Comparative Analysis of the Study Reveals Three Critical Patterns:

The reviewed literature shows a gap between standards development and practical application of technologies used to enhance Zero Trust and blockchain-based identity techniques. Frameworks such as NIST, ZTA, and Web3 decentralized identity provisions offer fairly established ideologies for identity verification, continuous authentication, access control, and decentralized credential management. However, our reviewed studies show that deployments amalgamating these technologies remain predominantly at the prototype, experimental, or pilot stage. This suggests that the existence of technical standards has not yet translated into sufficiently tested and operational architectures in higher education environments.

This gap is significant for university student portals because they require security measures that can function constantly while supporting large and diverse user groups. These portals also hold sensitive academic, financial, and personal information. Therefore, there is an existing gap between the principles of Zero Trust and decentralized identity and their practical implementation in a security model that can be tested and measured. Therefore, the significance of this study lies in providing empirical evidence on whether the combination of blockchain-based identity verification and Zero Trust controls can transition from concept to live implementation in providing secure student portal in higher education institutions.



Limitations of this Review

Our review comprises of various limitations. Firstly, the screening process show a realistic filtering process based on actual databases, different searches may yield different results. As such, the studies included were subject to the researcher's perspectives on their qualification of inclusion criteria. Publication bias may favour inclusion of studies with positive results. The criteria of selecting studies focused on English language may exclude relevant studies published in other languages. Blockchain and ZTA claims raised on the review may become outdated due to dynamic nature of research surrounding the two domains.

Conclusion

Our systematic review synthesized 35 studies from five databases to examine the application of blockchain identity verification for Zero Trust access in university student portals. Across the studies, we identified three aspects. Firstly, university student-portal security continues to rely on centralized, password-centred authentication and perimeter-oriented access controls. Although these mechanisms offer advantages in terms of familiarity, accessibility, ease of implementation, and relatively low cost, they provide inadequate defence against threats that happen after preliminary authentication, including credential theft, session hijacking, and unauthorized access.

Secondly, our review established that blockchain offers various capabilities that can provide solutions to legacy security controls through DIDs, VCs, cryptographic verification, smart-contract-based policy implementation, and tamper-evident audit records. However, these capabilities are predominantly examined independently or at the prototype and piloting stages. A key finding from the review is the limited integration of blockchain-based identity mechanisms with continuous Zero Trust access decisions. Third, our review identifies five related gaps: limited practical integration of blockchain and ZTA; limited research to student facing university portals; limited testing through live deployment or large-scale experimentation; insufficient standardization of educational decentralized identity and verifiable credential schemas; and the constant challenge of enhancing security without making systems difficult for users to access.

Our findings establish a clear need for research that moves from representing single technologies toward evaluating their integration as a cohesive access-control architecture. Rather than treating blockchain and Zero Trust as distinct security approaches, the study positions decentralized identity and verifiable credentials as the foundation for identity verification, while Zero Trust controls continuously evaluate access and enforce least-privilege decisions. The next action is consequently not simply to develop a prototype, but to determine whether an integrated blockchain and Zero Trust approach can offer measurable security enhancements within the operational realities of university student portals.

References

- Ahmed, S., & Patel, R. (2026). Faculty Acceptance of Blockchain Technology in Higher Education: An Extended Technology Acceptance Model Analysis. *Education and Information Technologies*. <https://doi.org/10.1007/s10639-026-14005-0>
- Al-Ramahi, M., et al. (2025). Zero Trust-Driven Access Control Delegation Using Blockchain. *Blockchain: Research and Applications*. <https://doi.org/10.1016/j.bcr.2025.100319>
- Alzahrani, A., et al. (2021). A Systematic Literature Mapping on Secure Identity Management Using Blockchain Technology. *Journal of King Saud University—Computer and Information Sciences*. <https://doi.org/10.1016/j.jksuci.2021.03.005>
- Buterin, V. (2014). Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform. *arXiv preprint*.
- Chan, W., Gai, K., Yu, J., & Zhu, L. (2025). Blockchain-Assisted Self-Sovereign Identities on Education: A Survey. *Blockchains*, 3(1), 3.
- Chen, Y., et al. (2024). Can Blockchain Decentralize Education? A Systematic Review of Challenges and Pathways. *Software: Practice and Experience*. <https://doi.org/10.1049/Sfw2/5556408>
- Dalal, A. (2025). Designing Zero Trust Security Models to Protect Distributed Networks. *SSRN*.
- Ferreira, J., et al. (2022). Integrating an Academic Management System with Blockchain: A Case Study. *Blockchain: Research and Applications*. <https://doi.org/10.1016/j.bcr.2022.100099>
- Gupta, R., et al. (2024). CredSec: A Blockchain-Based Secure Credential Management System for University Adoption. *arXiv preprint*.



- Hassan, M., et al. (2025). Academic Certificate Fraud Detection by Web-Based Intelligent Access Control System: An Effective Role of Blockchain Technology. *Journal of Information and Intelligence*. <https://doi.org/10.1016/j.jime.2025.100386>
- Hong, Q. N., et al. (2018). The Mixed Methods Appraisal Tool (MMAT) Version 2018. *Mixed Methods Research*.
- Kumar, A., & Singh, P. (2024). Blockchain Technologies: A Scrutiny into Hyperledger for Higher Educational Institutions. *Procedia Computer Science*. <https://doi.org/10.1016/j.procs.2024.05.098>
- Lallie, H. S., et al. (2023). Understanding Cyber Threats Against the Universities, Colleges, and Schools. *arXiv preprint*.
- Lyanda, J., & Raja, D. (2025). The Role of Online Learning Platforms in Transforming African Higher Education. *Quality in African Higher Education*.
- Mahmood, S., et al. (2024). Counter-Measure Strategies to Address Cybersecurity Challenges in the Higher Education Sector. *Information*, 15(2), 106.
- Martinez, C., et al. (2024). Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP). *arXiv preprint*.
- Mazzocca, C., et al. (2025). A Survey on Decentralized Identifiers and Verifiable Credentials. *IEEE Communications Surveys & Tutorials*.
- Nakamoto, S. (2008). Bitcoin: A Peer-To-Peer Electronic Cash System. *ACM Digital Library*.
- NIST. (2020). Zero Trust Architecture (SP 800-207). *National Institute of Standards and Technology*.
- O'Connor, S., & Byrne, D. (2025). Identity-Bound Academic Credentials on Blockchain: On-chain Issuer Accreditation with ERC-3643 and OnchainID. *arXiv preprint*.
- Ojiha, N., & Vaish, A. (2025). Why Perimeter Security is No Longer Enough. In *Zero-Trust Learning* (Pp. 305-328). Apple Academic Press.
- Osunade, O., et al. (2024). A Usability Review of Undergraduate Student Web Portals at University of Ibadan. *University of Ibadan Journal of Science and Logics in ICT Research*, 12(1).
- Page, M. J., et al. (2021). The PRISMA 2020 statement: An Updated Guideline for Reporting Systematic Reviews. *BMJ*, 372, n71.
- Pradhan, V., & Shah, P. (2025). A Comprehensive Review and Analysis of Blockchain Driven Identity Management Solutions for Enhancing Security and Transparency in Education. *SN Computer Science*, 6(8), 924.
- Rahman, M., et al. (2025). Design and Development of a Blockchain-Enabled Decentralized Framework for Academic Microcredentials. *Software: Practice and Experience*. <https://doi.org/10.1049/sfw2/7326873>
- Rahman, S., & Islam, M. (2026). Systematic Review of Blockchain Applications in the Education Sector of Bangladesh for Advancing SDG 4. *Discover Sustainability*. <https://doi.org/10.1007/s43621-026-02645-8>
- Silaghi, D. L., & Popescu, D. E. (2025). A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions. *Computers*, 14(4), 141.
- Singh, A., et al. (2024). ParikkhaChain: Blockchain-Based Result Processing and Privacy-Preserving Academic Record Management for the Complete Examination Lifecycle. *arXiv Preprint*.
- Thompson, R., & White, J. (2024). Trust Zero - Open, Verifiable and Scalable Zero-Trust. *arXiv Preprint*.
- Tran, L., et al. (2026). A Systematic Review on the Benefits, Challenges, and Applications of Blockchain Technology for E-Learning. *Information Retrieval Journal*. <https://doi.org/10.1007/s10791-026-10303-w>
- Wanjihia, M., et al. (2025). Analysis of Network Vulnerabilities and Attack Patterns in Kenyan Public University System. *Journal of African Cybersecurity*.
- Williams, T., & Davis, K. (2023). Web 3.0 and A Decentralized Approach to Education. *arXiv Preprint*.
- Zhang, Y., et al. (2023). Secure Sharing of University Data Using Hyperledger Fabric and IPFS System. *Procedia Computer Science*. <https://doi.org/10.1016/j.procs.2023.09.024>