Blockchain-Based Identity Verification for Zero Trust Access in Kenyan University Student Portals

Dickson Riungu[1*], Angolo Shem Mbandu[1], Benson Kituku[2]

[1] *Cooperative University of Kenya, P.O. Box 24814–00502, Nairobi, Kenya.*

[2] *Dedan Kimathi University of Technology, P.O. Box 657-10100, Nyeri, Kenya*

[*]*Correspondence email: dickson.kriungu@gmail.com*

Abstract

Kenyan universities increasingly rely on student portals for academic and administrative services, and the sensitive data these portals hold makes them attractive targets for cyberattacks. Zero Trust Architecture (ZTA) has been proposed as a more reliable security approach, yet empirical work on combining ZTA with blockchain-based identity verification in student portals is minimal, and the two are usually studied separately. This study analyzed how existing Kenyan university student portals handle identity validation and access control, then designed and evaluated a blockchain-based Zero Trust prototype for secure portal access. Using a Design Science Research Methodology, the prototype was implemented on Hyperledger Fabric and tested in five attack and usage scenarios, each run 10 times. An online questionnaire completed by 49 students of chartered universities showed that all relied on password-based authentication, 71.4% reported that their portal did not require multifactor authentication (MFA), 79.6% were never required to change their passwords, and 87.8% reported no re-verification on sensitive activities. In the simulated tests, the prototype recorded a true acceptance rate of 100%, a false acceptance rate of 0%, 100% ledger-chain integrity, and a composite effectiveness score of 100%; anomaly detection averaged 3.31 seconds in the summary results and 17.9 seconds on the live server. These results come from author-run simulations and a small purposive sample, so they demonstrate feasibility rather than effectiveness in the field. Universities should strengthen portal authentication with MFA and continuous verification, and blockchain-based identity merits evaluation in larger, independent tests.

Keywords: *blockchain, zero trust, verifiable credentials, decentralized identifiers, student portals*

IJPP 14(8); 72-80

1.0 Introduction

The widespread adoption of technology in higher education has transformed how universities deliver academic services. University student portals in Africa have become critical to this transformation, enabling students to register for courses, track academic records, take examinations, and manage fees (Iyanda & Raja, 2025). In Africa and other developing regions, adoption has been accelerated by increased internet penetration, remote and distance learning initiatives, and the need for flexible access to learning resources (Faturoti, 2022). Although these developments have improved education delivery, they have also created cybersecurity challenges, particularly in controlling access to sensitive resources and identifying users securely.

Recent studies point to a heavy threat load in Kenyan universities. Wanjihia et al. (2025) cite a 2025 cybersecurity report indicating that 74% of Kenyan universities experienced cyberattacks over the previous five years. Wambui et al. (2025) reported unauthorized cybersecurity incidents (20%) and phishing attacks (46.4%) in Kenyan university networks, and Okanda and Abass (2025) found that Kenyan university management systems face ransomware attacks, unauthorized access incidents, and data breaches.

Many universities still use perimeter-based models in which trust is implicitly granted after successful authentication, typically with a username and password. With today's threats, such techniques are inadequate for securing entry points. A perimeter-based model that relies on implicit trust creates vulnerabilities that can be exploited through credential compromise, identity theft, and insider threats (Dalal, 2025). Unauthorized access, manipulation of academic records, and data breaches are therefore common risks in university systems.

Zero Trust Architecture (ZTA) has been proposed as a modern way to eliminate implicit trust. It applies continuous verification to every access request, ensuring security through continuous checking of authenticated entities (Kim et al., 2024). This approach reduces the exposed attack surface and improves the security of remote access. Even so, Zero Trust still relies on centralized identity systems, which remain attractive targets and create single points of failure.

Progress in blockchain technology has opened possibilities for decentralized identity management. Standards such as decentralized identifiers (DIDs) and verifiable credentials (VCs) allow users to create their own digital identities instead of relying on centralized authorities. Blockchain-based identity systems can also provide immutable logging through their ledgers, creating reliable, tamper-resistant records (Mazzocca et al., 2025). These capabilities offer an opportunity to bring decentralized identity into Zero Trust.

Despite this relationship between Zero Trust and blockchain-based identity, research on their practical implementation in settings such as university student portals is limited. Kenyan university student portals are widely used but are secured mainly by perimeter-based methods (Owino et al., 2025). An identity-centered and more robust security mechanism is therefore needed, and the lack of an integrated model that combines continuous verification with decentralized identity is a critical gap in both research and implementation.

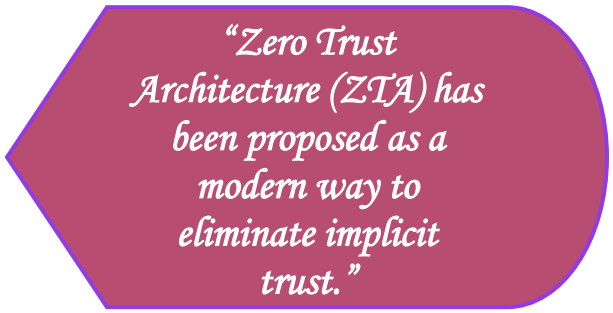
Objective of the Study

The objective of this paper is to analyse existing Kenyan university student portals in relation to identity validation and access control.

Cyber Threats in Learning Institutions

Recent studies describe a range of cyber threats facing learning institutions. Verizon Business (2024) reported that stolen credentials appeared in almost one-third (31%) of breaches over the preceding ten years. Mahmood et al. (2024) note

that universities' emphasis on accessibility, with little attention to secure design, increases vulnerabilities such as weak authentication. In a cybersecurity readiness assessment of Kenyan technical and vocational (TVET) institutions, Kiarie (2024) identified challenges that include the lack of structured cybersecurity teams to manage institutional portals, outdated systems, and unpatched network systems.



University Student Portals

A university student portal is a web-based application that gives students centralized access to administrative and academic resources. Portals support course registration, accommodation allocation, access to examination results, lecturer evaluation, and communication. They improve efficiency, reduce paperwork, and enable students to reach university resources independently (Momanyi et al., 2024; Osunade et al., 2024). Digital systems have also significantly improved records storage, retrieval, and service delivery (Ugonna & Afolabi, 2025).

Most portals are authenticated with usernames and passwords and are linked to university databases containing sensitive personal, academic, and financial data (Kemboi et al., 2025). Password-based authentication is widely used because it is easy and cheap to implement, but it is vulnerable to credential theft, phishing, and password reuse. According to Kiarie (2024), Momanyi and Achimwayi (2017) link such weak authentication to impersonation, phishing, password theft, credential compromise, and unauthorized access. Kimani (2022), in a study of Kenyan universities, found that legacy verification techniques are inadequate for protecting digital identities and proposed multifactor authentication (MFA) to strengthen portal security.

Kenyan university student portals have long relied on perimeter-based models, which assume that entities inside an organization's network can be trusted while threats originate outside it. Although perimeter defenses provide a first line of defense, they are inadequate as a single security paradigm in evolving digital learning contexts. This inadequacy calls for an identity-centered model that continuously validates users and devices, reducing the risks of credential theft, unauthorized access, and session hijacking.

Zero Trust and Blockchain-Based Identity

The Zero Trust concept advocates continuous verification through monitoring of entities both inside and outside the system (Chandramouli & Butcher, 2023). Zero Trust Architecture rests on the principle of "never trust, always verify": threats can exist both inside and outside a network, so implicit trust is removed regardless of device location. Access is granted according to policy, device status, and context such as device location and time (Chandramouli & Butcher, 2023). Its key principles include least-privilege access, continuous verification, micro-segmentation, and policy-driven access.

Blockchain technology has emerged as a promising alternative to centralized identity management because of its tamper resistance and decentralized nature. Din et al. (2024) argue that blockchain strengthens Zero Trust by providing verifiable credentials, decentralized identities, and immutable audit logs. These characteristics enhance identity assurance and support accountability through tamper-resistant logs of authorization and authentication attempts. Zero Trust verifies users continuously before granting access, and blockchain-based identity verification complements this by providing high assurance.

2.0 Materials and Methods

Research Design

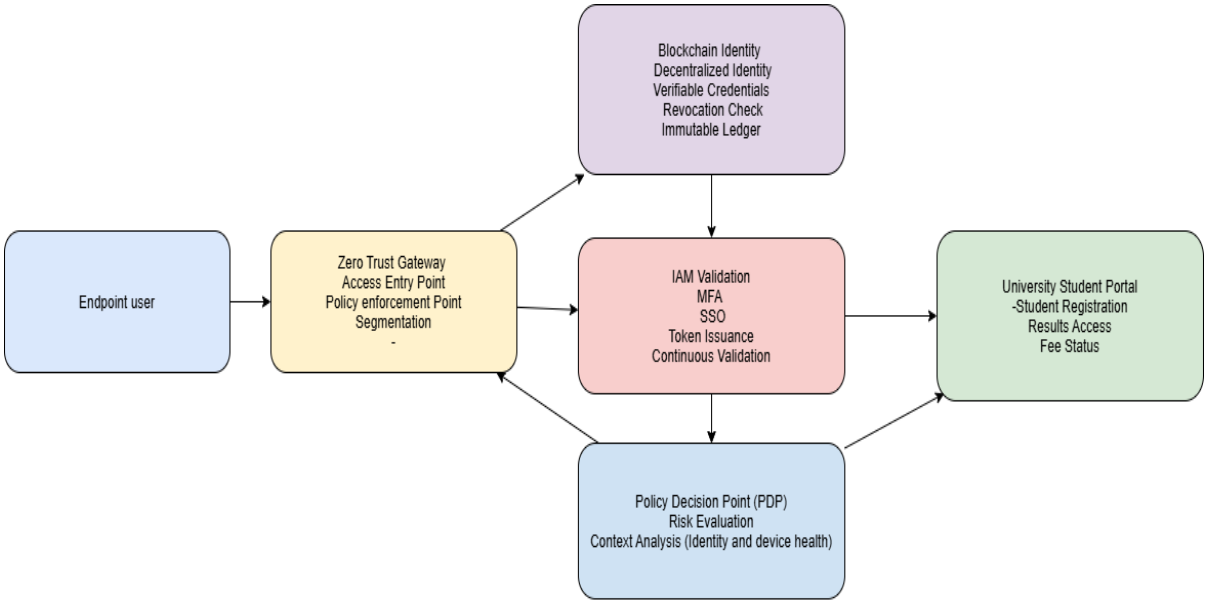
The study used a Design Science Research (DSR) methodology. It is system-based: the target population was operational university student portal systems and their security components, complemented by a survey of student portal users. Scenario-based and purposive sampling were used.

Proposed Model and Prototype

The proposed architecture is shown in Figure 1. A user requests access to the student portal. The system verifies the user's decentralized identity and verifiable credentials through the blockchain, and the verified identity is passed to the identity and access management (IAM) system. The policy decision point (PDP) then evaluates the request against device posture, verified identity, and device context, and access is granted or denied according to Zero Trust principles. The design aims to make identity verification decentralized and its audit trail tamper-evident.

Figure 1

Proposed Model Architecture



The prototype was implemented on Hyperledger Fabric. It combines DID and VC verification on the Fabric network, time-based one-time password (TOTP) enrollment guarded by single-use tokens issued by a registrar, a continuously computed trust score that drives ALLOW, CHALLENGE, DENY, and TERMINATE decisions, and hash-anchored immutable audit logging that operationalizes Zero Trust in a student portal.

Survey of Existing Student Portals

Data for the first objective were collected through a structured online questionnaire administered purposively to undergraduate and postgraduate students of chartered Kenyan universities between May 2026 and September 2026. The expected sample was 60 responses, determined with Slovin's formula. Forty-nine responses were received from different chartered universities, about 82% of the expected number.

Security Evaluation

Five security scenarios were evaluated: (a) genuine user login, (b) invalid credential login attempt, (c) credential stealing and imitation attack, (d) log tampering attempt, and (e) abnormal user behavior requiring continuous verification. Each scenario was run 10 times to reduce random variation. The scenarios were used to measure five security properties: session hijacking, tamper detection, session monitoring, authentication response time, and anomaly detection time. The tests were driven by the study's own attack simulation harness against the live deployed backend, in two runs (Run A and Run B) covering the live server and a local host.

Data Analysis

Survey data and experimental data from the scenario tests were analyzed using descriptive statistics, namely ratios, percentages, and averages, to evaluate prototype performance.

3.0 Results and Discussion

Authentication Practices in Existing Student Portals

All 49 respondents (100%) accessed their portal with password-based credentials: a registration number and password (49.0%), a username and password (28.6%), or an email and password (18.4%); the remaining two respondents (4.1%) used a combination of these. Only one respondent (2.0%) reported using an authenticator application. Thirty-five respondents (71.4%) said their portal did not require MFA and one (2.0%) was unsure, so 73.5% of respondents were not able to confirm MFA on their portal; 79.6% reported that they were never required to change their passwords (Table 1).

A further 87.8% reported that their portal did not re-verify them on sensitive activities, and 14.3% suspected unauthorized access to their own student portal accounts. These findings corroborate the literature reviewed above, which shows that Kenyan university portals rely on weak, password-only authentication (Kiarie, 2024; Owino et al., 2025). They also indicate that the portals do not apply continuous verification, which is the central Zero Trust principle.

Table 1

Authentication Practices Reported by Student Portal Users

Indicator	*n*	%
Portal login credentials		
Registration number and password	24	49.0
Username and password	14	28.6
Email and password	9	18.4
Combination of these methods	2	4.1
Uses an authenticator application	1	2.0
Multifactor authentication (MFA)		
Portal does not require MFA	35	71.4
Unsure	1	2.0
Never required to change password	39	79.6
No re-verification on sensitive activities	43	87.8
Suspected unauthorized access to own account	7	14.3

Note. $N = 49$. Percentages are of all respondents. The count for "combination of these methods" is the remainder of the 49 responses after the three single methods. Data are from the authors' survey.

Design of the Prototype

The second objective was to design a blockchain-enhanced identity verification model. The resulting prototype (Figure 1) implements DID and VC verification on a Hyperledger Fabric network, TOTP enrollment guarded by single-use registrar-issued tokens, a continuously computed trust score that drives ALLOW, CHALLENGE, DENY, and TERMINATE decisions, and hash-anchored immutable audit logging.

Security Evaluation of the Prototype

The third objective was addressed by evaluating the prototype's security measures (Table 2). In the tests, the prototype recorded a true acceptance rate (TAR) of 100% and a false acceptance rate (FAR) of 0%. Ledger-chain integrity was 100%, and the composite effectiveness score was 100%. These findings, however, are based on simulated data from the runs of each security scenario.

Table 2

Summary of Prototype Evaluation Results

Metric	Result
True acceptance rate (TAR)	100%
False acceptance rate (FAR)	0%
Ledger-chain integrity	100%
Composite effectiveness score	100%
Anomaly-detection time	3.31 seconds (summary results); 17.9 seconds (live server)
Authentication overhead	About 2.5 seconds, end to end, including the ledger round trip (threshold: 10 seconds)

Note. Values are as reported by the authors from simulated attack scenarios, each run 10 times. Data are from the authors' evaluation.

The simulation data showed that all attacks were contained across all runs. For instance, all stolen sessions were detected and terminated, and attempts to tamper with the database were detected and prevented. Tamper protection operated at both the blockchain and application layers. The blockchain layer also revoked compromised sessions independently, without any action by the user, and trust scores were recorded on the user dashboard.

Authentication added about 2.5 seconds of overhead, measured end to end including the round trip to the Fabric ledger. This remained below the 10-second threshold used as the upper limit for acceptable responsiveness. On the live server, anomaly detection averaged 17.9 seconds. This value is explained by the rescoring interval and by the number of risk events needed to trigger an anomaly; it does not indicate a slow response to a live threat, because in every observed case termination followed within one monitor cycle.

Taken together, the results indicate that the modeled Zero Trust properties operated as designed in the live deployment of the prototype and not only in a local environment. The composite effectiveness score of 100% means that every measured property (access control, continuous validation, audit integrity, and authentication performance) met its predefined success criterion on the live server. Because the criteria were defined by the study itself, this

shows that the prototype met its design targets; it is not independent evidence of resistance to real-world attacks.

Limitations

Several limitations should be kept in mind. The survey used purposive sampling and reached 49 respondents, about 82% of the 60 expected, all of whom were students; the results describe this sample and are self-reported. The security evaluation used attack scenarios run by the authors' own simulation harness, with 10 runs per scenario and no independent penetration test. The study did not compare the prototype with a baseline, such as MFA with Zero Trust policies but without blockchain, so the results cannot be attributed to blockchain specifically. Usability, user acceptance, cost, and scalability under large-scale use were not evaluated.

4.0 Conclusion

This study examined identity validation and access control in Kenyan university student portals and designed and evaluated a blockchain-based Zero Trust prototype. Among the 49 student respondents, all used password-based authentication, 71.4% reported that their portal did not require MFA, 79.6% were never required to change their passwords, and 87.8% reported no re-verification on sensitive activities. In simulated tests, the prototype contained all attacks, recorded a true acceptance rate of 100% and a false acceptance rate of 0%, and kept ledger-chain integrity at 100%, at the cost of about 2.5 seconds of authentication overhead.

These results show that a blockchain-based, continuously verifying Zero Trust design is technically feasible for student portals. They do not yet show that it is more effective than simpler measures such as MFA, nor that it performs the same way under real-world attack and load. Modern identity security mechanisms are clearly needed in university portals, and the proposed model offers a blueprint for further research on securing student portals in Kenya.

5.0 Recommendations

Password-centered student portals have weaknesses that can lead to the compromise of student data. Kenyan universities should strengthen portal authentication with MFA and continuous verification and should consider piloting blockchain-enabled Zero Trust access technologies to secure sensitive student data.

When implementing an identity verification system, administrators should issue authentication credentials and enrollment tokens out of band and in person, so that stolen credentials alone are not enough to gain access: a stolen username and password would require a complementary token. Private data collected by Hyperledger Fabric should remain off-chain. To keep latency low in large-scale deployments, live systems should use verifiable credential caching and asynchronous ledger anchoring.

Kenyan policy makers and data protection authorities should promote standards that require audit integrity, systems that notify users when their records are accessed, and continuous identity verification of sessions in systems that hold students' academic and personal data. Future work should test the model in larger, independent evaluations and compare it with non-blockchain Zero Trust baselines.

References

Chandramouli, R., & Butcher, Z. (2023). *A zero trust architecture model for access control in cloud-native applications in multi-location environments* (NIST Special Publication 800-207A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207A

Dalal, A. (2025). *Designing zero trust security models to protect distributed networks*

and minimize cyber risks. SSRN. https://ssrn.com/abstract=5268092

Din, I. U., Khan, K. H., Almogren, A., Zareei, M., & Díaz, J. A. P. (2024). Securing the metaverse: A blockchain-enabled zero-trust architecture for virtual environments. *IEEE Access, 12*, 92337–92347. https://doi.org/10.1109/ACCESS.2024.3423400

Faturoti, B. (2022). Online learning during COVID19 and beyond: A human right based approach to internet access in Africa. *International Review of Law, Computers & Technology, 36*(1), 68–90. https://doi.org/10.1080/13600869.2022.2030027

Iyanda, J., & Raja, D. (2025). The role of online learning platforms in transforming African higher education. In P. Neema-Abooki (Ed.), *Quality in African higher education: Development perspectives from selected regions* (pp. 249–268). Brill. https://doi.org/10.1163/9789004731271

Kemboi, B. O., Murungi, R. M., & Kiura, S. M. (2026). Technological determinants of adoption of in- house student management software in public universities in kenya. *Eastern Africa Journal of Contemporary Research*, *5*(2), 94–109. https://www.ajol.info/index.php/eajcr/article/view/316152

Kiarie, N. (2024). Enhancing digital resilience: A cybersecurity readiness assessment of Kenyan TVET institutions. *Journal of the Kenya National Commission for UNESCO, 5*(1). https://doi.org/10.62049/jkncu.v5i1.191

Kim, H., Kim, Y., & Kim, S. (2024). *A study on the security requirements analysis to build a zero trust-based remote work environment* (arXiv:2401.03675). arXiv. https://arxiv.org/abs/2401.03675

Kimani, C. W. (2022). *Developing a multi-factor authentication prototype for improved security of enterprise resource planning systems for Kenyan universities* [Doctoral dissertation, Africa Nazarene University]. https://repository.anu.ac.ke/handle/123456789/864

Mahmood, S., Chadhar, M., & Firmin, S. (2024). Counter-measure strategies to address cybersecurity challenges amidst major crises in the higher education and research sector: An organisational learning perspective. *Information, 15*(2), Article 106. https://doi.org/10.3390/info15020106

Mazzocca, C., Acar, A., Uluagac, S., Montanari, R., Bellavista, P., & Conti, M. (2025). A survey on decentralized identifiers and verifiable credentials. *IEEE Communications Surveys & Tutorials*. https://doi.org/10.48550/arXiv.2402.02455

Momanyi, M. E., & Achimwayi, A. E. (2017). The impact of Internet usage on library reference services in academic libraries in Kenya: A case study of Lukenya University Library. *Journal of African Interdisciplinary Studies*, *1*(2), 69-84. https://www.academia.edu/43961131/The_Impact_of_Internet_Usage_on_Library_Reference_Services_in_Academic_Libraries_in_Kenya_A_case_Study_of_Lukenya_University_Library

Momanyi, E. M., Ng'eno, E., & Kiplang'at, J. (2024). Enhancing information literacy skills of undergraduate medical students: a curriculum and policy analysis. *KLISC Journal of Information Science and Knowledge Management*, *2*(1), 1-16. https://doi.org/10.61735/gchda352

Okanda, P., & Abass, A. (2025). An evaluation of cyber incident management systems in higher education institutions (HEIs) in

Kenya. *Journal of Digital Security and Forensics, 2*(2), 11–37. https://doi.org/10.29121/digisecforensics.v2.i2.2025.50

Osunade, O., Adetimirin, A. E., & Asoro, B. O. (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), 22–32. https://journals.ui.edu.ng/index.php/uijslictr/article/view/1439

Owino, B., Oduor, C., & Chege, G. (2025). An empirical assessment of cybersecurity maturity in higher learning institutions. *Kabarak Journal of Research & Innovation, 15*(2). https://doi.org/10.58216/kjri.v15i02.612

Ugonna, V. A., & Afolabi, A. (2025). Examination of students' record management practices in National Open University of Nigeria (NOUN). *Interdisciplinary Journal of Lifelong Learning, 1*(1), 152–164. https://doi.org/10.52968/15061129

Verizon Business. (2024). *2024 data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/

Wambui, B., Mwinji, M., & Nyambura, H. (2025). AI-driven cybersecurity framework for safeguarding university networks from emerging threats. *Journal of Cyber Security, 7*(1). https://doi.org/10.32604/jcs.2025.069444

Wanjihia, M., Mukudi, F., & Mandela, N. (2025). Analysis of network vulnerabilities and attack patterns in Kenyan public university system networks. *Internet of Things and Cloud Computing, 13*(2), 38–51. https://doi.org/10.11648/j.iotcc.20251302.12