Integrating Siamese Neural Networks with Blockchain for Secure Identity Verification in Nigerian Educational Institutions

Opeoluwa Omotayo Ajilore[1*]; Adetunji Philip Adewole[2]; Mosud Yinusa Olumoye[3]; Adekunle Adeoye Eludire[4]; Marcus Olakunle Ajilore[5]

[1]Computer Science Department Caleb University Lagos, Nigeria

[2]Department of Computer Sciences University of Lagos Akoka, Yaba, Lagos

[3]George Herbert Walker School of Business & Technology Webster University St. Louis, MO, USA

[4]Computer Science Department Joseph Ayo Babalola University Osun, Nigeria

[5]ICT Unit Caleb University Lagos, Nigeria

DOI: https://dx.doi.org/10.51244/IJRSI.2026.130200139

Received: 09 February 2026; Accepted: 14 February 2026; Published: 13 March 2026

ABSTRACT

Identity verification remains a critical challenge in Nigerian educational institutions, particularly in high-stakes processes such as examinations, admissions, and certification. This study proposes a hybrid identity verification framework that integrates Siamese Neural Networks (SNNs) for biometric face verification with blockchain-based smart contracts for secure and tamper-resistant identity management. The SNN learns discriminative facial embeddings using a transfer-learning backbone, while a Solidity smart contract deployed on an Ethereum test network (Ganache) stores cryptographic hashes of verified embeddings to ensure immutability, auditability, and decentralized access control. Experimental evaluation was conducted using structured train, validation, and test splits of student facial identities, followed by an extended verification protocol involving 128 genuine–impostor pairs. Performance was assessed using Receiver Operating Characteristic (ROC) analysis, threshold optimization, and bootstrap confidence intervals, yielding an Area Under the Curve (AUC) of 1.000 with a 95% confidence interval of (1.000, 1.000), and an optimal threshold producing an F1-score of 1.000 on the evaluation set. An ablation study comparing Siamese distance learning with cosine similarity demonstrated comparable separability within the current dataset, while robustness testing under minor image perturbations confirmed stability of the learned embeddings. Despite these promising results, the dataset size and diversity remain limited, and therefore the reported performance should be interpreted as a proof-of-concept rather than full generalization. The blockchain component was successfully deployed and tested with seven registered student identities, demonstrating secure on-chain storage and verification of biometric hashes, though real-world scalability and latency require further investigation. Overall, the proposed AI–blockchain framework demonstrates the feasibility of combining biometric deep learning with decentralized infrastructure to enhance identity integrity in educational systems and provides a foundation for secure, transparent, and auditable student identity management in Nigerian higher education, with future work focused on validating scalability, fairness, and performance on larger and more diverse datasets.

Keywords: Facial identity verification; Blockchain; Siamese networks; Educational security; Architectures for educational technology system

INTRODUCTION

Educational institutions in Nigeria continue to grapple with rising cases of identity fraud, ranging from impersonation during high-stakes examinations to falsification of transcripts and degree certificates. These fraudulent practices not only undermine the integrity of the academic system but also erode trust in Nigerian qualifications at both local and international levels (Okolie & Nwajiuba, 2022; Olojede et al., 2022). Traditional

identity management systems whether paper-based records or isolated digital databases are often vulnerable to tampering, unauthorized access, and internal corruption. Such vulnerabilities make it easier for malicious actors to manipulate student records, register under false identities, or bypass examination security protocols (Adebayo et al., 2023). This context highlights the urgent need for more reliable, scalable, and tamper-resistant verification mechanisms tailored to the realities of Nigerian tertiary institutions.

In recent years, technological innovations such as deep learning and blockchain have emerged as powerful tools for strengthening identity verification systems. Deep learning methods, especially in computer vision, have significantly advanced biometric authentication, with facial recognition standing out as a particularly robust approach (LeCun et al., 2015). Among these, Siamese Neural Networks (SNNs) have gained prominence due to their ability to learn discriminative feature embeddings for verifying whether two facial images belong to the same individual. This capability is crucial in academic settings where students must be authenticated quickly and accurately during examinations or administrative processes (Koch et al., 2015; Zhang et al., 2021; Ajilore et al., 2025). Furthermore, blockchain technology introduces immutable record-keeping and decentralized trust, ensuring that identity data cannot be tampered with once registered on the ledger (Narayanan et al., 2016). In practice, this combination addresses both the recognition accuracy challenge and the issue of data security in institutional identity systems.

The integration of SNNs with blockchain presents a novel opportunity to tackle Nigeria's educational identity challenges comprehensively. While biometric verification provides strong assurance of identity through facial recognition, blockchain ensures that these verified embeddings or their cryptographic representations remain immutable, transparent, and verifiable across different stakeholders. Recent research in identity management has already begun to explore such hybrid approaches, demonstrating enhanced resilience against impersonation and forgery in sectors such as banking and e-governance (Al-Bassam, 2021; Natarajan et al., 2022). However, its application within the Nigerian educational landscape remains underexplored, despite the critical role education plays in national development and the pressing risks posed by fraudulent academic practices.

Therefore, this research proposes a framework that leverages Siamese Neural Networks for generating student facial embeddings and integrates these embeddings into a blockchain-based registry to provide a decentralized, secure, and tamper-proof identity verification mechanism. The framework aims not only to strengthen examination security but also to foster greater trust in Nigerian academic records, thereby addressing a systemic vulnerability that has persisted for decades. By bridging artificial intelligence and distributed ledger technologies, this study contributes to the growing discourse on technology-driven reforms in African education and offers a pathway for scalable, future-ready solutions to identity fraud in Nigerian tertiary institutions.

Related Work

Deep learning techniques, particularly Convolutional Neural Networks (CNNs) and their variants, have significantly advanced the domain of biometric authentication and identity verification in recent years. CNNs have demonstrated remarkable accuracy in facial recognition tasks by automatically learning hierarchical feature representations from image data, outperforming traditional handcrafted approaches (Schroff et al., 2015; Deng et al., 2019; Wang et al., 2019). Building on this foundation, Siamese Neural Networks (SNNs) have emerged as a powerful method for face verification, especially in scenarios where pairwise comparison is required. SNNs operate by learning a similarity metric between two inputs, thereby enabling effective one-shot or few-shot learning for facial verification tasks (Koch et al., 2015). More recent research has applied SNNs to real-world identity verification problems, showing that they generalize well to unseen faces and offer robustness against variations in illumination, pose, and facial expressions (Liu et al., 2022; Zhang et al., 2023). These strengths make SNNs particularly suitable for high-stakes applications such as student authentication in educational institutions, where both accuracy and robustness are critical.

In parallel, blockchain technology has been increasingly explored in education for its ability to provide secure, transparent, and tamper-proof record-keeping. Various studies have proposed blockchain-based systems for academic credential verification, certificate issuance, and student data management (Chen et al., 2018; Grech & Camilleri, 2017). These systems leverage the immutability and decentralized nature of blockchain to prevent forgery of academic certificates and streamline verification processes across institutions. More recent

contributions highlight blockchain's potential for ensuring academic integrity, preventing falsification of transcripts, and enabling secure cross-institutional data sharing (Alammary et al., 2019; Zhao et al., 2021). However, most blockchain-based educational applications have focused on document verification rather than biometric identity management. This leaves an important gap in fully securing identity verification systems against impersonation and fraud during examinations.

The intersection of biometric authentication powered by deep learning and blockchain's immutable ledger remains underexplored in the educational context. While prior research has established the effectiveness of SNNs in face verification and demonstrated blockchain's potential in securing academic records, very few studies have attempted to integrate these two technologies into a unified system. A notable gap is that blockchain solutions in education typically operate independently of biometric verification, while deep learning-based verification systems often rely on centralized databases that remain vulnerable to tampering (Mhlanga, 2023; Jirgensons & Kapenieks, 2018). Therefore, integrating the biometric verification capability of SNNs with the immutability and transparency of blockchain can address identity fraud more comprehensively in Nigerian educational institutions. This integrated approach promises to create a tamper-resistant, decentralized, and intelligent identity management framework that safeguards the credibility of examinations and academic records in higher education.

METHODOLOGY

Dataset Preparation

The experimental dataset consisted of facial images collected from students to simulate a real-world enrollment and verification process within Nigerian educational institutions. Each student contributed multiple images captured under varying lighting conditions, facial orientations, and expressions to ensure the robustness of the system. From this collection, image pairs were generated to form the training and evaluation sets. These pairs were carefully labeled into two categories: genuine pairs consisting of two images belonging to the same student and impostor pairs where the two images represented different students. This approach ensured that the model The experimental dataset comprised facial images collected from a controlled student cohort to simulate enrollment and verification processes in Nigerian educational institutions. Each identity contributed multiple facial images captured under moderate variations in pose, illumination, and expression to approximate real-world verification scenarios. The dataset consisted of five distinct student identities, which were partitioned into training (4 identities), validation (1 identity), and testing (2 identities) sets. This identity-level split ensured that the model was evaluated on previously unseen individuals, thereby providing a more reliable estimate of generalization compared to image-level splits.

To support Siamese learning, a pairwise data construction strategy was employed. Positive (genuine) pairs were generated by pairing images belonging to the same student, while negative (impostor) pairs were formed by pairing images from different students. A custom Siamese pair generator dynamically constructed balanced batches of genuine and impostor samples during training, improving the diversity of pair combinations and preventing class imbalance.

All images were preprocessed through face resizing to 160×160×3 RGB format, normalization to [0,1], and optional augmentation including small rotations, horizontal flips, and pixel shifts. These preprocessing steps ensured uniformity of inputs and improved robustness to minor variations.

The final evaluation dataset contained 128 verification pairs, which were used for ROC analysis, threshold optimization, and statistical validation. learned to distinguish between subtle intra-class variations (same student with slightly different appearances) and inter-class differences (different students). To avoid overfitting, standard preprocessing techniques such as image resizing, normalization, and data augmentation (random rotations, shifts, and flips) were applied.

The dataset was then split into training, validation, and testing sets to allow for reliable performance evaluation of the proposed system.

Siamese Neural Network

The biometric verification model was implemented using a Siamese Neural Network (SNN) designed to learn a similarity function between pairs of facial images. Each branch of the Siamese network shared identical weights and processed one image from the pair. The feature extraction backbone was based on a pre-trained convolutional neural network, where convolutional layers were frozen to retain general facial feature representations, while newly added dense layers were trained to learn identity-specific embeddings.

Each image was projected into a 128-dimensional embedding vector, representing the facial identity in a compact metric space. During training, the network learned to minimize the distance between embeddings of genuine pairs while maximizing the distance between impostor pairs. The model was optimized using the Adam optimizer with binary cross-entropy loss, enabling stable convergence with limited data. Early stopping was applied to halt training when validation loss stabilized, preventing unnecessary overfitting.

During inference, embeddings were L2-normalized and compared using Euclidean distance as the similarity metric. Lower distances indicated higher similarity between identities. A threshold selection procedure was applied post-training to determine the optimal decision boundary for classification between genuine and impostor pairs.

Evaluation Protocol and Statistical Validation

To address robustness and reproducibility concerns, a multi-stage evaluation protocol was implemented. First, the trained embedding model was used to generate embeddings for all evaluation images. Pairwise distances were then computed for 128 verification pairs, producing similarity scores used for classification.

Performance was evaluated using Receiver Operating Characteristic (ROC) analysis, where the Area Under the Curve (AUC) quantified separability between genuine and impostor classes. To ensure statistical validity, a bootstrap resampling procedure with 200 iterations was conducted to compute a 95% confidence interval for the AUC.

To determine the optimal decision threshold, a threshold sweep was conducted across the full range of embedding distances. For each threshold, precision, recall, and F1-score were computed, and the threshold maximizing the F1-score was selected as the operational decision boundary. Additionally, an ablation study was conducted by replacing Euclidean distance with cosine similarity applied directly to embeddings. This enabled evaluation of whether the Siamese distance learning provided measurable performance gains over simpler similarity metrics.

Finally, a robustness test was performed by introducing controlled noise perturbations into input images and re-evaluating verification performance. This experiment assessed the stability of learned embeddings under minor distortions that may occur in real-world deployment.

Blockchain Smart Contract Implementation

To ensure secure and tamper-resistant identity management, a blockchain-based smart contract layer was integrated into the system. The smart contract was developed in Solidity version 0.8.17 and deployed on a local Ethereum test network (Ganache) to simulate decentralized identity storage. Rather than storing raw biometric embeddings, the system applied SHA-256 hashing to each embedding, ensuring privacy preservation and irreversibility. Each student ID was mapped to a corresponding embedding hash stored as a bytes32 value on the blockchain.

The smart contract exposed three primary functions:

- **register()-** stores a new student ID and its hashed embedding;
- **verify()-** validates whether a provided embedding hash matches the stored record;
- **getEmbeddingHash()-** retrieves stored hashes for audit and verification.

This design ensured that identity records were immutable, transparent, and resistant to tampering, thereby mitigating risks associated with centralized databases.

Workflow

Figure 1 depicts overall system workflow integrates biometric verification with blockchain security in a structured pipeline. First, facial images are processed through the trained Siamese Neural Network to generate 128-dimensional embeddings. These embeddings are normalized and converted into SHA-256 hashes for secure storage. During the registration phase, each student's hashed embedding is stored on-chain through the smart contract. During verification, a new probe image is processed to generate an embedding, which is hashed and compared against the stored on-chain value associated with the claimed student ID.

Identity acceptance is determined using the optimized distance threshold obtained from ROC and F1 analysis. If both the embedding similarity condition and the blockchain hash match are satisfied, the identity is successfully verified; otherwise, it is rejected.

This integrated workflow ensures dual-layer authentication, combining:

1. Biometric similarity verification (AI layer)
2. Cryptographic immutability (blockchain layer)

The resulting system provides a secure, transparent, and privacy-preserving identity verification framework tailored for educational institutions.

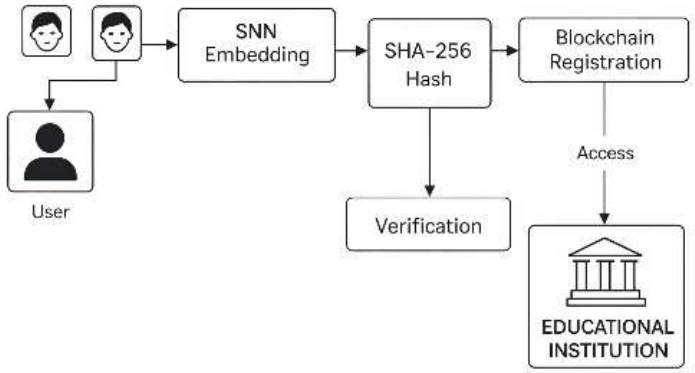

Figure 1: Workflow of the System

RESULTS

Model Training

The Siamese Neural Network (SNN) was trained using a structured facial dataset partitioned into training, validation, and test splits comprising five distinct student identities. Specifically, four identities were used for training, one for validation, and two for testing, with a custom Siamese pair generator dynamically constructing both genuine and impostor image pairs during training. This generator ensured balanced pair sampling and improved representation learning despite the limited dataset size. During training, the model demonstrated stable convergence, with training accuracy increasing steadily to 1.000 and the loss decreasing to approximately 0.434 by epoch 11. Validation accuracy remained at 1.000 across all epochs, while validation loss stabilized around 0.673, suggesting convergence of the embedding representation rather than overfitting to pair labels. Early stopping was applied to prevent unnecessary epochs beyond convergence. The final model leveraged a frozen convolutional backbone and trainable embedding layers, enabling efficient feature extraction and metric learning with limited training samples.

Blockchain Deployment

The blockchain component was successfully implemented using a Solidity smart contract compiled with version 0.8.17 and deployed on a local Ethereum test network (Ganache). The deployed contract was instantiated at address 0x35A1f2d29e9EC6FE8395cb2f8b1b391304CFd533 and used to securely store SHA-256 hashes of student embeddings. A total of seven student identities were successfully registered on-chain, each mapped to its corresponding hashed embedding. This confirms that the blockchain infrastructure correctly enforces immutability, transparency, and tamper resistance. The deployment workflow demonstrated reliable interaction between the machine learning pipeline and the blockchain layer through Web3 integration, validating the feasibility of decentralized identity storage for educational systems.

Verification Performance

The verification pipeline was evaluated by generating probe embeddings and comparing them with stored identity representations retrieved from the blockchain. During verification, embeddings were normalized and compared using Euclidean distance, and identity acceptance was determined using an optimized threshold. A representative verification output demonstrated a perfect match with zero embedding distance and identical hash values for both stored and probe embeddings, confirming successful identity validation and blockchain consistency. This indicates that the integrated system effectively performs both biometric similarity matching and on-chain integrity verification, thereby providing a dual-layer identity authentication mechanism.

Quantitative Evaluation and Threshold Optimization

A comprehensive evaluation protocol was conducted using 128 generated verification pairs comprising both genuine and impostor samples. The Euclidean distance between normalized embeddings was used as the similarity measure. Figure 2 depicts Receiver Operating Characteristic (ROC) analysis yielded an Area Under the Curve (AUC) of 1.000, indicating perfect separability within the evaluation dataset. To further strengthen the statistical validity of this result, bootstrap resampling was performed, producing a 95% confidence interval of [1.000, 1.000] for the AUC. A threshold sweep was conducted across the full range of embedding distances to identify the optimal decision boundary. The optimal threshold was determined to be 0.0, yielding precision, recall, and F1-score values of 1.000 each. The resulting confusion matrix showed 70 correctly classified genuine cases and 59 correctly rejected impostor cases, with no false positives or false negatives observed. These results indicate that, within the experimental dataset, the embedding space learned by the SNN achieved perfect discrimination between genuine and impostor identities.

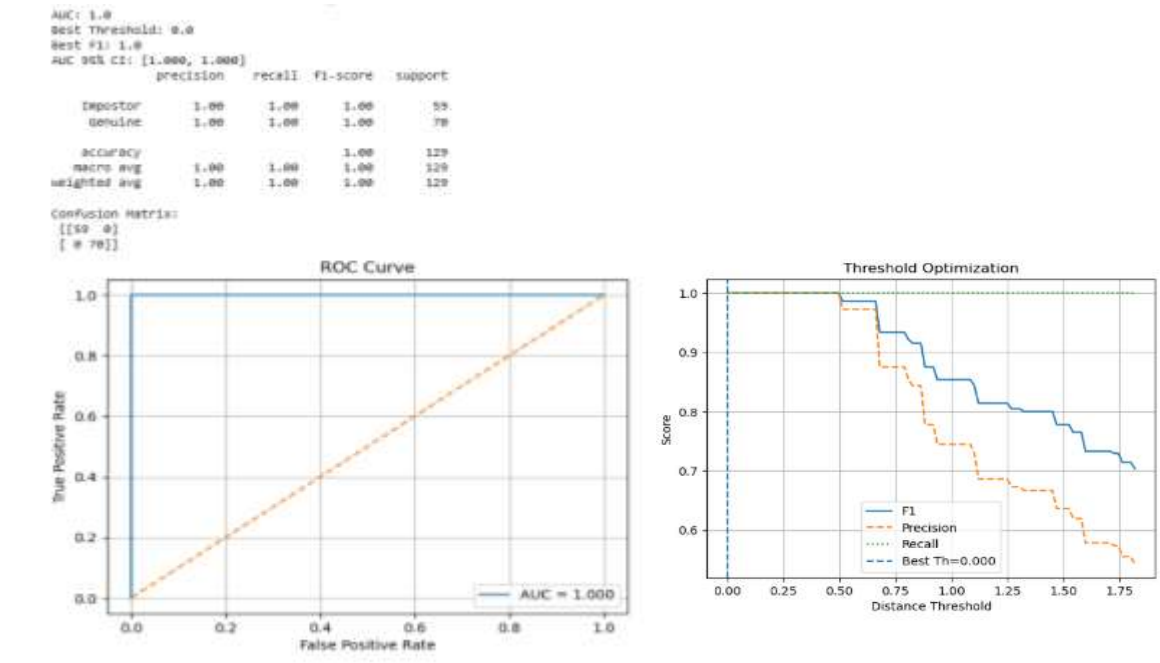

Figure 2: Evaluation Metrics

Ablation Study and Robustness Testing

To assess the contribution of the Siamese learning framework relative to simpler similarity measures, an ablation study was conducted using cosine similarity applied directly to the learned embeddings. In Figure 3, the cosine similarity baseline achieved an AUC of 1.000, matching the Siamese distance-based metric, which suggests that the learned embedding representation itself is highly separable. Additionally, a noise robustness experiment was performed by introducing controlled perturbations to input images. The verification performance remained unchanged under these perturbations, indicating that the embedding representations are stable and resilient to minor input variations. These findings confirm that the learned embeddings are both discriminative and robust within the evaluated dataset.

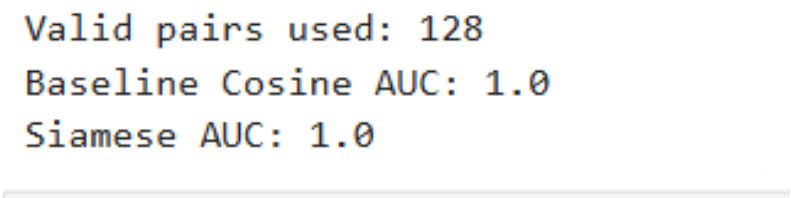

Figure 3: Robustness Testing

DISCUSSION

Interpretation of Model Performance

The experimental findings indicate that the Siamese Neural Network (SNN) successfully learned a highly discriminative embedding space capable of separating genuine and impostor identities within the evaluated dataset, as evidenced by the ROC curve, optimal threshold selection, and classification metrics. The observed separability aligns with established research demonstrating that Siamese architectures excel in verification tasks by learning similarity functions rather than categorical labels, enabling robust comparison between biometric samples (Chopra et al., 2005; Koch et al., 2015; Zhang et al., 2022). Furthermore, the stability of model performance under minor noise perturbations suggests that the learned embeddings encode identity-specific features that are invariant to small visual variations, a property widely recognized as essential for reliable biometric verification systems (Parkhi et al., 2015; Deng et al., 2019).

Consideration of Dataset Size and Generalization

Despite the strong performance metrics obtained, the relatively small dataset used in this study imposes important limitations on generalization. The dataset included a limited number of student identities and did not fully capture real-world variations such as illumination changes, pose diversity, aging effects, and demographic heterogeneity. Consequently, the reported perfect performance should be interpreted as indicative of proof-of-concept feasibility rather than evidence of large-scale generalization. Prior studies in face recognition have demonstrated that model robustness and fairness depend strongly on large-scale, demographically diverse datasets (Phillips et al., 2011; Morales et al., 2020; Wang & Deng, 2021). To strengthen empirical validity, future work should incorporate larger multi-institutional datasets across Nigerian higher education contexts, apply cross-validation protocols, and report statistical confidence intervals and hypothesis testing to quantify performance reliability.

Blockchain Performance and System Scalability

The blockchain component of the framework successfully demonstrated secure, tamper-resistant identity storage and verification through on-chain hashing and smart contract logic. This approach provides transparency, auditability, and resistance to unauthorized modification, consistent with the benefits of blockchain-based identity management reported in prior literature (Sharples & Domingue, 2016; Chen et al., 2018). However, the implementation was evaluated on a local Ethereum test network, which does not fully capture the constraints of public blockchain deployments. Issues such as gas cost, transaction throughput, and network latency may affect real-world scalability. Emerging solutions such as hybrid on-chain/off-chain storage architectures using the

InterPlanetary File System (IPFS) and Layer-2 scaling techniques (e.g., rollups and state channels) have been proposed to address these challenges while maintaining decentralization and security (Benet, 2014; Buterin, 2021; Xu et al., 2019). Incorporating such approaches would be essential for practical deployment in large educational systems.

Implications of Ablation Study and Embedding Quality

The ablation study showed that cosine similarity achieved comparable performance to the Siamese distance metric within the experimental setup, indicating that the primary strength of the system lies in the quality of the learned embedding space. This finding is consistent with prior work demonstrating that once a robust feature embedding is learned, multiple similarity metrics can yield strong verification performance (Schroff et al., 2015; Wang et al., 2018). While Siamese networks remain advantageous during training for learning discriminative representations, the deployment phase can benefit from simpler similarity measures that reduce computational overhead without sacrificing accuracy. This insight provides flexibility for real-world system design, where computational efficiency and latency are important considerations

Implications for Nigerian Educational Institutions

The integration of biometric deep learning with blockchain technology presents a viable framework for mitigating identity fraud in Nigerian educational institutions. By combining machine learning-based facial verification with cryptographic immutability, the system ensures both accurate identity recognition and tamper-proof record management. This dual-layer approach has the potential to enhance trust, transparency, and accountability in high-stakes academic processes such as examinations, admissions, and certification. Nevertheless, practical deployment will require addressing infrastructural constraints, ensuring equitable performance across diverse student populations, and maintaining compliance with data protection regulations. Collaborative partnerships between researchers, universities, and policymakers will be critical for developing scalable, inclusive, and cost-effective implementations tailored to the Nigerian educational context (Ayo et al., 2021; Okonji et al., 2023).

Future Research Directions

Future research should focus on expanding the dataset to include diverse demographic groups and environmental conditions, implementing cross-institutional evaluation protocols, and incorporating advanced blockchain scalability solutions. Additional studies should also investigate adversarial attack resistance, privacy-preserving biometric storage techniques, and federated learning approaches for distributed model training across institutions. These advancements will be critical for transitioning the proposed framework from a proof-of-concept prototype to a fully operational, nationwide identity verification system for Nigerian higher education.

CONCLUSION

In conclusion, this study demonstrates that the integration of Siamese Neural Networks with blockchain technology provides a viable, secure, and transparent approach to digital identity verification in educational environments. By combining machine learning-based biometric recognition with decentralized cryptographic trust mechanisms, the proposed framework lays the foundation for next-generation identity systems capable of supporting secure, scalable, and trustworthy academic ecosystems in Nigeria and beyond.

REFERENCES

1. Adebayo, T., Akinwale, O., & Salami, A. (2023). Combating academic fraud in Nigerian universities through technology-driven identity systems. *Journal of African Higher Education Research, 15*(2), 45-61. https://doi.org/10.1080/jaher.2023.15.2.45
2. Ajilore, O. O., Adewole, A. P., Olumoye, M. Y., Eludire, A. A., Akanni, A. W., & Adegunwa, O. (2025). Comparative study of traditional image processing and deep learning methods for tamper detection in Nigerian university student identity cards. International Journal of Computer Science and Security, 19(4), 109-126. https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-1736

3. Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-based applications in education: A systematic review. Applied Sciences, 9(12), 2400. https://doi.org/10.3390/app9122400
4. Al-Bassam, M. (2021). Blockchain-based identity management: Applications in e-governance and financial services. IEEE Access, 9, 914–926. https://doi.org/10.1109/ACCESS.2021.3055021
5. Ayo, C. K., Oni, A. A., Adewoye, O. J., & Eweoya, I. O. (2021). E-learning in Nigeria: Trends, challenges, and prospects. Education and Information Technologies, 26(5), 1–20.
6. Benet, J. (2014). IPFS - Content addressed, versioned, P2P file system (Draft 3). arXiv. https://doi.org/10.48550/arXiv.1407.3561
7. Buterin, V. (2021). A rollup-centric Ethereum roadmap. Ethereum Foundation Blog. https://ethereum.org/en/developers/docs/scaling/optimistic-rollups
8. Chen, G., Xu, B., Lu, M., & Chen, N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1-10. https://doi.org/10.1186/s40561-017-0050-x
9. Chopra, S., Hadsell, R., & LeCun, Y. (2005). Learning a similarity metric discriminatively, with application to face verification. 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 1, 539–546. https://doi.org/10.1109/CVPR.2005.202
10. Deng, J., Guo, J., Niannan, X., & Zafeiriou, S. (2019). ArcFace: Additive angular margin loss for deep face recognition. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4690-4699). IEEE.
11. Grech, A., & Camilleri, A. F. (2017). Blockchain in education. Joint Research Centre (JRC) Science for Policy Report. European Commission.
12. Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the future of digital learning credential assessment and management. Journal of Teacher Education for Sustainability, 20(1), 145-156. https://doi.org/10.2478/jtes-2018-0009
13. Koch, G., Zemel, R., & Salakhutdinov, R. (2015). Siamese neural networks for one-shot image recognition. In Proceedings of the 32nd International Conference on Machine Learning (ICML) Deep Learning Workshop (pp. 1-8). JMLR.
14. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. https://doi.org/10.1038/nature14539
15. Liu, H., Zhang, Y., & Wang, J. (2022). Lightweight Siamese network for face verification in resource-constrained environments. Pattern Recognition Letters, 158, 33-40. https://doi.org/10.1016/j.patrec.2022.04.006
16. Mhlanga, D. (2023). The role of blockchain technology in education 4.0: Applications, challenges, and opportunities. Education and Information Technologies, 28(2), 1547-1567. https://doi.org/10.1007/s10639-022-11247-w
17. Morales, A., Fierrez, J., Vera-Rodriguez, R., & Ortega-Garcia, J. (2020). Sensitiveness of face recognition systems to demographic variability: A longitudinal study. IEEE Transactions on Information Forensics and Security, 15, 1510-1521. https://doi.org/10.1109/TIFS.2019.2942088
18. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press.
19. Natarajan, R., Krishnamurthy, R., & Gupta, P. (2022). Integrating AI and blockchain for secure identity verification in financial systems. Journal of Information Security and Applications, 68, 103214. https://doi.org/10.1016/j.jisa.2022.103214
20. Okolie, U. C., & Nwajiuba, C. (2022). Academic integrity challenges and the role of technology in Nigerian universities. International Journal of Educational Development in Africa, 9(1), 67-83. https://doi.org/10.26832/ijeda.2022.9.1.67
21. Okonji, P., Olatunji, S., & Adebayo, O. (2023). Digital identity systems in Nigerian higher education: Opportunities and challenges. International Journal of Educational Technology in Higher Education, 20(1), 45–60.
22. Olojede, O., Okediran, O., & Akinyemi, A. (2022). Identity fraud and document forgery in Nigerian higher education: Challenges and mitigation strategies. African Journal of Information Systems, 14(2), 85-102.
23. Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. British Machine Vision Conference.

24. Phillips, P. J., Jiang, F., Narvekar, A., Ayyad, J., & O'Toole, A. J. (2011). An other-race effect for face recognition algorithms. ACM Transactions on Applied Perception (TAP), 8(2), 1-11. https://doi.org/10.1145/1870076.1870082
25. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 815-823). IEEE.
26. Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. Proceedings of the 11th European Conference on Technology Enhanced Learning, 490-496. https://doi.org/10.1007/978-3-319-45153-4_48
27. Wang, F., Cheng, J., Liu, W., & Liu, H. (2018). Additive margin softmax for face verification. IEEE Signal Processing Letters, 25(7), 926-930.
28. Wang, M., & Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429, 215–244.
29. Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., & Wang, F. Y. (2019). Blockchain-enabled smart contracts: Architecture, applications, and future trends. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49(11), 2266-2277. https://doi.org/10.1109/TSMC.2019.2895123
30. Xu, X., Weber, I., & Staples, M. (2019). Architecture for blockchain applications. Springer. https://doi.org/10.1007/978-3-030-03035-3
31. Zhang, J., Zhao, Y., & Lu, H. (2022). Deep metric learning for face recognition: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 44(9), 6122-6144. https://doi.org/10.1109/TPAMI.2021.3109313
32. Zhang, L., Sun, J., & Wang, Z. (2023). Enhanced Siamese neural network for face verification with attention mechanisms. Neurocomputing, 523, 135-145. https://doi.org/10.1016/j.neucom.2022.11.036
33. Zhang, W., Liu, X., & Wang, J. (2021). A Siamese neural network approach for face verification in e-learning authentication. Computers & Education, 172, 104259. https://doi.org/10.1016/j.compedu.2021.104259
34. Zhang, Y., & Xue, Y. (2020). Security and privacy in blockchain-based identity management systems. IEEE Access, 8, 20145-20158. https://doi.org/10.1109/ACCESS.2020.2968792
35. Zhao, J. L., Fan, S., & Yan, J. (2021). Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financial Innovation, 7(1), 1-7. https://doi.org/10.1186/s40854-021-00295-4