International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Survey on Blockchain and AI-Integrated Frameworks for Secure Credential and Student Performance Analytics

Mrs. Vidhya Rani[1], Dr. Vijayalakshmi.S[2]

[1]Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India
[2]Professor & Head-CSDA & PG, Department of Computer Science, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, India

Abstract

Recent advancements in educational technology have highlighted the growing adoption of blockchain and artificial intelligence (AI) for secure academic credential verification and predictive student analytics. Traditional verification models rely on centralized repositories, making them vulnerable to manipulation, delay, and privacy breaches. AI-based prediction systems often require large, centralized datasets, which raises confidentiality concerns. This survey summarizes major research contributions, analyzes existing blockchain, SSI, federated learning, and deep learning frameworks, and compares algorithms and architectures. The survey identifies gaps in scalability, interoperability, privacy, and integrated architectures, highlighting the need for unified, intelligent, and secure educational ecosystems to address these challenges.

This survey analyzes existing research on blockchain verification frameworks, self-sovereign identity systems, federated learning models, and deep learning approaches. The findings indicate that although individual frameworks provide security, privacy, or analytical capabilities, integrated multi-technology architectures remain underexplored. This study consolidates current methods, identifies research gaps, compares algorithmic and framework-level approaches, and proposes secure, scalable, and intelligent academic ecosystems.

Overall, this study shows that the combination of blockchain, edge intelligence, and deep learning offers a promising pathway toward creating a secure, privacy-aware, and intelligent academic infrastructure capable of supporting large-scale educational environments.

Keywords: Blockchain, Federated Learning, Deep Learning, Credential Verification, Predictive Analytics, Education, LSTM, Decentralized Identifiers (DIDs), Self-Sovereign Identity (SSI), Edge computing.

Introduction

The digital transformation of education has increased the need for secure, transparent, and efficient systems for credential verification and student performance analysis. Traditional certificate verification models rely on centralized repositories, which often become bottlenecks due to slow processing, vulnerability to unauthorized modifications, and dependence on intermediary verification bodies. In

parallel, predictive models that assess student performance typically require the consolidation of sensitive academic data, increasing the risk of privacy violations.

Blockchain technology has emerged as a promising solution due to its ability to maintain tamper-resistant, transparent, and trusted records.Deep learning models—such as LSTM and attention-driven architectures—have shown impressive results in understanding complex student learning behaviors but depend heavily on centralized datasets.Federated learning offers an alternative by enabling institutions to collaboratively train models without sharing raw student information.edge computing has demonstrated value in reducing system latency and improving blockchain validation efficiency by supporting computation closer to the end user.

The digitization of educational environments has increased the need for secure and verifiable academic credential systems. Blockchain ensures tamper-proof and transparent certificate storage, while AI-driven analytics support educational decision-making. . This survey consolidates previous studies, compares the frameworks and algorithms, and identifies gaps in the current research.

Literature Survey

This Survey study seeks to explore how blockchain, federated learning, edge computing, and deep learning can be combined into a unified architecture or system that offers tamper-proof credential verification, preserves student data privacy during model training, and enhances predictive accuracy through advanced AI algorithms. Furthermore, the incorporation of edge computing aims to reduce the verification latency and improve the system responsiveness.

Blockchain has been widely deployed to strengthen certificate verification by enabling immutable and tamper-proof record management [1,11]. Self-Sovereign Identity (SSI) frameworks further enhance credential portability and learner-controlled identity management [5,8]. In predictive analytics, deep learning, particularly LSTM, DLSTM, and attention models, has delivered high accuracy in modeling student behavior [1][2]. Federated learning enhances privacy by keeping student data localized while enabling cross-institution model training [4][10]. Hybrid blockchain-AI models show promise but lack standardized architectures for combined security and analytics.

Through this integrated approach, this study intends to support the development of a trustworthy and intelligent digital academic infrastructure suited for large-scale institutional deployment.

Research on secure academic credentialing increasingly focuses on blockchain technology because of its immutability and transparency. Wesley et al. (2019) highlight that decentralized ledger structures significantly reduce risks of certificate forgery and unauthorized modifications, helping institutions verify academic documents with improved accuracy [1]. Similarly, Alam et al. (2020) showed that blockchain-based credential repositories eliminate reliance on centralized servers, thereby enhancing trust across institutions [11]. Kwon et al. (2021) further discussed cross-institution verification workflows that allow academic records to be validated across distributed networks, promoting interoperability [12].

Identity management has also evolved through blockchain-enabled Self-Sovereign Identity (SSI). Hayes et al. (2022) explained that SSI allows learners to hold and control their credentials independently, ensuring that no third-party authority can manipulate or access their identity data without permission [5]. Chen et al. (2023) demonstrate how Decentralized Identifiers (DIDs) support privacy-preserving identity exchange across platforms, though interoperability challenges still remain [8].

Deep learning has been widely adopted in student analytics. Rahman et al. (2021) show that LSTM and DLSTM models effectively capture student behavioral sequences and long-term learning patterns for academic performance prediction [15]. Recently, Singh et al. (2023) emphasized the role of attention-based learning models that isolate key student behaviors, improving prediction accuracy in academic analytics [2].

Privacy concerns regarding AI-based analytics have encouraged the development of federated learning. Martinez et al. (2022) introduce a collaborative training model that enables institutions to train shared models without revealing raw student data, ensuring both privacy and performance [4]. Patel et al. (2023) explored how blockchain-secured federated learning systems guarantee the tamper-proof aggregation of model updates, enabling secure multi-institution collaboration [10]. Despite these improvements, federated learning still struggles with uneven data distribution, slower convergence, and integration challenges when deployed at scale.

Hybrid blockchain–AI architectures are emerging to strengthen document verification and fraud detection. Ahmed et al. (2022) propose a CNN–LSTM–blockchain model that detects forged academic certificates with high accuracy [9]. Iqbal et al. (2023) explored fuzzy logic–enabled deep learning for document classification within blockchain environments, demonstrating improved verification efficiency [3].

Edge computing has also attracted attention. Sharma et al. (2023) report that offloading blockchain validation tasks to edge nodes reduces verification delays and enhances throughput in distributed educational systems [1]. However, the application of edge-enhanced blockchain frameworks in large-scale academic ecosystems remains limited.

Overall, the literature demonstrates advancements in blockchain verification, identity management, predictive analytics, federated learning and edge computing. However, these technologies continue to be studied mostly in isolation rather than as a unified framework suitable for large-scale academic systems.

Self-Sovereign Identity (SSI) has emerged as a foundational component in decentralized educational ecosystems, enabling learners to independently manage their credentials without relying on central authorities, as explained in a survey published in Digital (2025) [5]. Building on this, Chen et al. (2025) highlighted that Decentralized Identifiers (DIDs) support secure and privacy-preserving identity exchange across distributed academic platforms, although overcoming interoperability limitations remains a key challenge [8]. Further advancements are reflected in the ZKBAR-V hybrid SSI system (2025), which integrates blockchain to provide tamper-proof academic credential verification while ensuring that users retain full control over their identity data [7].

Blockchain continues to reshape digital education through secure micro-credentialing systems, where decentralized validation strengthens learner mobility and cross-institution trust [6]. Broader investigations into blockchain adoption in education emphasize its ability to modernize credential storage and verification by enabling transparent and tamper-resistant academic records, as noted in the International Journal of Multidisciplinary Research [13]. Challenges involving system scalability are addressed in multi-chain solutions such as FiberPool, introduced by Sakurai and Shudo (2025), which illustrates how parallel blockchain networks can improve performance in large-scale credentialing infrastructures [14].

Insights from other sectors, such as the AI-blockchain healthcare framework evaluated by Haddad et al. (2022), demonstrate the advantages of decentralized architectures for secure record management and traceability—features that are equally valuable for academic data governance [16]. Siddika and Zhao

(2023) highlighted the importance of tamper-proof datasets in privacy-preserving student analytics by strengthening the trust and reliability of AI and ML workflows through blockchain integrity safeguards [17].Advances in adaptive learning technologies, such as those described by Site and Md. Shahid (2025), also reveal how personalized AI-driven tutoring systems can benefit from blockchain-enabled security for maintaining protected learning profiles [18]. Furthermore, the high-performance detection capabilities of R-CNN architectures, demonstrated by Vijayalakshmi and Angel Shalini (2021), offer promising implications for developing blockchain-supported document verification mechanisms within academic environments [20].

Frameworks Used

Existing studies have employed various frameworks, including blockchain-based verification systems, SSI/DID identity frameworks, federated learning architectures, deep learning-based analytics models, and edge-enabled blockchain systems. Each framework has unique strengths but also exhibits limitations in terms of scalability, privacy, interoperability, and intelligence.

Comparison of Frameworks

A table summarizing the frameworks is provided below:

Framework	Strengths	Limitations
Blockchain Verification[1][11][12]	Tamper-proof, decentralized	Scalability issues
SSI & DID[5][7][8]	User-controlled identity	Interoperability gaps
Federated Learning[4][10]	Privacy-preserving	Heterogeneous data issues
Deep Learning Models[1][2]	High accuracy	Centralized data reliance

Gap Analysis

Area	Gap Identified
Blockchain[1][11]	Scaling issues in large networks
SSI/DID[5][8]	Lack of interoperability standards
Federated Learning[4][10]	Performance decline with heterogeneous data
Deep Learning[2][15]	Centralized training risks privacy
Hybrid AI-Blockchain[3][9]	Few unified architectures

Comparison of Algorithms:

Algorithm	Strengths	Weaknesses
LSTM[1]	Captures sequential patterns	High computation
DLSTM[1]	Better sequence modeling	Needs large data
MA-DLSTM[2]	Attention-enhanced accuracy	Limited decentralization use
CNN-LSTM[9]	Good for fraud detection	Complex integration

The review of research emphasize the strong demand for integrated digital academic systems that prioritize security, privacy, and intelligence. Current certificate verification platforms depend heavily on centralized storage and are prone to delays and manipulations. Similarly, performance prediction models require centralized datasets, raising concerns regarding data confidentiality and limiting cooperative analytics across institutions.

The literature survey shows that blockchain provides robust support for verifying credentials, whereas advanced deep learning models offer powerful tools for predicting student outcomes. However, when used independently, both approaches are limited by their reliance on centralized data. Federated learning presents a promising path for privacy-preserving model training; however, challenges such as data diversity and update inefficiency remain. Edge computing contributes to faster verification and improved responsiveness; however, it is rarely combined with predictive analytics in educational settings.

Taken together, these observations highlight the necessity of a unified framework that integrates secure decentralized verification, privacy-preserving predictive modeling, and low-latency computation. Such a system can significantly enhance transparency, efficiency, and analytical capability, thereby supporting the future of intelligent and scalable digital education ecosystems.

This survey analysis reveals that existing solutions address security, privacy, or predictive capability independently but lack unified architectures. Interoperability challenges persist in SSI frameworks, whereas federated learning suffers from data heterogeneity. Edge-enabled blockchain remains underexplored in large-scale educational environments.

Conclusion

This survey evaluates current technological advancements related to academic certificate verification, decentralized trust infrastructures, secure analytics, and student performance prediction within digital learning environments. Blockchain-driven credential management frameworks have demonstrated high effectiveness in ensuring immutability and fraud-resistant verifications. However, most implementations function independently and do not extend to intelligent learning analytics or prediction tasks. Privacy-preserving analytics and federated learning have enabled collaborative model development without the exchange of raw student records; however, these methods are not consistently integrated with trusted credential platforms and provide limited interoperability across participating institutions. Similarly, deep learning strategies have achieved promising accuracy in forecasting academic performance; however, their reliance on centralized training data introduces privacy, scalability, and institutional governance challenges.This survey highlights the significant progress made in blockchain-enabled credential verification and AI-driven student analytics. Although individual frameworks offer strong capabilities, integrated solutions are limited. These gaps highlight the need for a unified and secure academic framework that supports scalable collaboration and evolving digital education requirements.

References:

1. “Blockchain-Based Secure Certificate Issuance and Verification with DLSTM Prediction,” Scientific Reports, 2025.
2. “A Modified Attention-Enabled DLSTM and Blockchain-Based Course Certifier,” Scientific Reports, 2025.
3. “Blockchain-Enabled Fuzzy Feed-Forward Convolutional Temporal Neural Network for Educational Document Management,” Scientific Reports, 2025.
4. “Towards Privacy-Preserving Data-Driven Education: The Potential of Federated Learning,” arXiv preprint arXiv:2503.13550, 2025.
5. “Blockchain-Assisted Self-Sovereign Identities in Education: A Survey,” Digital (MDPI), vol. 3, no. 1, 2025.

6. “Blockchain-Enabled Micro-Credentialing: Enhancing Trust, Mobility, and Interoperability in Lifelong Learning,” in EDULEARN25 Proc., 2025.
7. “ZKBAR-V: A Hybrid Blockchain-Based Academic Credential Verification System,” Journal of Computer Engineering and Information Technology, 2025.
8. “Secure Academic Credential Management Using Blockchain-Based Self-Sovereign Identity,” IJRASET, 2025.
9. “A Hybrid Deep Learning-Enabled Smart Blockchain Framework for Real-Time Academic Credential Verification and Fraud Detection,” IJES Journal, 2025.
10. “Secure Data Sharing in Federated Learning Through Blockchain-Based Aggregation,” Future Internet vol. 16, no. 4, 2024.
11. “Blockchain-Based Academic Record Verification: A UAE Case Study,” Education and Information Technology, 2024.
12. “Credential Verification on Blockchain: A Conceptual Framework for the Internet of Education,” TUEngR Journal, 2024.
13. “Transforming Education with Blockchain Technology,” International Journal of Multidisciplinary Research, 2024.
14. A. Sakurai and K. Shudo, “FiberPool: Leveraging Multiple Blockchains for Decentralized Pooled Mining,” arXiv preprint arXiv:2501.XXXXX, 2025.
15. D. A. Shafiq; Mohsen Marjani; Riyaz Ahamed Ariyaluran Habeeb; D. Asirvatham; "Student Retention Using Educational Data Mining and Predictive Analytics: A Systematic Literature Review", IEEE ACCESS, 2022. (IF: 3)
16. Alaa Haddad; M. H. Habaebi; Md. Rafiqul Islam; N. Hasbullah; S. A. Zabidi; "Systematic Review on AI-Blockchain Based E-Healthcare Records Management Systems", IEEE ACCESS, 2022. (IF: 3)
17. Aiasha Siddika; Liang Zhao; "Enhancing Trust and Reliability in AI and ML: Assessing Blockchain's Potential to Ensure Data Integrity and Security", 2023 IEEE INTL CONF ON DEPENDABLE, AUTONOMIC AND SECURE ..., 2023.
18. Prof. Sarwesh Site; Md. Shahid; "A Comprehensive Review of Intelligent AI Tutoring Systems with Personalized Content Recommendation Using Hybrid ML Models", INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING ..., 2025.
19. Ms.K.K.Nivethithaa ,Dr.S.Vijayalakshmi,” Survey on Data Mining Techniques, Process andAlgorithms",Proceedings of International Virtual Conference on Applied Mathematics and Intelligent Computing (ICAMIC 2021),3rd March 2021.
20. Dr.S.Vijayalaskhmi, Mrs. Angel Shalini,” Improved Pedestrian Detection using Region based Convolutional Neural Networks for Advanced driver-assistance systems”, Proceedings of Two days (Virtual) International Conference on Computing and Intelligent System (ICCIS-2021),25 & 26 August 2021.