CYBERSECURITY TECHNOLOGIES FOR ELECTRONIC EDUCATION RECORD (EER) SYSTEMS BASED ON BLOCKCHAIN AND CLOUD COMPUTING

Kyrychenko Oleg
ORCID ID: 0009-0006-4445-4057
PhD Student
Department of Software Engineering and Management Intelligent Technologies
National Technical University "Kharkiv Polytechnic Institute", Ukraine

Scientific advisor: Shmatko Oleksandr
ORCID ID: 0000-0002-2426-900X
Ph.D., Associate Professor, Associate Professor
Department of Digital Technologies and Project Analytical Solutions
Technical University "Metinvest Polytechnic" LLC, Ukraine

Abstract. *Traditional electronic education record (EER) management systems operate as isolated silos in which each educational institution maintains its own records independently. This separation complicates the verification and sharing of academic information across different platforms. Blockchain technology has recently emerged as a promising solution for secure and transparent record sharing among institutions operating on diverse infrastructures. However, storing complete education records directly on a blockchain remains impractical due to inherent storage limitations and the associated computational cost. To mitigate these challenges, this paper proposes a cloud-assisted blockchain model that combines the immutability of blockchain with the scalability of cloud storage.*

In the proposed architecture, blockchain technology ensures data integrity and access control through immutable transaction logs, while cloud computing provides an efficient and flexible medium for storing encrypted educational records. Elliptic Curve Cryptography (ECC) is employed to enable secure communication and mutual authentication among entities. The system has been validated through informal and formal methods, including AVISPA simulation and BAN logic analysis, demonstrating resistance to common cyber threats and confirming mutual authentication. Comparative evaluation indicates that the proposed model offers a practical balance between security, scalability, and efficiency, making it suitable for real-world academic environments.

Introduction. The digitization of education has accelerated the transition toward electronic education records, which store and manage student credentials, transcripts, and achievements in digital form. Despite their advantages, traditional EER systems remain largely centralized, where each

institution maintains an independent database. This isolation causes duplication, inconsistencies, and difficulties in verifying academic credentials across institutions. In addition, the lack of interoperability among legacy systems creates vulnerabilities that threaten data privacy and authenticity [1].

Blockchain technology has emerged as a transformative solution capable of addressing these limitations by providing a decentralized, immutable ledger of transactions. It enables trust among untrusted participants through distributed consensus and cryptographic integrity [2]. Nevertheless, fully blockchain-based EER systems face scalability constraints, as storing large amounts of data within blocks is both costly and inefficient [3-4]. Furthermore, the static nature of blockchain records limits flexibility when handling diverse data formats such as scanned certificates and learning portfolios.

This study presents a hybrid solution that integrates blockchain with cloud computing. Blockchain serves as a trust layer that records transaction metadata and ensures data integrity, while the cloud provides scalable and accessible storage for encrypted educational data. This combination leverages the strengths of both technologies—immutability and scalability—while mitigating their individual weaknesses. The architecture aims to establish a secure, transparent, and efficient framework for academic record management applicable across universities, accreditation agencies, and certification authorities.

Related work. The idea of integrating blockchain with educational data management has received growing attention over the past decade. Sharples and Domingue (2016) were among the first to propose using blockchain for issuing and verifying digital credentials, emphasizing the potential of distributed trust systems in academia. Subsequent initiatives such as Blockcerts and EduCTX demonstrated practical implementations for degree authentication and transcript verification. However, these systems often relied on public blockchains, which suffer from high transaction latency, privacy concerns, and limited scalability.

More recent studies have focused on hybrid and private blockchain architectures to improve performance and control. In [5] introduced a blockchain framework that uses off-chain storage for educational data, achieving improved efficiency but limited encryption strength. In [6] proposed blockchain-based smart contracts for degree validation but did not fully address the challenge of securely linking blockchain transactions with external storage systems.

In contrast, the model presented in this paper integrates blockchain with cloud computing through secure RESTful communication. The use of ECC cryptography provides lightweight encryption suitable for resource-constrained educational infrastructures, while the application of formal verification tools such as AVISPA ensures that the proposed authentication protocol is resistant to common cyber threats. This approach not only enhances security but also provides the scalability required for large-scale educational ecosystems.

System design and architecture. The proposed system consists of four primary entities: the network administrator, the educational institution, the student, and the blockchain network supported by a cloud server [7=8]. The system is initialized when both students and educational institutions register with the network administrator, who assigns unique digital identities based on ECC key pairs. Once registered, the student is authenticated by the institution through a secure channel that establishes a trust relationship for subsequent communication.

After authentication, the educational institution generates a smart contract defining the permissions, ownership, and conditions under which the student's records can be accessed. This contract is permanently stored in the blockchain ledger, ensuring transparency and immutability. When a student's academic data is updated, the institution encrypts the corresponding EER files using ECC-based public keys and uploads them to the cloud server. Instead of storing the full content on-chain, the blockchain records only metadata such as file hashes, timestamps, and institutional signatures. This mechanism ensures that the data remains confidential while its integrity can be independently verified.

The cloud server acts as a distributed repository for encrypted academic data. It supports secure retrieval and synchronization with blockchain transactions, enabling authorized parties to access records without compromising privacy. The blockchain operates as a permissioned network managed by accredited institutions to ensure that only verified participants can append or read transactions. The combination of blockchain immutability and cloud scalability forms a hybrid environment capable of supporting large datasets with verifiable provenance.

The architecture employs ECC-based encryption for both data storage and communication, offering high cryptographic strength with reduced key sizes compared to traditional methods such as RSA. This choice improves

performance without sacrificing security, making the system efficient even for institutions with limited computational resources. All interactions between the blockchain and cloud components occur through a secure RESTful API, minimizing communication overhead and enabling interoperability across different software infrastructures.

Security validation of the proposed architecture was conducted using a combination of informal reasoning and formal verification tools. The system's security model was examined against standard network attack scenarios, including replay, man-in-the-middle, and data modification attacks. Because each transaction on the blockchain is digitally signed and timestamped, the immutability of the ledger ensures that no record can be altered without detection. The hash pointers linking blockchain entries to encrypted cloud data prevent unauthorized replacement or deletion of files.

To formally validate the authentication protocol, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool was employed. The AVISPA simulations confirmed that the system maintains secrecy and authenticity under both active and passive adversary models, ensuring that legitimate entities alone can participate in the exchange of credentials. The BAN (Burrows–Abadi–Needham) logic analysis further verified that mutual authentication is achieved between the institution and the student, confirming that both parties can trust the validity of the established session keys and the integrity of exchanged data.

Performance analysis focused on computational cost, communication efficiency, and overall system responsiveness. The lightweight ECC operations required significantly fewer computational cycles compared to traditional public key mechanisms. Communication overhead was minimized by storing only minimal transaction metadata on-chain, while large datasets were maintained securely in the cloud. The evaluation demonstrated that the system achieves improved throughput and reduced delay compared with purely blockchain-based solutions, confirming its practicality for deployment in academic settings with varying technological capabilities.

Conclusion. This research introduced a blockchain-based, cloud-assisted electronic education record system designed to provide secure, efficient, and scalable management of academic data. By combining blockchain's immutability and transparency with the scalability and accessibility of cloud computing, the proposed architecture resolves key limitations of existing centralized and blockchain-only systems. Elliptic Curve Cryptography was integrated to ensure confidentiality and authentication, while formal

verification using AVISPA and BAN logic established robustness against cyber threats.

The results demonstrate that the system effectively achieves a balance between data integrity, operational efficiency, and privacy protection. Future work will focus on extending the prototype into a consortium network encompassing multiple universities and accreditation bodies. Further optimization of smart contract logic and the adoption of emerging standards such as W3C Verifiable Credentials will enhance interoperability and cross-border recognition of academic achievements. The proposed model lays the groundwork for a transparent and trustworthy educational ecosystem based on decentralized technologies.

References:

1. Hurst, W., & Shone, N. (2024). Critical infrastructure security: Cyber-threats, legacy systems and weakening segmentation. In Management and Engineering of Critical Infrastructures (pp. 265-286). Academic Press.
2. Ali, A. (2025). Advancements and Transformative Applications of Blockchain Technology. Journal of Engineering and Computational Intelligence Review, 3(1), 36-51.
3. Rao, I. S., Kiah, M. M., Hameed, M. M., & Memon, Z. A. (2024). Scalability of blockchain: a comprehensive review and future research direction. Cluster Computing, 27(5), 5547-5570.
4. Fernández-Iglesias, M. J., Delgado von Eitzen, C., & Anido-Rifón, L. (2024). Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy. Applied Sciences, 14(23), 11078.
5. Wang, Q., Kong, L., & Cui, L. (2024, May). A Complete Protection, Certification and Traceability System for Academic Degrees Based on Collaborative Storage on and Off the Chain. In 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 401-406). IEEE.
6. Cardenas-Quispe, M. A., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. Scientific Reports, 15(1), 9281.
7. Shmatko, O., Borova, T., Yevseiev, S., & Milov, O. (2021). TOKENIZATION OF EDUCATIONAL ASSETS BASED ON BLOCKCHAIN TECHNOLOGIES. Journal «ScienceRise: Pedagogical Education» №, 3, 42.