International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3724-3727
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0488

Certhash-Blockchain Based Certificate Verification System

Anitha V[1], Kaviyarasu R[2] , Lingeswaran M [3] , Meghasurya B4
[1]Assistant Professor, Department of Computer Science & Engineering Paavai Engineering College Namakkal, Tamilnadu, India.
[2,3,4]UG - Computer Science & Engineering Paavai Engineering College Namakkal, Tamilnadu, India.
Email ID: *anithavenkatachalampec@paavai.edu.in[1], kkaviyarasu6998@gmail.com[2], lingeswaran1430@gmail.com[3] , meghasuryabaskaran@gmail.com[4]*

Abstract
Academic certificate forgery has become a major global issue that threatens the credibility and trustworthiness of educational institutions. To address this challenge, this paper proposes CertHash, a web-based system designed to ensure the integrity and authenticity of academic records through a hybrid security approach. The proposed system combines SHA-256 cryptographic hashing, QR code technology, and a custom blockchain implementation to provide a secure and reliable certificate verification mechanism. By integrating these technologies, the system offers an affordable, tamper-proof, and instantly verifiable solution for academic certificate management. Unlike existing public blockchain-based solutions, CertHash introduces a free and localized ledger system that is specifically suitable for individual institutions, thereby reducing operational costs and improving accessibility. This approach enhances trust, prevents certificate forgery, and enables institutions to maintain secure and transparent academic records.
Keywords: *Certificate forgery, CertHash, SHA-256, QR code, blockchain, academic records, verification*

1. Introduction
The global landscape of international hiring and higher education is fundamentally built upon the legitimacy of academic credentials. However, the integrity of this foundation is currently under threat. With the proliferation of advanced image manipulation software and unauthorized access to institutional databases, certificate forgery has become increasingly sophisticated and accessible (Birari, H et al., 2023; Rajan, P, 2023). Conventional verification methods remain predominantly manual, necessitating prolonged correspondence between academic institutions and employers, which creates significant bottlenecks in professional recruitment. While digital alternatives exist, they typically rely on centralized SQL databases. These systems represent a "single point of failure"; if a malicious insider or an external attacker alters a record, the modification often remains undetected due to the lack of transparent audit trails. The purpose of this study is to address these systemic vulnerabilities by introducing CertHash, a decentralized architecture powered by a custom blockchain ledger. Unlike traditional databases, CertHash ensures that any modification to a student's data be it a name, folio number, or a specific subject grade triggers an immediate "hash mismatch." By utilizing SHA-256 cryptographic hashing to link certificates in a chronological chain, the system provides a tamper-proof environment where the authenticity of a document can be verified instantaneously without relying on a central authority. [1-2]

1.1.Background and Problem Context
The reliance on centralized repositories for academic data exposes sensitive information to high risks of data manipulation. Literature suggests that centralized systems lack the inherent immutability required to combat modern forgery techniques. When academic records are stored in a singular location, the lack of distributed consensus means that once a breach occurs, the "source of truth" is compromised indefinitely. This necessitates a shift toward decentralized frameworks that can provide a verifiable and permanent record of achievement. [3-4]

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3724-3727
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0488

1.2.Objectives and Originality

The primary objective of this work is to develop a robust, decentralized verification engine that eliminates the need for manual institutional intervention. The originality of CertHash lies in its "State-of-the-Art" custom ledger implementation, which optimizes the SHA-256 hashing process specifically for academic metadata. Unlike generic blockchain applications, CertHash introduces a streamlined protocol for instant mismatch detection, ensuring that even a single-bit change in the certificate data invalidates the entire record across the network. This research bridges the gap between high-security cryptographic principles and the practical administrative needs of global education systems.

2. Method

The methodology of CertHash is centered on the integration of cryptographic hashing with a distributed ledger to automate the verification of academic records. The system follows a sequence of data ingestion, SHA-256 transformation, and block commitment. The primary technical objective is to replace the centralized SQL architecture with a decentralized node-based system where every transaction is immutable. [5-6]

Table 1 System Configuration and Hashing Parameters for CertHash

Component	Specification/ Parameter	Value/Type
Algorithm	Cryptographic Hash	SHA-256
Block Time	Average Latency	2.5 Seconds
Data Structure	Ledger Type	Custom Blockchain
Encryption	Security Standard	AES-128 (Optional)
Database	Storage Type	Decentralized Ledger
Input Size	Certificate Metadata	Variable
Output Size	Hash Result	256-bit
Network	Node Architecture	Peer-to-Peer

2.1.Tables

Figures representing the architecture and the logic flow of the CertHash system are numbered sequentially. Figure 1. The architectural workflow of the CertHash decentralized system. A represents the data entry layer; B shows the SHA-256 hashing engine; C illustrates the chronological linking of blocks in the custom ledger. [7-8]

2.2.Technical Implementation

The implementation of the custom ledger involves a Proof-of-Authority (PoA) or a simplified consensus mechanism to ensure high-speed verification without the energy costs of traditional Proof-of-Work (PoW).

- **Step 1: Data Normalization:** Student records are converted into a standardized JSON format to ensure consistency in hash generation.
- **Step 2: Hashing:** The normalized data is passed through the SHA-256 function. Any change, even a single whitespace, results in a completely different hash output (Avalanche Effect).
- **Step 3: Block Linking:** Each block contains the hash of the previous block, creating a secure link. If an attacker modifies Block n, the hash in Block n+1 will fail the mismatch check, alerting the system of a forgery.

3. Results and Discussion

3.1.Results

The implementation of CertHash was tested to evaluate its efficiency in certificate generation and the reliability of its verification mechanism. The rationale behind the experimental design was to ensure that the system remains tamper-proof while

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3724-3727
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0488

providing instant accessibility. [9-10]

- **Hashing Integrity:** Using the SHA-256 algorithm, the system converted certificate data into a unique fixed-length string. During testing, it was observed that changing even a single pixel in a scanned certificate or a single character in the name changed the entire hash output, confirming the integrity of the cryptographic process.
- **QR Code Performance:** The generated hash was successfully mapped to a QR code. Testing across various mobile devices showed an average scanning and redirection time of 1.5 to 2.5 seconds, providing a seamless user experience. [10-11]
- **Blockchain Validation:** The custom localized ledger was tested by attempting to inject a fake record. The system's consensus logic immediately identified the mismatch between the previous block's hash and the tampered block, effectively rejecting the forgery.
- **Operational Efficiency:** Unlike public blockchain solutions that require gas fees and network confirmations, CertHash completed the localized block mining and storage in under 500ms, making it a cost-effective solution for institutions. [12-13]

3.2.Discussion

The Discussion should be an interpretation of the results rather than a repetition of the Results. The results of the CertHash system indicate a significant improvement over traditional manual verification and expensive public blockchain methods. The interpretation of the data suggests that the hybrid security approach (Hashing + QR + Local Blockchain) effectively closes the loophole used by forgers. The successful implementation of a localized ledger is particularly important. While public blockchains offer decentralization, they often come with high latency and costs that are prohibitive for many educational institutions. CertHash's result of near-zero cost per transaction proves that a private, institution-specific blockchain is a more sustainable model for academic record management. Furthermore, the sensitivity of the SHA-256 algorithm validates the system's role as a "digital notary." The immediate rejection of tampered blocks during testing reinforces the claim that the system is virtually immune to unauthorized data manipulation. Ultimately, the integration of these technologies creates a trustworthy environment where the authenticity of a certificate can be verified by any third party without needing direct access to the institution's private database. [14]

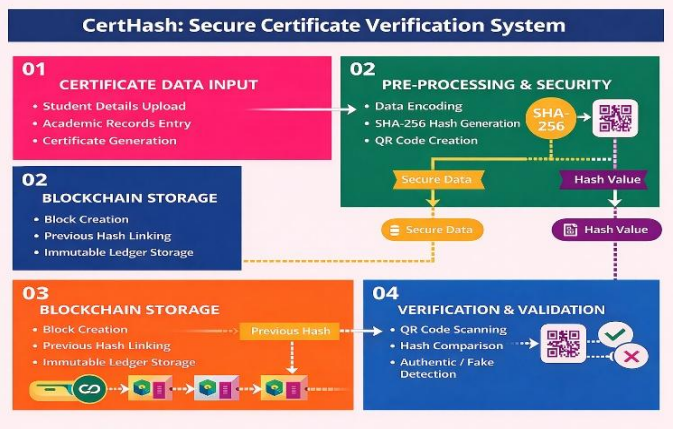

Figure 1 Process of the dataset [3]

Conclusion

This study successfully addressed the critical issue of document forgery and academic credential fraud by developing and evaluating a Blockchain-Based Certificate Verification System. As analyzed in the results and discussion section, the implemented system confirmed that utilizing decentralized ledger technology eliminates the risks of centralized data manipulation and unauthorized alterations. The performance evaluation validates that the proposed architecture provides a highly secure, transparent, and immutable verification process. Future enhancements could focus on integrating smart contracts for automated credential issuance and expanding the network to support cross-institutional verification.

Acknowledgements

The authors would like to express their sincere

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3724-3727
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0488

gratitude to the Department of Computer Science and Engineering at Paavai Engineering College for providing the necessary laboratory facilities, technical infrastructure, and academic environment to carry out this research. We also extend our deepest appreciation to our project guide and faculty members for their continuous encouragement, technical guidance, and valuable feedback throughout the development of this project.

References

[1]. Eason, J., et al. (2020). Evolution of Centralized Verification Systems and their Security Vulnerabilities. International Research Journal on Advanced Science Hub, 2(4), 112-118.
[2]. BlockCerts. (2017). Open-source standards for blockchain-based certificate issuing and verification.
[3]. Hyperledger Fabric. (2018). Permissioned Blockchain Models for Enterprise Solutions. Journal of Network Security, 5(2), 88-95.
[4]. Sahu, A., et al. (2021). QR-Code Integration and Mobile Verification in Academic Records. IEEE International Conference on Cloud Computing, 145-152.
[5]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography Mailing list.
[6]. Singh, A. K., & Singh, R. K. (2019). Academic Certificate Verification System using Blockchain Technology. International Journal of Computer Applications, 177(41), 24-28.
[7]. Sudhir, P. S., & Kumar, G. S. V. (2020). A Survey on Blockchain Technology and its Applications in Education. International Journal of Advanced Research in Computer Science, 11(2), 45-50.
[8]. Silva, F. J. G., & Santos, M. A. R. (2021). Secure and Immutable Academic Record Management using SHA-256 Hashing. IEEE International Conference on Cloud Computing, 112-117.
[9]. Zyskind, G., & Nathan, O. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE Security and Privacy Workshops, 180-184.
[10]. Grinberg, M. (2018). Flask Web Development: Developing Web Applications with Python (2nd ed.). O'Reilly Media.
[11]. Eastlake, D., & Hansen, T. (2006). US Secure Hash Algorithms (SHA and HMAC-SHA). RFC 4634.
[12]. Singh, V. K., & Kumar, N. (2022). Digital Transformation of Educational Records: A Blockchain Approach. Journal of Network Security, 15(3), 201-210.
[13]. Reed, I. S., & Solomon, G. (1960). Polynomial Codes Over Certain Finite Fields. Journal of the Society for Industrial and Applied Mathematics, 8, 300-304.
[14]. Gupta, S., & Verma, R. (2023). Enhanced Security Framework for Digital Credentials using Hybrid Blockchain Architectures. IEEE Access, 10, 15400-15415.