International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Advanced Fake Certificate Detection Using Blockchain Technology

Lenka Meghan Mahesh[1], Lohitha Kalla[2], Karri Sri Sai Kanaka Dharani Dhar[3], Kanuri Ganesh Satya Siva Ram[4], Adari Venkata Bhuvaneshwar[5]

[1,2,3,4,5]*Computer Science and Engineering Department, Raghu Engineering College, Visakhapatnam, India.*

Abstract - Due to institutional digitization efforts, digital credentials are now widely used in professional certifications and education. They increase efficiency and accessibility, but they raise issues with security and authenticity because digital tools make it simple to create fake certificates. These problems make it difficult for institutions and employers to use standard verification procedures. Current systems rely on manual reviews, institutional checks, or centralised databases, all of which are laborious, prone to errors, and susceptible to manipulation or interruptions. Many existing technologies are unable to offer verification that is safe, transparent, and impervious to tampering. This study suggests a blockchain-based method for identifying fraudulent certificates. Smart contracts store cryptographic hashes of certificates along with timestamps and issuer information. Verifiers can authenticate documents by comparing their hashes with on-chain records, administrators can manage issuer authorizations, and institutions can issue certificates using specific blockchain addresses. This framework integrates a blockchain network with a web application to support issuance and verification functionalities. Its effectiveness in detecting fraudulent certificates while preserving tamper-proof records is confirmed by empirical evaluations. In conclusion, this framework provides a strong, scalable way to reduce certificate fraud, increase confidence in digital credentials, and highlight the benefits of blockchain technology.

Key Words:
Certificate Verification, Digital Certificate Authentication, Tamper Detection, Smart Contract Security, Blockchain Technology.

1. INTRODUCTION

In recent years, the use of digital certificates has increased significantly in education, professional training, and employment sectors. Universities, online learning platforms, and certification bodies now issue certificates in digital format due to their convenience, easy storage, and quick sharing capabilities. However, this rapid digitalization has also introduced a major challenge: the rise of fake and tampered certificates. With the availability of advanced editing tools, it has become very easy to create or modify certificates, making it difficult for organizations to verify their authenticity.

Traditional certificate verification methods rely on manual processes, centralized databases, or institutional confirmation. These approaches are often time-consuming, inefficient, and prone to errors. Moreover, centralized systems are vulnerable to data manipulation, security breaches, and single points of failure. As a result, there is a growing need for a secure, transparent, and reliable system that can ensure the authenticity of digital certificates without depending on a central authority.

Blockchain technology offers a promising solution to this problem. Blockchain is a decentralized and immutable digital ledger where data, once stored, cannot be altered or deleted. This makes it highly suitable for applications that require security, transparency, and trust. By using blockchain, it is possible to store certificate information in a tamper-proof manner, ensuring that any attempt to modify a certificate can be easily detected.

The proposed project **"**Advanced Fake Certificate Detection using Blockchain Technology**"** aims to develop a secure system for issuing and verifying digital certificates. In this system, each certificate is converted into a cryptographic hash, which is then stored on the blockchain along with issuer details and timestamp. When a certificate needs to be verified, its hash is compared with the blockchain record to determine its authenticity.

The system follows a role-based approach involving three main entities: administrator, issuer, and verifier. The administrator manages issuer approvals, the issuer generates and uploads certificates, and the verifier checks the authenticity of certificates. By integrating blockchain technology with a web-based application, the proposed system ensures secure certificate storage, faster verification, and prevention of fraud.

This project not only enhances the reliability of certificate verification but also reduces the dependency on manual processes and centralized systems. It provides a scalable and efficient solution for detecting fake certificates and improving trust in digital credential systems. Unlike existing approaches, the proposed system focuses on a lightweight and practical implementation using a local blockchain environment, making it suitable for academic demonstrations and prototype-level deployments.

2. LITERATURE SURVEY

Several approaches have been proposed in recent years to address the issue of fake certificate detection and verification. Traditional systems rely on centralized databases managed by educational institutions or third-party authorities, where verification is performed manually or through controlled access. While these systems are widely used, they suffer from limitations such as lack of transparency, vulnerability to data manipulation, and dependency on a single authority. To overcome these challenges, blockchain-based solutions have been introduced, leveraging the decentralized and immutable nature of distributed ledgers to store certificate data securely. Existing blockchain-based certificate verification systems typically involve storing certificate hashes on the blockchain, allowing users to verify authenticity by comparing hashes. Some studies have also explored the use of smart contracts to automate verification processes and enhance security. However, many of these systems face challenges such as high implementation complexity, scalability issues, and dependence on public blockchain networks with associated transaction costs. Additionally, certain approaches lack practical implementation details or user-friendly interfaces for real-world usage. In contrast, the proposed system focuses on a lightweight and practical implementation using a local blockchain environment, integrating cryptographic hashing with a web-based interface to provide an efficient and accessible solution for certificate verification while maintaining security and data integrity.

3. PROPOSED SYSTEM

The proposed system presents a blockchain-based certificate verification framework designed to ensure the authenticity and integrity of academic credentials. The system consists of three main components: a Flask-based backend, a blockchain network implemented using Ganache, and a SQLite database for managing certificate-related data. During the certificate issuance process, the issuer uploads the certificate file along with a unique certificate identifier. The system generates a SHA-256 hash of the certificate, which acts as a digital fingerprint, and stores this hash securely on the blockchain to ensure immutability. Simultaneously, relevant metadata such as the certificate ID, issuer details, and issuance timestamp are stored in the local database. For verification, the user provides the certificate ID and uploads the certificate file. The system computes the hash of the uploaded certificate and compares it with the corresponding hash stored on the blockchain. If both hashes match, the certificate is considered valid; otherwise, it is flagged as tampered or invalid. This approach ensures that any modification to the certificate, even at the smallest level, results in a hash mismatch, thereby enabling effective tamper detection. The proposed system offers a secure, efficient, and user-friendly solution for certificate verification while leveraging the advantages of blockchain technology for maintaining data integrity and trust.

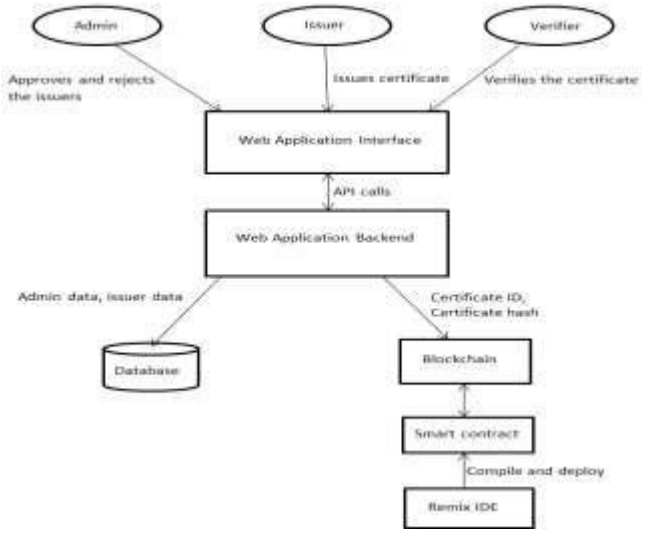

Fig -1: System Architecture

4. RESEARCH METHODOLOGY

The proposed system is implemented at a local system level to provide a practical demonstration of certificate issuance and verification using blockchain technology. A Flask-based backend is used to manage application logic, Ganache is employed as a local blockchain environment for testing smart contract interactions, and SQLite is used as a lightweight database for storing certificate metadata. This setup allows efficient development, testing, and validation of the system without requiring a live blockchain network.

4.1 Certificate Issuance

The certificate issuance process begins when the issuer uploads a certificate file along with a unique certificate identifier. The system processes the uploaded file and generates a cryptographic hash using the SHA-256 hashing algorithm. This hash acts as a unique digital fingerprint of the certificate. The generated hash is then stored on the blockchain network using a smart contract, ensuring immutability and resistance to tampering. Additionally, relevant metadata such as certificate ID, issuer details, and timestamp are stored in a SQLite database for quick access and management.

4.2 Hash Generation using SHA-256

To ensure data integrity, the system employs the SHA-256 hashing algorithm to generate a fixed-length hash value from the certificate file. SHA-256 is a widely used cryptographic hash function that produces a unique output for each distinct input. Even a minor modification in the certificate results in a completely different hash value, making it highly effective for detecting tampering.

4.3 Blockchain Storage

The generated certificate hash is stored on a blockchain network implemented using Ganache. A smart contract is used to securely record and retrieve hash values. Since blockchain provides an immutable and decentralized ledger, once the hash is stored, it cannot be altered or deleted, ensuring the authenticity and reliability of certificate data.

4.4 Certificate Verification

During the verification process, the user provides the certificate ID and uploads the certificate file. The system computes the SHA-256 hash of the uploaded file and retrieves the corresponding hash from the blockchain. Both hashes are compared to determine the authenticity of the certificate. If the hashes match, the certificate is considered valid; otherwise, it is flagged as invalid or tampered.

4.5 Tamper Detection Mechanism

The system ensures tamper detection by leveraging the properties of cryptographic hashing. Any change in the certificate content, even a single character, results in a completely different hash value. This mismatch between the generated hash and the stored hash allows the system to effectively identify forged or modified certificates.

4.6 System Integration

The entire system is integrated using a Flask-based backend that handles API requests for certificate issuance and verification. Ganache is used as a local blockchain environment for testing and development, while SQLite serves as a lightweight database for storing metadata. This integration provides a complete and functional framework for secure certificate management and verification.

5. RESULTS AND DISCUSSIONS

The developed blockchain-based certificate verification system was tested within a local setup using Flask, Ganache, and SQLite to evaluate its capability in validating certificate authenticity and identifying tampering attempts. The evaluation primarily focused on system functionality, integrity verification, and execution efficiency.

5.1 Functional Testing

The system was examined under multiple scenarios to verify its ability to correctly classify certificates as genuine or invalid. During the issuance phase, SHA-256 hashes were generated for each certificate and successfully recorded on the blockchain. In the verification phase, the system recalculated the hash of the uploaded certificate and compared it with the stored value.

Table 5.1: Test Cases

Test Case	Input Condition	Output
Test Case 1	Original certificate	Valid
Test Case 2	Modified certificate	Fake
Test Case 3	Incorrect certificate ID	Not Found

Table 5.1 shows the outputs for different test cases. The corresponding results are shown in the Fig 5.1.1, Fig 5.1.2, Fig 5.1.3. The functional testing demonstrates the reliability and accuracy of the system.

Fig 5.1.1: Test Case 1

Fig 5.1.2: Test Case 2

Fig 5.1.3: Test Case 3

5.2 Tamper Detection Analysis

To evaluate the robustness of the system, certificates were intentionally modified by altering small portions of their content. Even minor changes resulted in completely different SHA-256 hash values due to the avalanche effect of the hashing algorithm. When these modified certificates were verified, the system detected mismatches and correctly flagged them as invalid. This demonstrates the effectiveness of cryptographic hashing in maintaining data integrity.

5.3 Performance Evaluation

The performance of the system was measured based on the time required for certificate issuance and verification. The results are summarized in Table 5.3.

Table 5.3: Performance

Operation	Time Taken
Certificate issuance	1–2 seconds
Certificate verification	1 second

The results indicate that the system performs efficiently and is capable of providing near real-time verification. This makes it suitable for practical applications such as academic verification and recruitment processes.

5.4 System Reliability

The reliability of the system is strengthened by the integration of blockchain technology, which ensures immutability of stored data. Once a certificate hash is recorded, it cannot be modified or removed, thereby preventing unauthorized alterations. Additionally, the use of cryptographic hashing provides a dependable mechanism for identifying any inconsistencies in certificate content.

5.5 Discussion

The experimental findings indicate that the proposed system provides an effective and secure solution for certificate verification. The combination of blockchain and cryptographic hashing enhances transparency and ensures tamper-proof validation compared to traditional centralized approaches. The system reduces reliance on manual verification processes, thereby minimizing human error and improving operational efficiency. Although the current implementation is limited to a local blockchain environment, the results demonstrate its feasibility and potential for deployment in real-world scenarios using public blockchain networks. Furthermore, the system achieved accurate identification of valid and tampered certificates under all evaluated test conditions

6. CONCLUSION

This paper presents the design and implementation of a blockchain-based certificate verification system aimed at addressing the challenges associated with fake and tampered certificates. By utilizing the SHA-256 cryptographic hashing algorithm, the system generates a unique and secure digital fingerprint for each certificate, which is then stored on a blockchain network to ensure immutability and protection against unauthorized modifications. The integration of a Flask-based backend with Ganache as a local blockchain environment and SQLite for data management enables a complete and efficient framework for certificate issuance and verification.

The experimental evaluation confirms that the system is capable of accurately identifying authentic and tampered certificates, as even minor alterations in the certificate content result in significant hash changes. This demonstrates the effectiveness of the hashing mechanism in preserving data integrity. Furthermore, the use of blockchain enhances security and trust by eliminating the risks associated with centralized storage systems.

In conclusion, the proposed system provides a reliable, secure, and efficient solution for certificate authentication. It significantly reduces the dependency on manual verification processes and ensures a higher

level of transparency and trust. Although the current implementation is limited to a local environment, it successfully demonstrates the practicality and effectiveness of blockchain-based verification systems and lays the groundwork for future enhancements and real-world deployment.

7. FUTURE ENHANCEMENTS

Although the proposed blockchain-based certificate verification system demonstrates effective detection of fake and tampered certificates, there are several opportunities for further enhancement and real-world deployment. One of the key improvements would be the integration of a public blockchain network instead of a local blockchain environment, enabling global accessibility and decentralized verification across multiple organizations. Additionally, the system can be extended by incorporating decentralized storage solutions such as IPFS to store certificate files securely, while maintaining only the hash on the blockchain for improved scalability.

Another potential enhancement is the implementation of QR code-based verification, allowing users to quickly verify certificates through mobile devices. The system can also be improved by introducing user authentication and role-based access control to support multiple issuers and verifiers in a secure manner. Furthermore, performance optimization techniques can be applied to handle large-scale certificate data and improve system efficiency.

Future work may also explore the integration of advanced technologies such as machine learning for detecting suspicious patterns in certificate data and enhancing fraud detection capabilities. Overall, these enhancements can transform the proposed system into a fully scalable, secure, and user-friendly platform suitable for real-world academic and professional applications.

REFERENCES

1. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications. Telematics and Informatics, 36, 55–81.
2. Grech, A., & Camilleri, A. F. (2017). Blockchain in education. Publications Office of the European Union.
3. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and cryptocurrency technologies. Princeton University Press.
4. MIT Media Lab. (2016). Bloc`kcerts: An open infrastructure for academic credentials on the blockchain.
5. Turkanovic, M., Hölbl, M., Kosic, K., Hericko, M., & Kamisalic, A. (2018). EduCTX: A blockchain-based higher education credit platform. IEEE Access, 6, 5112–5127.
6. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352–375.
7. Sharples, M., & Domingue, J. (2016). The blockchain and kudos: A distributed system for educational record, reputation and reward. In Proceedings of the European Conference on Technology Enhanced Learning.
8. Buterin, V. (2014). A next-generation smart contract and decentralized application platform.
9. G Hari Hara Kumar, J Swapna, M Sirisha, K Siva Gowthami, B Srinivas Kumar, Detection of Fake Certificate using Blockchain Technology, International Journal for Modern Trends in Science and Technology, 2024, 10(09), pages. 137-144. https://doi.org/10.46501/IJMTST100902
10. Lutfiani , N., Apriani , D., Nabila , A.E, Sari , A.A, Febrianto , K.R, Decentralization Of Information Using Blockchain Technology On Mobile Apps E-Journal Blockchain Frontier Technology *(B-Front)*, *1*(2), 55-64. DOI: https://journal.pandawan.id/b-front/article/view/37