Block chain Based Fake Certificate Detection Using Quantum Computing

Vajrapu Bala Murali[1], Mrs.M.Revati[2], Mr.P.Mareswara Rao[3], Mr.Ch.Raja Jacob[4]

[1]PG student ,Department Of Computer Science & Engineering, Mother Teresa Institute Of Science And Technology Autonomous, Sanketika Nagar, Kothuru (V), Sathupally - 507303, Khammam Dist., Telangana,India

[2,3,4]Assistant Professor , Department Of Computer Science & Engineering, Mother Teresa Institute Of Science And Technology Autonomous, Sanketika Nagar, Kothuru (V), Sathupally - 507303, Khammam Dist., Telangana,India

***Abstract*—**The rapid growth of digital education, online certifications, and remote recruitment has increased the risk of fake certificate generation and misuse across academic and professional sectors. Traditional certificate verification methods rely on manual validation processes, centralized databases, or machine learning approaches that often struggle with scalability, data tampering, privacy concerns, and cyberattacks. To address these issues, the proposed project titled "Blockchain Based Fake Certificate Detection Using Quantum Computing" introduces an advanced framework that combines blockchain technology with quantum computing algorithms for secure, transparent, and intelligent certificate verification. The proposed system aims to create a decentralized and tamper-proof environment where certificates are securely stored, verified, and monitored in real time.

This project is highly beneficial in educational institutions, multinational companies, government recruitment agencies, and online learning platforms where certificate authenticity is critical. The integration of blockchain and quantum computing represents a next-generation solution capable of addressing current and future challenges in digital certificate security. Overall, the proposed system enhances trust, reliability, efficiency, and security in certificate verification processes while reducing fraud and administrative complexity.

I. INTRODUCTION

In the modern digital era, academic and professional certificates are essential documents used for employment, higher education admissions, scholarships, and professional licensing. With the widespread availability of editing tools and digital forgery techniques, fake certificates have become a serious issue across the world. Many individuals create forged educational credentials to secure jobs, promotions, or admissions illegally. This growing problem negatively affects organizations, educational institutions, and society by reducing trust in digital documentation systems. Traditional certificate verification methods are time-consuming, expensive, and vulnerable to

Doi:10.48047/ijiee.2026.16.2.54

tampering because they depend mainly on centralized databases or manual validation procedures.

Machine learning-based certificate verification systems have been introduced to automate fraud detection. These systems analyze patterns, signatures, fonts, QR codes, and metadata to determine certificate authenticity. Although machine learning provides better automation compared to manual systems, it still faces limitations such as data manipulation attacks, model bias, insufficient scalability, and reduced efficiency when processing extremely large datasets. Additionally, centralized storage systems used in many machine learning frameworks are vulnerable to cyberattacks, unauthorized access, and database corruption.

Blockchain technology emerged as a revolutionary solution for secure and decentralized data management. Blockchain maintains records in distributed blocks connected using cryptographic hashes. Once data is stored in a blockchain, it cannot be modified without network consensus, making it highly secure and tamper-resistant. Educational certificates stored in blockchain networks become immutable and easily verifiable by authorized users. Blockchain also increases transparency because every transaction is permanently recorded and traceable.

Along with blockchain, quantum computing is becoming a transformative technology capable of solving complex computational problems faster than classical computers. Quantum computing uses quantum bits, superposition, and entanglement to process massive datasets simultaneously. In certificate verification systems, quantum algorithms can improve fraud detection speed, optimize verification accuracy, and strengthen cryptographic security mechanisms. Quantum-assisted blockchain systems can efficiently detect anomalies and unauthorized modifications in certificates while supporting scalable verification processes.

II. LITERATURE SURVEY

1. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification

Authors: Avni Rustemi, Fisnik Dalipi, Vladimir Atanasovski, Aleksandar Risteski

- **Technique Used:** Blockchain-based certificate issuance, verification, and tamper-proof storage.
- **Pros:**
  - Eliminates certificate forgery.
  - Provides transparent verification.
  - Reduces manual validation efforts.
- **Cons:**
  - Scalability issues in large deployments.
  - Dependence on blockchain infrastructure.

Doi:10.48047/ijiee.2026.16.2.54

2. Blockchain-Based Academic Certificate Fraud Detection: A Comparative Review and Combined Framework

Authors: Priti Golar, Tanushri Kalaskar, Jennifer Joseph, Mayuri Atkar, Sakshi Bute

- **Technique Used:** Blockchain, QR Codes, IPFS, Machine Learning, and Deep Learning for certificate verification.
- **Pros:**
  - Detects forged certificates effectively.
  - Immutable certificate storage.
  - Supports automated verification.
- **Cons:**
  - Higher implementation complexity.
  - Storage overhead for large datasets.

3. Towards Blockchain-Based Auditable Storage and Sharing of Data

Authors: Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, Simon Duquennoy

- **Technique Used:** Blockchain-based immutable storage and auditing mechanisms.
- **Pros:**
  - Ensures integrity of records.
  - Provides traceability and transparency.
  - Prevents unauthorized modifications.
- **Cons:**
  - Increased transaction latency.
  - Resource-intensive blockchain operations.

4. Post-Quantum Distributed Ledger Technology: A Systematic Survey

Authors: Nikhil Kumar Parida, Chandrashekar Jatoth, V. Dinesh Reddy, Md. Muzakkir Hussain, Jamilurahman Faizi

- **Technique Used:** Post-Quantum Cryptography (PQC) integrated with Blockchain and Distributed Ledger Technology.
- **Pros:**
  - Resistant to future quantum attacks.
  - Enhances blockchain security.
  - Supports long-term certificate authenticity.
- **Cons:**
  - Larger key sizes.
  - Increased computational overhead.

5. A Survey on Lattice-Based Digital Signature

Authors: Fengxia Liu, Zhiyong Zheng, Zixian Gong, Kun Tian, Yi Zhang, Zhe Hu, Jia Li

- **Technique Used:** Lattice-based digital signatures for post-quantum authentication.
- **Pros:**
  - Strong resistance to quantum attacks.
  - Suitable for secure certificate signing.

Doi:10.48047/ijiee.2026.16.2.54

  - NIST-recognized post-quantum approach.
- **Cons:**
  - Larger signature sizes.
  - Complex implementation.

III. EXISTING SYSTEM

Existing fake certificate detection systems mainly rely on machine learning techniques and centralized databases for certificate verification. These systems use algorithms such as Support Vector Machines, Random Forest, Decision Trees, Neural Networks, and Convolutional Neural Networks to identify forged certificates based on visual features, metadata, QR codes, signatures, and text patterns. Machine learning models are trained using datasets containing genuine and fake certificates to classify suspicious documents automatically.

In many existing systems, certificates are stored in centralized servers managed by institutions or verification agencies. When verification requests are received, machine learning algorithms compare uploaded certificates with stored records and detect inconsistencies. Optical Character Recognition techniques are also used to extract text from certificates for pattern analysis. Deep learning models analyze logos, signatures, watermarks, and layout structures to determine authenticity.

Disadvantages

Existing fake certificate detection systems based on machine learning and centralized databases suffer from several technical and operational disadvantages. One of the major limitations is centralized data storage. Since certificate information is stored in a single database or server, attackers can target the central repository to modify, delete, or manipulate records. This creates serious cybersecurity risks and reduces trust in verification systems.

Another major disadvantage is limited transparency. Most existing systems depend on institutional authorities for certificate verification. Users cannot independently validate certificates without contacting the issuing organization. This increases processing time and creates administrative burdens for institutions. Manual intervention in verification workflows also increases operational costs and delays recruitment or admission processes.

IV. PROPOSED SYSTEM

The proposed system combines blockchain technology and quantum computing algorithms to create a highly secure and intelligent fake certificate detection framework. The system is designed to overcome the limitations of traditional machine learning and centralized verification systems by introducing decentralization, transparency, high-speed processing, and advanced fraud detection capabilities.

In the proposed framework, educational institutions issue digital certificates that are converted into cryptographic hash values using secure hashing algorithms. These hash values are stored inside blockchain blocks connected through distributed ledgers. Blockchain ensures immutability, meaning certificates cannot be altered once they are registered. Every transaction is validated by

Doi:10.48047/ijiee.2026.16.2.54

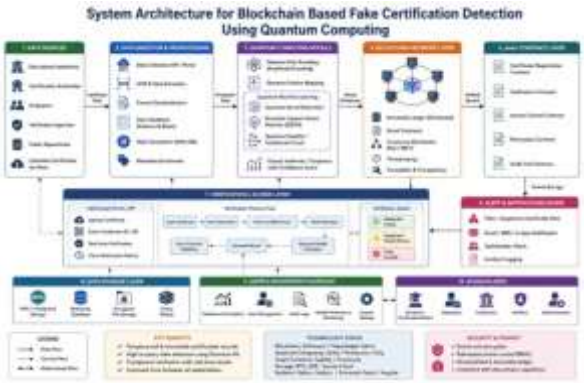
blockchain nodes through consensus mechanisms, preventing unauthorized modifications and improving trust among participants.

Advantages

The proposed blockchain and quantum computing-based fake certificate detection system provides several advantages over traditional machine learning and centralized verification frameworks. One of the major advantages is enhanced security. Blockchain technology ensures that certificate records are immutable and tamper-proof. Once certificates are stored in the blockchain ledger, attackers cannot modify or delete them without network consensus. This significantly reduces the risk of certificate forgery and unauthorized data manipulation.

Another important advantage is decentralization. Unlike centralized systems that depend on a single server or authority, the proposed framework distributes certificate data across multiple blockchain nodes. This removes single points of failure and increases system reliability. Even if one node is compromised, the remaining nodes maintain the integrity of the network.

V. SYSTEM ARCHITECTURE



The architecture combines multiple advanced technologies including blockchain networks, quantum cryptographic security, decentralized storage, certificate validation engines, artificial intelligence modules, and user authentication systems. Blockchain ensures that certificate records are immutable and transparent, while quantum computing introduces high-speed processing and advanced security mechanisms capable of resisting future cyberattacks. The integration of these technologies creates a powerful platform capable of detecting forged certificates in real time while maintaining data privacy and institutional trust.

VI. RESULTS AND OUTCOMES

Screen 1: Home page

Screen 2: Login Page

Doi:10.48047/ijiee.2026.16.2.54

Screen 3: Admin Page

VII. CONCLUSION

The proposed blockchain-based fake certificate detection system using quantum computing presents an advanced and secure approach for verifying academic, professional, and organizational certificates in the digital era. Traditional certificate verification methods often suffer from problems such as manual validation delays, document forgery, centralized database vulnerabilities, and lack of transparency. By integrating blockchain technology with quantum computing concepts, the system creates a highly secure, decentralized, and tamper-resistant framework for certificate authentication. Blockchain ensures that certificate records are permanently stored in distributed ledgers where unauthorized modifications become nearly impossible. Each certificate is assigned a unique cryptographic hash and timestamp, enabling institutions, employers, and government agencies to verify authenticity quickly and accurately.

The incorporation of quantum computing further strengthens the proposed model by improving computational efficiency and enhancing cryptographic operations. Quantum algorithms can process large-scale verification tasks much faster than classical systems, making the framework suitable for handling millions of certificates across educational institutions and industries. Quantum-based encryption mechanisms also provide stronger security against advanced cyberattacks and fraudulent activities. The combination of blockchain immutability and quantum-enabled security forms a reliable ecosystem for digital certificate management.

VIII. BIBLIOGRAPHY

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[2] M. Swan, Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O’Reilly Media, 2015.

[3] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT: Challenges and opportunities,” Future Generation Computer Systems, vol. 88, pp. 173–190, Nov. 2018.

[4] K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the Internet of Things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.

[5] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Blockchain technology: Beyond bitcoin,” Applied Innovation Review, vol. 2, no. 6, pp. 6–19, 2016.

[6] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction

Doi:10.48047/ijiee.2026.16.2.54

Ledger," Ethereum Project Yellow Paper, 2014.

[7] V. Buterin, "A next-generation smart contract and decentralized application platform," Ethereum White Paper, 2014.

[8] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124–134.

[9] L. K. Grover, "A fast quantum mechanical algorithm for database search," in Proc. 28th Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 1996, pp. 212–219.

[10] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge, U.K.: Cambridge Univ. Press, 2010.

Doi:10.48047/ijiee.2026.16.2.54