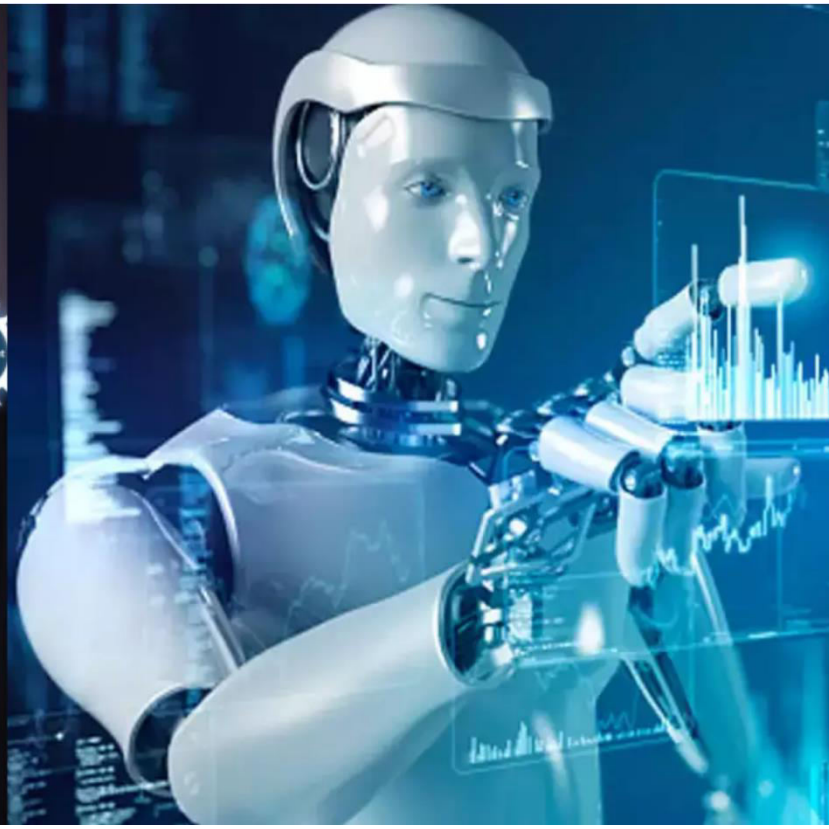
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411031|

Blockchain for Academic Integrity and Credential Verification

Pooja V. Kale[1], Prof. Sachin Bhosale[2], Dr. Anand Khatri[3], Dr. Shubhangi Gunjal[4]

Student, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India[1]

Professor, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India[2]

Professor & HOD, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India[3]

Professor, Department of Computer Engineering, Jaihind College of Engineering, Pune, Maharashtra, India[4]

ABSTRACT: The proposed e-certificate generation and verification system leverages blockchain technology to address the recurring problem of document falsification within India's education sector. The model makes digital credential management safe, transparent, and verifiable by utilizing blockchain's decentralized and immutable features. Each certificate is represented by a cryptographic hash and recorded on a distributed ledger, ensuring that any alteration attempt is immediately detectable. Authorized users can verify certificates instantly through a QR code or verification ID accessible via web or mobile platforms. The framework simplifies validation for employers and academic organizations while reducing the likelihood of fraud, data loss, and unauthorized modification. To promote trust and widespread adoption of this digital credential ecosystem, collaboration between educational institutions, government agencies, and technology partners is essential for its successful implementation.

KEYWORDS: Blockchain, E-Certificate Generation, Digital Verification, Fog Computing, Security, Decentralization

I. INTRODUCTION

Blockchain technology offers a distributed, immutable, and decentralized solution for secure data storage and validation. Unlike traditional centralized systems, blockchain maintains synchronized copies of a ledger across multiple nodes, eliminating the need for a single authority and reducing the risks of data tampering, manipulation, or cyberattacks. Its features of transparency, accountability, and traceability make it suitable for sensitive domains such as finance, voting systems, supply chain management, and digital identity verification.

In the domain of educational certification, blockchain empowers individuals to manage and verify credentials without reliance on intermediaries. Rather than storing raw data, only hashed or encrypted records are saved on the blockchain, ensuring privacy and user ownership of information. This makes blockchain a robust foundation for secure and verifiable e-certificates, where data integrity and authenticity are critical.

Traditionally, E-Certificate Generation Systems depend on manual or centralized processes for record creation and validation. Such systems are prone to security threats like SQL injection, collusion, and brute-force attacks, making them unreliable for large-scale deployments. A blockchain-based decentralized framework mitigates these risks by enabling trustless, peer-validated transactions that prevent tampering and ensure persistent data availability.

Additionally, Fog Computing—often called fog networking or fogging—extends cloud computing by positioning computation and storage resources closer to the network edge. This paradigm reduces latency, enhances responsiveness, and distributes control across localized fog nodes. These nodes act as intermediate servers, supporting real-time processing and decision-making near end users. Integrating fog computing with blockchain technology further improves the scalability and efficiency of decentralized e-certificate systems by enabling hierarchical and virtualized architectures optimized for high performance and reliability.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411031|

II. SURVEY OF EXISTING WORK (LITERATURE SURVEY)

Braccescu *et al.* [1] proposed a blockchain-based digital identity framework that emphasizes data privacy, integrity, and interoperability. By employing Decentralized Identifiers (DIDs) and verifiable credentials, their system minimizes dependence on third-party providers and introduces role-based access control through smart contracts, ensuring secure identity validation.

De Salve *et al.* [2] developed a multi-layer trust model for Self-Sovereign Identity (SSI) systems. Their layered approach—covering issuer, verifier, and credential trust—assigns dynamic trust scores using smart contracts, enhancing the overall reliability and scalability of decentralized identity management frameworks.

Peng *et al.* [3] presented a consortium blockchain-based peer-to-peer file storage system. The approach restricts access to authenticated participants, integrates identity management, and leverages smart contracts for automated permission control. Their model improves data integrity and performance compared to public blockchain networks.

Alexandru-Cristian *et al.* [4] analyzed the potential of blockchain to revolutionize digital identity ecosystems. Their study highlights the limitations of centralized providers and recommends blockchain-driven solutions using smart contracts and DIDs for GDPR-compliant, privacy-preserving identity systems.

Xu and Guo *et al.* [5] proposed a hybrid identity authentication model combining fog computing and private blockchain for smart homes. Their architecture provides low-latency authentication and resists spoofing and replay attacks, outperforming traditional cloud-based systems in speed and security.

Elisa *et al.* [6] introduced an identity and access management framework for e-government platforms using blockchain and Artificial Immune System (AIS) algorithms. The blockchain ensures transparency and immutability, while AIS detects anomalies in real-time, safeguarding against unauthorized access and improving trust in digital governance.

Venkatraman and Parvin [7] explored blockchain's role in IoT identity management, where each device maintains a unique blockchain-registered identity. Smart contracts automate registration, authentication, and access control, eliminating central points of failure and enhancing system scalability.

Thorve *et al.* [8] proposed a smart contract-based decentralized identity management system using Ethereum. Their model supports selective disclosure and interoperability, reducing risks of identity theft and enabling user-centric identity control for both mobile and web environments.

Maldonado-Ruiz *et al.* [9] presented a decentralized identity framework that enables users to manage identities independently, using smart contracts for validation and lifecycle management. Their prototype demonstrates tamper-resistant and auditable performance suited for finance and healthcare sectors.

Stockburger *et al.* [10] investigated the use of Self-Sovereign Identity (SSI) in public transportation systems, providing users with complete control over digital credentials. The system employs verifiable credentials and DIDs, improving efficiency, privacy, and regulatory compliance in real-world identity verification scenarios.

III. METHODOLOGY

The proposed system introduces a blockchain-based decentralized architecture for e-certificate generation and verification. The workflow is divided into four modules:

- **Student Module:** Students upload academic details via a secure web portal. Instead of submitting physical documents, they receive a QR code or certificate ID that serves as a unique digital identifier.
- **Academic Institution Module:**

Educational institutions (schools, colleges, or universities) act as verifying authorities. Upon validation, certificate metadata is recorded on the blockchain, and a unique hash is generated. This ensures immutability and prevents unauthorized alterations.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411031|

- **Organization Module:** Employers or third-party entities can verify certificates by scanning the QR code or entering the certificate ID. Smart contracts on the blockchain validate the request, ensuring authenticity and tamper-proof
- **Blockchain Layer:** The distributed ledger stores all verified records and manages decentralized access rights using cryptographic mechanisms. The blockchain infrastructure ensures data consistency, traceability, and resilience against malicious tampering or unauthorized access.

IV. SYSTEM ARCHITECTURE

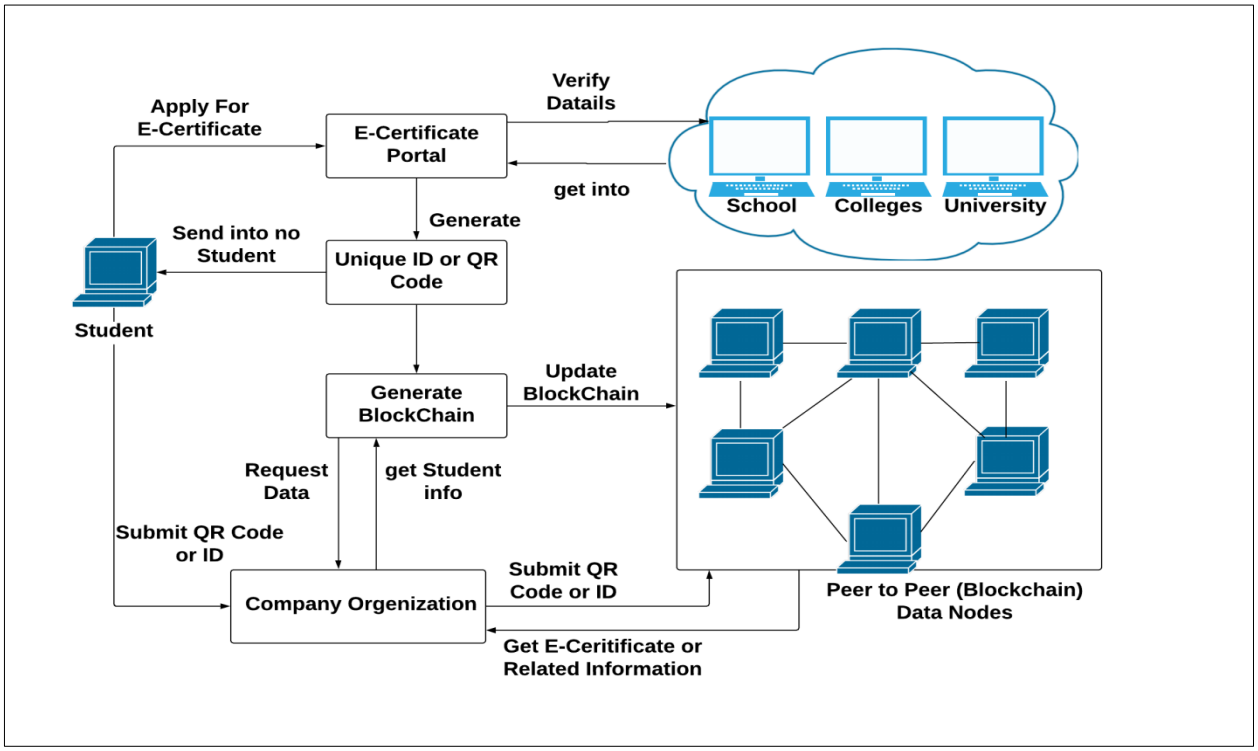


Figure 1:System architecture

V. FUTURE SCOPE

- Educational system to generate online certificate in secure manner.
- Any kind organization system where to save historical data into secure database.
- Secure database systems and approaches

VI. CONCLUSION

The integration of blockchain technology into the academic certification process provides a secure, transparent, and reliable mechanism for managing digital credentials. By decentralizing control, the system eliminates dependence on intermediaries and ensures tamper-proof record storage. The proposed model enhances trust, interoperability, and efficiency while safeguarding against common cyber threats. In combination with fog computing, this framework supports real-time validation and scalability, paving the way for next-generation digital certification systems that are both secure and accessible.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 11, November 2025

|DOI: 10.15680/IJIRSET.2025.1411031|

REFERENCES

1. Alaidaros, H., Mahmuddin, M., Al Mazari, A., et al. AdStop : Efficient flow-based mobile adware detection using machine learning. Computers & Security, Vol. 117, 2022.
2. Seraja, S., Pavlidis, M., Trovat, M., & Polatidis, N. MadDroid: Malicious Adware Detection in Android using Deep Learning. Journal of Cyber Security Technology, 2023.
3. Park, J., & Jung, S. Android Adware Detection using Soot and CFG. J. Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, Vol. 13, No. 4, Dec 2022.
4. Reddy, K. S. U., Chakkaravarthy, S. S., Gopinath, M., & Mitra, A. A Study on Android Malware Detection Using Machine Learning Algorithms. ICISML 2022 (Publ. in 2023).
5. Cybersecurity SpringerOpen. Android Malware Category Detection using a Novel Feature Vector-based Machine Learning Model. 2023.
6. FSSDroid: Feature Subset Selection for Android Malware Detection. World Wide Web, 2024.
7. Hybrid Android Malware Detection and Classification Using Deep Neural Networks. Int. J. of Computational Intelligence Systems, 2025 (recent large-scale static features + APIs + intents).
8. Wang, T., Xu, Y., Zhao, X., et al. Android malware detection via efficient API call sequences extraction and machine learning classifiers. IET Software, 2023.
9. A system call-based Android malware detection approach with homogeneous & heterogeneous ensemble machine learning. Computers & Security, 2023.
10. Muzaffar, A., Hassen, H. R., Zantout, H., & Lones, M. DroidDissector: A Static and Dynamic Analysis Tool for Android Malware Detection. 2023.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details