IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

# A Decentralized Approach to Certificate Authentication and Issuer Trust Using Blockchain

**Dr.B.Ranjitha**
Assistant Professor, Department of CSE
Guru Nanak Institute of Technology,
Hyderabad, Telangana, India
https://orcid.org/0009-0000-6299-7991
**Sayini Varshini, Kondapuram Sharadha, Nagelly Srujana Reddy, Ramavanth Akshitha**
Students, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, Telangana, India

**Publication History**
Manuscript Reference No: IJIRIS/RS/Vol.12/Issue04/ISAP26.ISAP10081
Research Article | Open Access | Double-Blind Peer-Reviewed| ArticleID: IJIRAE/RS/Vol.12/Issue04/ISAP26.ISAP10081
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijiris.com/volumes/Vol12/iss-04/02.ISAP26.ISAP10081.pdf
**Article Citation:Dr.Ranjitha,Sayini,Kondapuram,Nagelly,Ramavanth(2026)**,A Decentralized Approach to Certificate Authentication and Issuer Trust Using Blockchain, IJIRIS: International Journal of Innovative Research in Information Security,Volume 12, Issue 04 of 2026 pages 264-271 **Doi:>** https://doi.org/10.26562/ijiris.2026.v1204.02
**BibTeX Key: Dr.Ranjitha@2026Decentralized**
IJIRIS papers should be cited as IJIRIS (International Journal of Innovative Research in Information Security, AM Publications, India 2026, ISSN 2349-7017, https://doi.org/10.26562/ijiris.2026.v1204.02 The journal's official abbreviation is IJIRIS. Orcid: https://orcid.org/0009-0004-9398-7488



**Abstract:** Verifying the authenticity of educational certificates is a critical challenge in modern recruitment and academic validation processes. Traditional systems rely on manual verification and centralized databases, which are prone to delays, inefficiencies, and data tampering. This paper proposes a decentralized blockchain based system for certificate authentication and issuer trust validation. The system utilizes Ethereum blockchain technology to store certificate hashes, ensuring immutability and security. Smart contracts automate certificate issuance and verification, reducing human intervention. A hash-based search mechanism improves lookup efficiency, enabling faster verification. Experimental analysis demonstrates that the proposed system is secure, efficient, and cost-effective, providing a reliable solution for digital certificate management.

**Keywords:** Blockchain, Certificate Authentication, Smart Contracts, SHA-256, Bloom Filter, Decentralization, DataSecurity

## I. INTRODUCTION

In the modern digital era, academic certificates play a crucial role in validating an individual's educational qualifications and professional eligibility. These certificates are widely used during recruitment, higher education admissions, and professional verifications. However, traditional certificate verification systems are largely manual, time-consuming, and inefficient. Organizations often rely on physical document verification or communication with issuing institutions, which leads to delays and increased operational costs. With the rapid advancement of digital technologies, the problem of forged and fake certificates has increased significantly. Fraudulent documents can be easily created using editing tools, making it difficult for employers and institutions to verify their authenticity. Centralized database systems, which are commonly used for storing certificate data, are also vulnerable to cyberattacks, data tampering, and single points of failure. These limitations highlight the need for a secure, transparent, and efficient verification system. Blockchain technology has emerged as a promising solution to address these challenges. It is a decentralized and distributed ledger system that ensures data immutability, transparency, and security. Once data is recorded on the blockchain, it cannot be altered or deleted, making it highly reliable for storing sensitive information such as certificates. By leveraging cryptographic hashing techniques like SHA-256, each certificate can be converted into a unique digital fingerprint, ensuring its authenticity and integrity. In this proposed system, blockchain is used to store certificate hashes instead of actual documents, enhancing security and reducing storage requirements. Smart contracts are implemented to automate the processes of certificate issuance, validation, and verification without the need for intermediaries. Furthermore, the decentralized nature of the system ensures that no single authority has complete control, thereby increasing trust among stakeholders such as students, institutions, and employers. The system also improves transparency by maintaining a permanent and verifiable record of all transactions. Overall, the proposed blockchain-based certificate authentication system provides a secure, efficient, and scalable solution to overcome the limitations of traditional verification methods, ensuring trust and reliability in academic and professional environments.

## II. LITERATURE SURVEY

Priyadarshini et al. (2025)[1] proposed an integrated blockchain-based system for certificate authentication and issuer validation.

The system utilizes smart contracts and Bloom Filter-based hash mapping to enable fast certificate lookup and automated validation, while incorporating a decentralized voting mechanism to approve trusted issuers, resulting in improved security, reduced gas consumption, and enhanced verification efficiency compared to traditional centralized approaches. Said et al. (2025) developed a comprehensive block chain-based framework (ElimuChain) for managing and verifying educational credentials. The system leverages decentralized storage using IPFS and smart contracts for automated issuance and validation, achieving high data integrity, transparency, and fault tolerance, while significantly reducing verification time[2]. Ifeyemi et al. (2024) introduced a blockchain-based digital certificate verification framework to address fraud in academic systems. The model employs cryptographic hashing and smart contracts on Ethereum to store immutable certificate records, enabling instant verification and reducing dependency on intermediaries, thereby improving security, scalability, and cost efficiency over traditional verification methods[3].

Gangwar et al. (2024) proposed a blockchain-enabled certificate verification system integrated with QR code technology. The approach uses decentralized applications and cryptographic hashing to verify certificates through QR-based retrieval of blockchain data, ensuring instant authentication, reduced administrative overhead, and enhanced transparency compared to manual verification processes[4]. Kumar et al. (2023) designed a blockchain-based certificate authentication system using smart contracts to automate issuance and validation. The system stores hashed credentials on a decentralized ledger, enabling fast and tamper-proof verification while eliminating third-party dependency, resulting in improved trust, reduced delays, and enhanced operational efficiency[5]. Huang et al. (2023) investigated an improved consensus mechanism for blockchain in IoT environments. The proposed hybrid DPoSPBFT model incorporates a credit-based node evaluation system and dynamic grouping to enhance reliability and efficiency, achieving high success rates, reduced latency, and improved scalability under heavy workloads compared to traditional consensus algorithms[6]. Chandana et al. (2022) proposed a blockchain-based academic certificate verification system to eliminate forgery and inefficiencies. The system utilizes cryptographic hashing, smart contracts, and decentralized storage to enable real-time verification, ensuring data immutability, reduced administrative effort, and improved trust among stakeholders[7]. Ghosh et al. (2021) explored a decentralized blockchain framework for secure academic record verification. The system employs smart contracts and cryptographic techniques to ensure data integrity and transparency, while integrating off-chain storage for scalability, resulting in faster processing, enhanced security, and improved collaboration across institutions[8].

## III. EXISTING SYSTEM

The existing certificate verification system primarily relies on centralized databases and manual validation processes. Institutions store certificate records in isolated systems, requiring verification through emails, phone calls, or physical document checks. This approach leads to significant delays and increased administrative workload. Moreover, centralized storage makes the system vulnerable to data tampering, unauthorized access, and single points of failure. The absence of a unified verification platform further complicates the process, especially when dealing with multiple institutions. Additionally, the growing availability of digital editing tools has increased the risk of forged certificates, making verification more challenging. Traditional systems also lack transparency, as users cannot independently verify certificate authenticity. The dependency on intermediaries increases operational costs and reduces efficiency. Overall, the existing system is inefficient, insecure, and not scalable for modern digital requirements [9,10].

### A. Disadvantages of Existing Systems

- Time-consuming verification process.
- High dependency on manual effort.
- Risk of data tampering and fraud.
- Lack of transparency and scalability.
- Inefficient for large-scale data handling.

### B. Proposed System:

The proposed system introduces a decentralized blockchain-based approach for secure certificate authentication and issuer trust validation. Instead of storing complete certificates, the system generates a unique cryptographic hash (using SHA-256) for each certificate and stores it on the blockchain, ensuring immutability and security. Smart contracts are used to automate certificate issuance, validation, and verification processes, eliminating the need for intermediaries[11,12]. The decentralized architecture ensures that no single authority has complete control, enhancing transparency and reliability. Users can verify certificates in real-time by comparing hash values, significantly reducing verification time from days to seconds. Additionally, the system prevents certificate forgery by ensuring that any modification in the document changes its hash value. The integration of blockchain also improves data integrity and traceability. Overall, the proposed system provides a secure, efficient, and scalable solution compared to traditional verification methods.

### C. Advantages of the Proposed System:

- Ensures high data security and integrity using blockchain technology.
- Prevents certificate forgery through unique SHA-256 hash generation.
- Enables real-time and instant certificate verification.
- Provides a decentralized and transparent system without a single authority.
- Reduces operational cost and minimizes manual human effort.
- Improves traceability and builds trust with a permanent audit trail.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 04, April 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

## IV. SYSTEM ARCHITECTURE

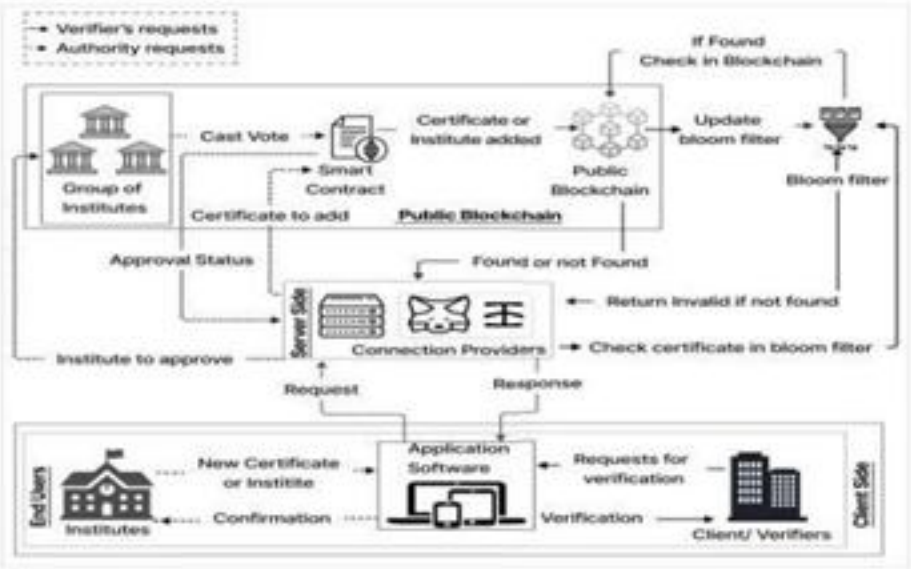



**Fig: 1.1** System architecture

1. Institution & Validation Layer:A consortium of institutions validates new institutions through voting using smart contracts. Based on votes, institutions are approved or rejected.
2. Smart Contract & Blockchain Layer: Approved institutions store certificate hashes on the blockchain via smart contracts.This ensures immutability, security, and transparency of certificate data[13].
3. Bloom Filter Optimization Layer: Certificate hashes are added to a Bloom Filter for fast lookup. It quickly checks existence before performing blockchain verification.
4. Server & Connection Layer: Acts as a bridge between application and blockchain network. Processes requests and returns verification results to users.
5. Application Layer (Frontend):Handles certificate upload, verification requests, and displays results.
6. Client/User Layer: Includes institutions and verifiers who use the system. Users receive outputs like valid, invalid, or tampered certificates.

### Methodology:

Algorithm: Certificate Authentication using SHA-256 and Blockchain
Step 1.The issuing authority uploads the certificate data (C) along with issuer credentials to the system.
Step 2.Thesystem verifies the issuer identity using authentication mechanisms and rejects unauthorized issuers.
Step 3.The system generates a SHA-256 hash value h(C) for the certificate.
Step 4. The generated hash h(C) along with certificate metadata (ID, issuer, timestamp) is sent to the blockchain smart contract.
Step 5.Thesmart contract records (h(C), certificate ID, issuer details, timestamp) immutablyon the blockchain.
Step 6.The actual certificate document C is stored off-chain (local storage/IPFS), and a reference link r is maintained.
Step 7.The user (verifier/employer) submits the certificate or certificate ID for verification.
Step 8.The system generates a new hash h(C') from the submitted certificate.
Step 9.The blockchain is queried via smart contract to retrieve the original stored hash h(C).
Step 10.The system compares h(C') with h(C) to check authenticity.
Step 11. If both hashes match, the certificate is marked as Valid; otherwise, it is marked as Invalid/Tampered.
Step 12.The verification result along with issuer details and timestamp is displayed to the user..

### Module Names:

- User Registration Module
- Certificate Issuance Module
- Blockchain Storage Module
- Off-Chain Storage Module
- Verification Module
- Smart Contract Module
- Authentication and Authorization Module
- Result Display Module

1. User Registration Module: This module allows users (students, issuers, and verifiers) to register and create accounts in the system. It ensures secure authentication and role-based access control.
2. Certificate Issuance Module: In this module, authorized institutions upload certificate details and generate certificates. A unique SHA-256 hash is created and stored on the blockchain for security.

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 04, April 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

3. Blockchain Storage Module: This module handles storing certificate hash values and metadata on the blockchain using smart contracts. It ensures immutability, transparency, and tamper-proof data storage[14].
4. Off-Chain Storage Module:The actual certificate files are stored outside the blockchain (e.g., local storage or IPFS). Only the hash and reference link are maintained on-chain to optimize storage.
5. Verification Module: This module allows users to verify certificates by uploading documents or entering certificate IDs. It compares hash values to determine authenticity.
6. Smart Contract Module: Smart contracts automate the processes of certificate issuance, storage, and verification. They enforce rules and ensure secure and trust less interactions.
7. Authentication and Authorization Module: This module verifies user identities and ensures only authorized entities can issue or verify certificates. It enhances system security and prevents unauthorized access.
8. Result Display Module: This module displays the verification results to the user, including certificate status (valid/invalid), issuer details, and timestamp for transparency.

## IMPLEMENTATION

In the existing system, certificate verification was carried out using traditional manual and centralized approaches. These methods relied on direct communication with institutions through emails, phone calls, or physical document checks. While this approach provided a basic mechanism for validation, it suffered from several limitations such as delays, lack of transparency, and vulnerability to data tampering. The absence of a secure and unified system made it difficult to ensure the authenticity of certificates, especially in large-scale scenarios. To overcome these challenges, we introduced a more advanced approach using blockchain technology for certificate authentication and verification. Blockchain provides a decentralized and tamper-proof environment where certificate data can be securely stored. Each certificate is converted into a unique cryptographic hash using SHA-256, ensuring that even the smallest modification in the data results in a completely different hash value. This guarantees the integrity and authenticity of certificates. In our implementation, blockchain is used as the core component for storing certificate hashes in a distributed ledger. Smart contracts are integrated to automate the processes of certificate issuance, validation, and verification. Additionally, Bloom Filter techniques are applied to improve the efficiency of searching and verifying certificates within the system. The combination of blockchain, cryptographic hashing, and smart contracts allows the system to overcome the limitations of the existing approach. It ensures secure storage, real-time verification, and improved transparency. The system is capable of handling large volumes of certificate data efficiently while preventing fraud and unauthorized modifications. By using these advanced technologies, the proposed system significantly enhances the performance and reliability of certificate verification. It reduces verification time from days to seconds and provides a trustworthy platform for institutions, students, and employers. This approach not only improves system efficiency but also ensures a secure and scalable solution for future applications.

### Algorithm Used:

Existing Algorithm: Manual Verification Process:
The existing system follows a manual verification approach where certificate details are checked through institutional records. This process involves human intervention and communication with issuing authorities, making it time-consuming and inefficient. It also lacks automation and is prone to errors and fraud[15].
Proposed Algorithm: Blockchain with SHA-256

### Smart Contracts:

The proposed system uses blockchain technology combined with SHA-256 hashing for secure certificate authentication. Each certificate is converted into a hash and stored on the blockchain. During verification, the hash of the input certificate is compared with the stored hash. Smart contracts automate the verification process, ensuring fast and accurate results.

## EXPERIMENTAL RESULTS

The proposed blockchain-based certificate authentication system was deployed on an Apache Tomcat server backed by a MySQL database for managing user and certificate data. Blockchain[16,17] functionality is implemented using SHA-256 hashing and smart contracts, with certificate files stored off-chain. The following screens illustrate the key system's interfaces.

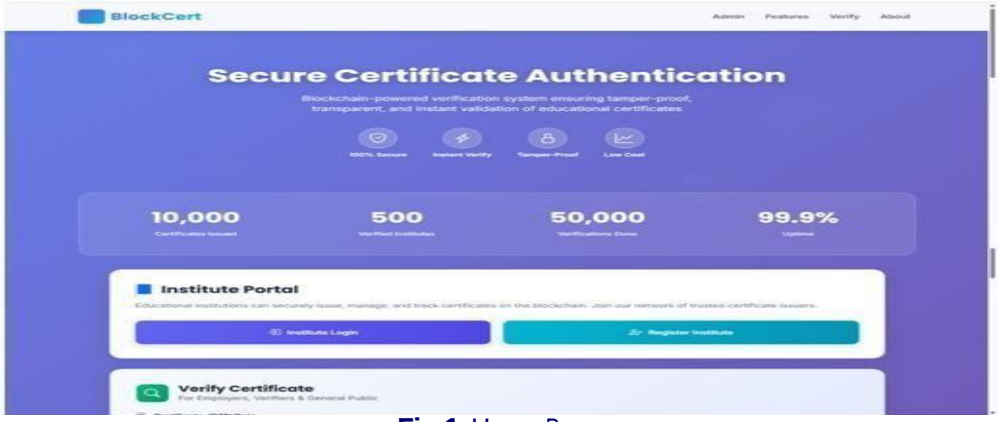



**Fig-1:** Home Page:

IJIRIS: International Journal of Innovative Research in Information Security
Volume 12, Issue 04, April 2026
E-ISSN: 2349-7017
P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

This snapshot represents the main landing page of the BlockCert system, which is designed to provide a secure and efficient solution for certificate authentication using blockchain technology.

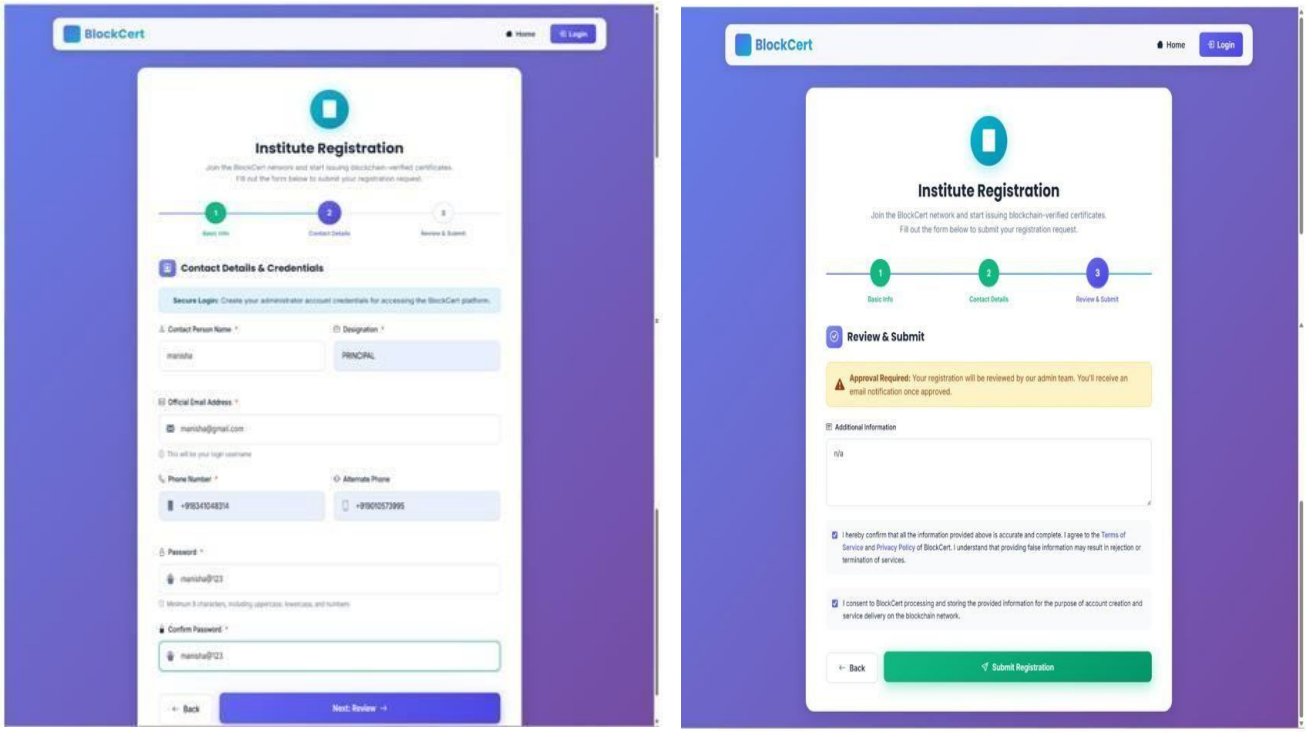



**Fig-2:** Registration Page:

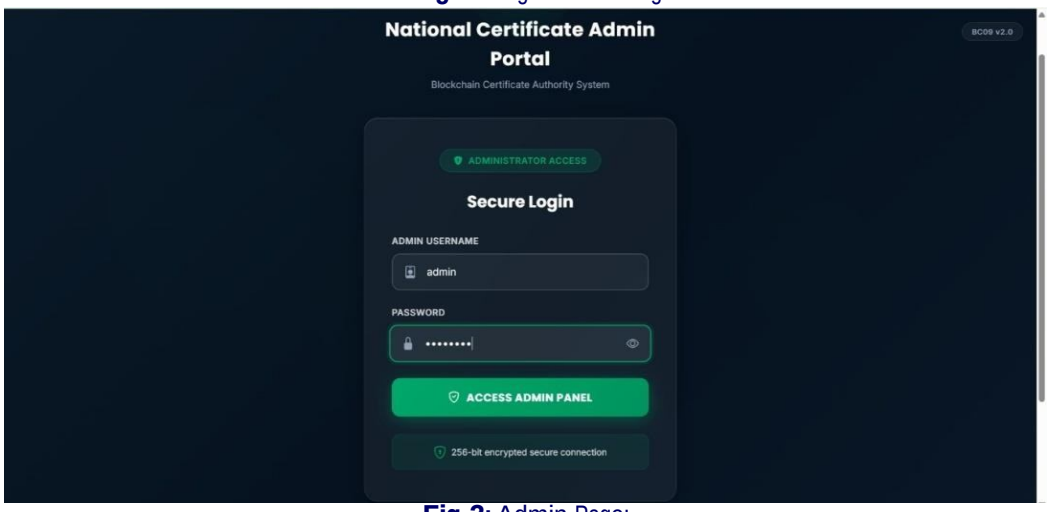



**Fig-3:** Admin Page:

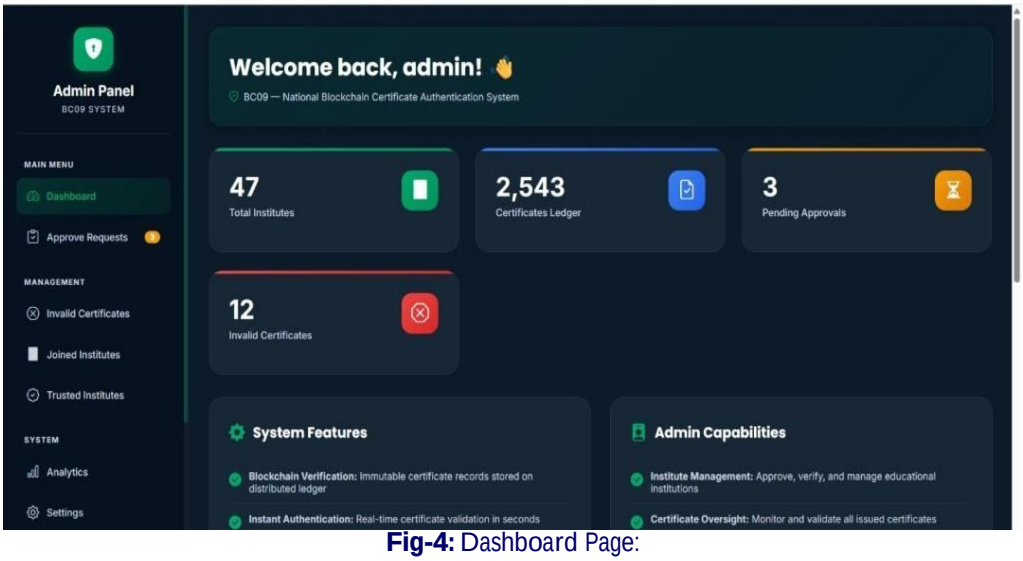



**Fig-4:** Dashboard Page:

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 04, April 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

Provides It shows a step-by-step process starting with Basic Information. Users need to fill details to join the blockchain certificate system. It includes fields like institute type, year established, address, and website. This displays the Contact Details & Credentials form. It includes fields like name, email, phone number, and password creation. Users must provide login credentials for accessing the platform. The admin page displays all issued certificates along with their hash values, issuer details, and timestamps for monitoring and management. It also allows the admin to verify records, track activities, and ensure the integrity of stored certificate data. The dashboard page provides an overview of system activities, including total certificates issued, verified, and pending requests. It offers quick navigation to key modules and displays real-time statistics for efficient system monitoring.

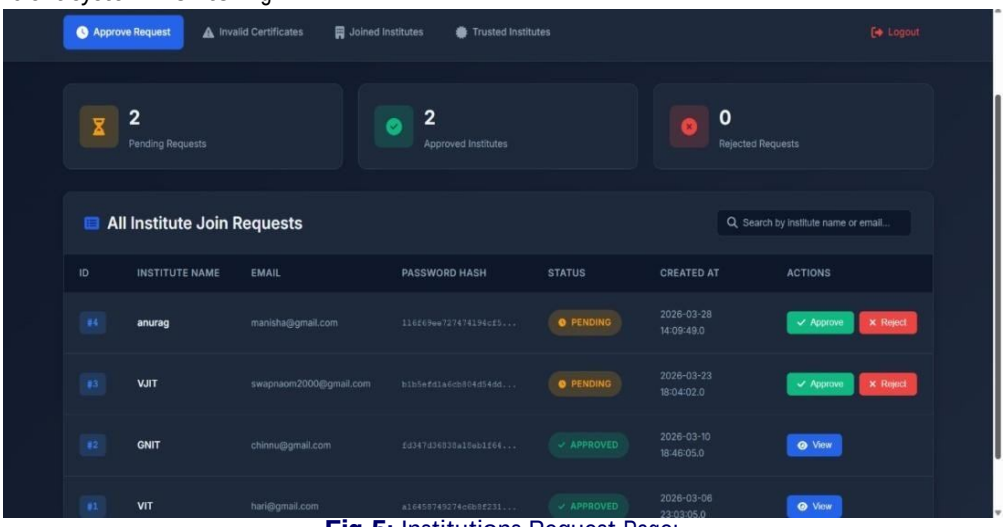



**Fig-5:** Institutions Request Page:

The institute request page enables institutions to submit requests for certificate issuance or registration within the system. It allows admin verification of institution details to ensure only authorized entities can issue certificates.

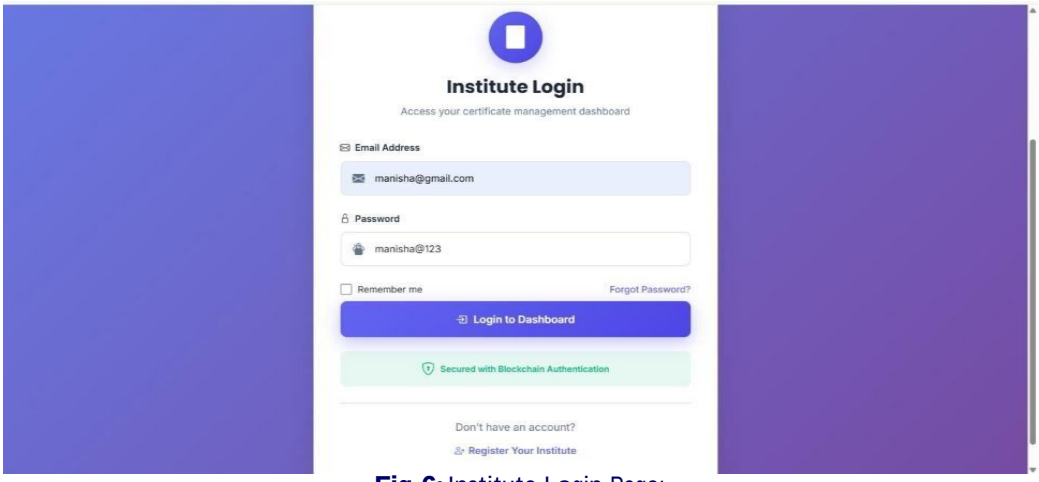



**Fig-6:** Institute Login Page:

The institute login page allows authorized institutions to securely access the system using their credentials. It ensures authentication and restricts access to certificate issuance and management features.

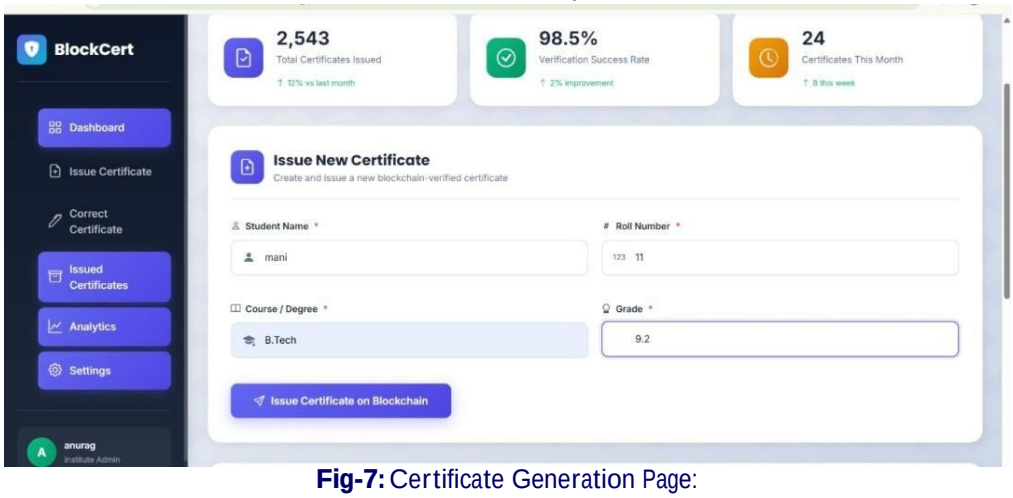



**Fig-7:** Certificate Generation Page:

IJIRIS: International Journal of Innovative Research in Information Security E-ISSN: 2349-7017
Volume 12, Issue 04, April 2026 P-ISSN: 2349-7009
https://www.ijiris.com/archives
https://doi.org/10.26562/ijiris.2026.v1204.02

The certificate issue page allows authorized institutions to generate and upload new certificates for students. It creates a unique SHA-256 hash and stores it on the blockchain for secure and tamper-proof verification.

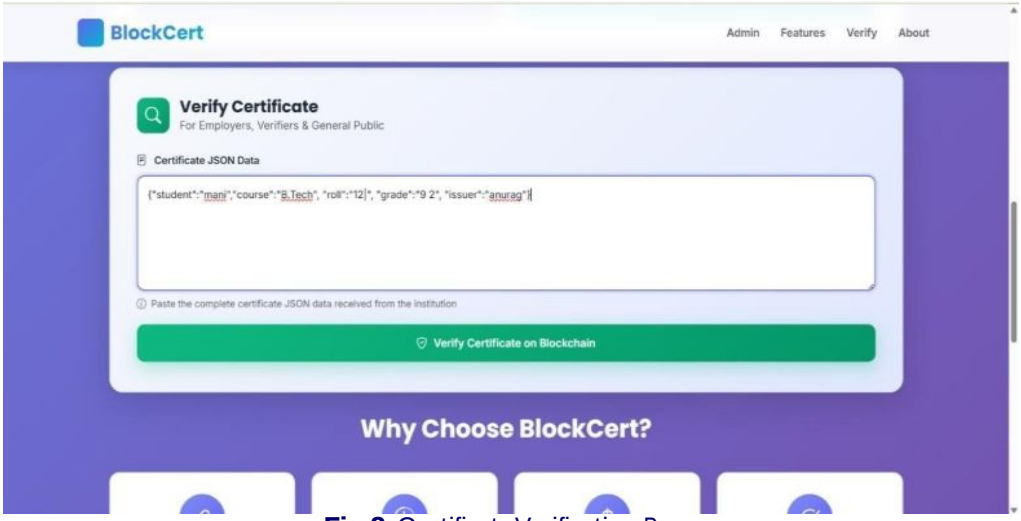
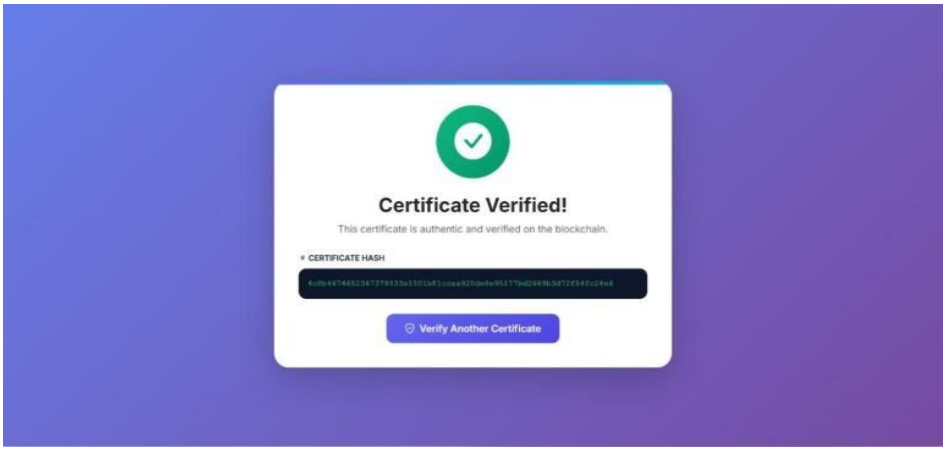



**Fig-8:** Certificate Verification Page:

The certificate authentication page allows users or verifiers to upload a certificate or enter a certificate ID for validation. It compares the generated hash with the blockchain-stored hash to determine whether the certificate is valid or tampered.



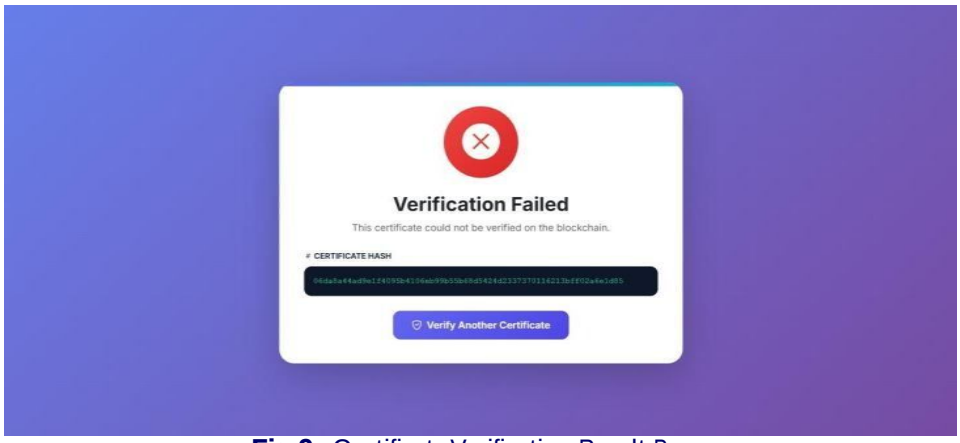




**Fig-9:** Certificate Verification Result Page:

The certificate result page displays the outcome of the verification process, indicating whether the certificate is valid or invalid. It also shows details such as issuer information, timestamp, and authentication status for user reference.

## CONCLUSION

The proposed blockchain-based certificate verification system provides a secure, transparent, and efficient solution for validating institutions and authenticating certificates. By integrating a public blockchain with smart contracts, the system ensures that only verified institutions can issue certificates, thereby preventing fraudulent activities. Once certificate data is stored on the blockchain, it becomes immutable and tamper-proof, guaranteeing document authenticity and integrity. The use of cryptographic hash functions enhances data security, while the integration of a Bloom Filter significantly improves search efficiency during the verification process.

The decentralized validation mechanism eliminates dependence on a single authority and promotes trust among participants. Overall, the system offers a reliable and scalable framework for digital certificate management, ensuring transparency, faster verification, and enhanced data protection.

## FUTURE ENHANCEMENT

The proposed system can be enhanced by integrating real blockchain networks to improve security and enable practical real-world deployment. It can be extended to support multi-institution and global collaboration, allowing universal certificate verification across different universities and organizations. A mobile application can be developed to provide easy access and efficient certificate management for users. Additionally, QR code-based verification can be implemented to enable quick and user-friendly authentication of certificates. Integration with government and recruitment systems can further allow automatic verification during job applications and admissions processes. The system can also incorporate AI-based fraud detection techniques to identify fake or suspicious certificates more effectively. Furthermore, advanced security mechanisms such as multi-factor authentication and stronger encryption can be added to enhance overall system protection and data privacy.

## REFERENCES

1. A.Osseiran et al., "The foundation of the mobile and wireless communications system for 2020 and beyond: Challenges, enablers and technology solutions," in Proc. IEEE Veh. Technol. Conf., 2013, pp. 1–5.
2. Z.Xuetal.,"Age-awaredataselectionandaggregatorplacementfortimely federated continual learning in mobile edge computing," IEEE Trans. Comput., vol. 73, no. 2, pp. 466–480, Feb. 2024.
3. R.Bhardwaj et al., "Ekya: Continuous learning of video analytics models on edge compute servers," in Proc. 19th USENIX Symp.Netw. Syst. Des. Implementation, 2022, pp. 119–135.
4. X.Hou and S.Dey, "Motion prediction and pre-rendering at the edge to enable ultra-low latency mobile 6DoF experiences," IEEE Open J. Commun. Soc., vol. 1, pp. 1674–1690, 2020.
5. F. Nawab, D.Agrawal, and A. El Abbadi, "DPaxos: Managing data closer to users for low-latency and mobile applications," in Proc. Int. Conf. Manage. Data, 2018, pp. 1221– 1236.
6. Amazon, "AWS wavelength for media & entertainment," 2021. [On line].
7. Z. Xu, Y. Fu, Q. Xia, and H. Li, "Enabling age-aware Big Data analytics in serverless edge clouds," in Proc. IEEE Conf. Comput.
8. Commun., 2023, pp. 1–10.
9. E.Schurman and J. Brutlag, "The user and business impact of server delays, additional bytes, and HTTP chunking in web search," Velocity Web Perform. Operations Conf., Oreilly, 2009.
10. S.C.Lin et al., "The architectural implications of autonomous driving: Constraints and acceleration," in Proc. 23rd Int. Conf. Architectural Support Program. Lang. Operating Syst., 2018, pp. 751–766.
11. S.Ma, S.Guo, K. Wang, W. Jia, and M. Guo, "A cyclic game for service-oriented resource allocation in edge computing," IEEE Trans .Serv .Comput., vol. 13, no. 4, pp. 723–734, Jul./Aug. 2020.
12. Z.Xu et al., "Collaborate or separate? distributed service caching in mobile edge clouds," in Proc. IEEE Conf. Comput. Commun., 2020, pp. 2066–2075.
13. Y.Mao,C.You,J.Zhang,K.Huang, and K.B.Letaief, "A survey on mobile edge computing: The communication perspective,"IEEE Commun. Surveys Tuts., vol. 19, no. 4, pp. 2322–2358, Fourth Quarter 2017.
14. X.Xia,F.Chen, Q.He, J. Grundy, M. Abdelrazek, and H. Jin, "Online collaborative data caching in edge computing," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 2, pp. 281– 294, Feb. 2021.
15. J.Zhou, F.Chen, Q.He, X.Xia, R.Wang, and Y. Xiang, "Data caching optimization with fairness in mobile edge computing," IEEE Trans. Serv. Comput., vol. 16, no. 3, pp. 1750–1762, May/Jun. 2023.
16. Tripathy, R., Satyanarayana Murty, P.T., Maram, B., Garg, A., Daniya, T., Santhosh Kumar, B. (2025). IoT-Based Secure Healthcare Framework Using Blockchain Technology with Nature-Inspired Optimization Algorithms. In: Stroe, DI., Nasimuddin, Laskar, S.H., Pandey, S.K. (eds) Emerging Electronics and Automation. E2A 2023. Lecture Notes in Electrical Engineering, vol 1202. Springer, Singapore. https://doi.org/10.1007/978-981-97-3090-2_23.
17. P.Chinnasamy,R.K.Ayyasamy,V.Tiwari,S.Dhanasekaran,B.S.Kumar,T.Sivaprakasam,"Blockchain Enabled Privacy-Preserved Supply-Chain Management for Tracing the Food Goods," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India,2024, pp. 1-5, https://doi.org/10.1109/ICSTEM61137.2024.10560589
18. P.Chokkamreddy, A.Palagati, A.L.P.Rao, P.Maheswari,V.Mahadevan,S.K.Balan,"Utilizing Blockchain Technology for Financial Services in Parallel, Distributed, and Grid Computing Frameworks," 2024 International Conference on Computing and Intelligent Reality Technologies (ICCIRT), Coimbatore, India, 2024, pp. 1-6, https://doi.org/10.1109/ICCIRT59484.2024.10922035