IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

SecureCert: A Blockchain-Based Decentralized Framework for Tamper-Proof Academic Certificate Verification and Management

Basamma Halli[1], Ganesh G A[2], K Vishnu[3], Keerthana Nagendra[4], Prof. Pavithra N[5]

Student, Information Science and Engineering, Bangalore Institute of Technology, Bangalore, India[1]

Student, Information Science and Engineering, Bangalore Institute of Technology, Bangalore, India[2]

Student, Information Science and Engineering, Bangalore Institute of Technology, Bangalore, India[3]

Student, Information Science and Engineering, Bangalore Institute of Technology, Bangalore, India[4]

Assistant Professor, Department of Information Science and Engineering,

Bangalore Institute of Technology, Bengaluru, India[5]

Abstract: The rise in fake diplomas causes big problems for schools, companies, and groups that check credentials. Because old-school checks rely on central record systems and hand reviews, they tend to be sluggish, costly, while opening doors to tampering. Instead of sticking with those outdated methods, this study introduces SecureCert - a system that issues and confirms certificates across a decentralized network using Ethereum's blockchain, file hosting via IPFS, data protection through SHA-256 encryption, identity checks with scannable QR tags, along with an automated tool made in Python. The system lets schools make PDF certificates, then calculate digital fingerprints - after that, they're sent to IPFS while info gets locked into Ethereum via smart contracts. To check validity, users scan a QR code or type in an ID, which pulls data from the chain and confirms the IPFS hash along the way.

Keywords: Blockchain, Ethereum, SecureCert, Academic Certificate Verification, Decentralized Systems, IPFS, Smart Contracts, SHA-256 Encryption, QR Code Verification, Tamper Proof Records, Digital Credentials

I. INTRODUCTION

Certificates have a substantial effect on demonstrating an individual's education, training, and accomplishments. They are commonly needed for jobs, admissions, internships and most types of official verifications. And because they are valuable, people sometimes abuse them, by editing and copying or even entirely making up certificates. This has the effect of making it more difficult for organizations to trust the documents they receive.

In much of the country, checking a certificate is based on antiquated methods. One person could send out an email to the college, also be making phone calls and turning to files that potentially had not been kept up to date. These procedures take time, involve more than a single person and do not always provide clarity. And when the stored data is altered or the physical archive vanishes. These problems sparked SecureCert's creation. It uses simple coding tools like Python and HTML to generate credentials for its system, while boosting safety through SHA-256 encryption. Once ready, the document gets stored on IPFS spread across many nodes instead of sitting in just one spot. Details about every credential are locked into the Ethereum blockchain, where they can't be changed without notice. A scannable QR code sits on each issued paper, letting people verify validity fast using any smartphone.

Cutting out manual oversight while reducing ties to central servers, SecureCert uses blockchain-sent info so you can check credentials safely. That way, any changes to the document get caught right away. Or grab a digital pass to save and send it online to businesses whenever needed

1.2 NEED FOR THE SYSTEM

The exiting certificate management mechanism has a few shortcomings. Here are some of the more frequent complaints: Fake certificates are increasingly 'common It still requires manual verification and decisioning is delayed. Centralized data is hackable, deletable and editable. Paper certificates may be lost, destroyed or replaced There's no quick, easy way to verify if a pdf is the original source. Those are the reasons why schools and enterprises need a moderately reliable system that no one can tamper with it. Blockchain and IPFS were made for that. When a certificate is uploaded and recorded, it's kept safe and can't be quietly altered. SecureCert is a new way to verify. Verification is simple with scan, check and confirm.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15152

OBJECTIVES

SecureCert is designed to:

- Generate certificates using Python and HTML
- Create a SHA-256 hash for each certificate
- Save files on IPFS
- Record certificate info on the Ethereum blockchain
- Add QR codes for instant verification
- Provide an admin panel to issue certificates
- Give students a place to access their certificates
- Offer a simple page for employers to verify them

These points together form a complete digital certificate system.

II. PURPOSE OF THE STUDY

The main intention of this project is to build a certificate system that is simple to create, safe to store, and effortless to verify. Institutions should be able to generate certificates with minimal steps, students should have a reliable digital copy, and verifiers should get results instantly without contacting the issuer.

To make this workflow possible, the system combines several technologies:

- Python + HTML for creating the actual certificate
- SHA-256 hashing to ensure that any change is noticeable
- IPFS to store files in a decentralized network
- Ethereum to keep certificate details secure and unalterable
- QR codes to make verification quick and user-friendly

The study aims to produce a complete solution were issuing and validating certificates becomes smooth, fast, and secure.

III. SCOPE OF THE PROJECT

While this system is mainly designed for academic certificates, the same approach can be used for any organization that issues important documents. Training institutes, private companies, and government agencies can use this model to ensure their certificates or records are genuine.

The project includes:

- Generating certificates
- Storing files in a decentralized manner
- Using blockchain to confirm authenticity
- QR code–based validation
- User-friendly web portals

As the system grows, it can support multiple institutions, mobile verification apps, and integrations with digital identity platforms.

APPLICATION

The Blockchain Certificate System works in many fields especially were safe, unchangeable, proof-ready records matter. Not just schools - it fits any place that checks credentials or confirms data. Main uses cover: Educational Institutions: Schools or colleges might use blockchain to send out diplomas, so they’re real and don’t need checking by hand. Training spots plus universities could do the same thing keeps things honest without extra paperwork.

Recruitment & HR Departments:

Workers' qualifications get checked fast - no need to call schools or offices, which speeds up job offers while cutting down on fake resumes.

Government & Public Sector Agencies: Departments responsible for issuing licenses, permits, or identification documents can store verification data securely on the blockchain to prevent fraud.

Professional Certification Bodies: Orgs offering certs - like IT classes, medical drills, legal workshops, or trade skills - can make sure their proof of completion checks out globally.

Online Learning Platforms (EdTech): Services such as Coursera or Udemy - along with public online learning tools - gain trust when they hand out digital credentials stored on open networks. These records can't be faked, making them solid proof of achievement.

Research & Academic Archives: Filing school papers for years keeps them safer, so they won’t get lost or ruined later - using digital copies helps protect them better over the years.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

Cross-Institutional Verification: Campuses might team up to keep joint records when students move between schools, apply from abroad, or need credits checked - using links instead of repeating work.
International Student Migration: Students going overseas might send digital records through blockchain so colleges there check them fast - no paperwork needed at all.
Skill-Based Industry Certifications: Sectors like IT or healthcare - also aviation, plus manufacturing use blockchain to check if skill certs are real.
Corporate Training & Employee Upskilling: Workers who join company classes might get digital proofs on a secure network system. These records show what each person learned or completed during work hours.
Freelancers & Gig Economy Professionals: Checked online credentials let freelancers show what they can do, while gaining client confidence across countries. University Admissions & Credit Transfer:
Colleges check student records right away when they apply. Moving credits from one school to another works smoothly, cutting down on wait times or arguments about who qualifies.
Alumni Credential Management: Ex-learners might misplace paper diplomas as days go by. With blockchain storage, grads can access or send proof of achievements whenever needed - no matter how much time has passed.
Scholarship & Fellowship Verification: Groups that give out scholarships check student records fast, so only eligible candidates get the money - these cuts down on lies and keeps things fair. While some might try to fake their way in, quick checks stop them early, making sure aid goes where it's needed most.
Background Verification Companies: Outside checkers get straight access to locked school records, so things move faster while cutting out slow paper checks. Judicial & Legal Evidence Validation:
Academic or work certificates used in court show up clear, so fake papers don't sway rulings.
Defense & Security Services: Military groups check training proofs from new members using secure methods, so they meet tough entry rules. Security teams verify school records through reliable systems, making sure applicants fit tight skill requirements.
Healthcare Workforce Credentialing: Hospitals or medical boards check a doctor's, nurse's, or tech's skills right away - cutting down danger from false papers.

IV. PROPOSED METHOD

A. Dataset

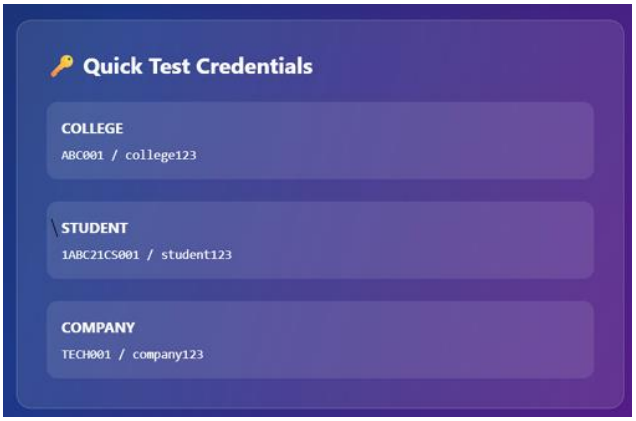

Fig. 1 Sample images from Dataset

A new idea uses blockchain to handle school certificates online in a safe way - this setup works without central control. It creates records, keeps them stored securely, while letting people check their validity anytime. This method brings clear tracking plus stops fake documents before they become an issue. No more slow paperwork checks since everything runs automatically.

Key Features of the Proposed System:

- Blockchain-Based Storage

Certificates live on the blockchain as digital fingerprints - once saved, no one can change them, remove them, or fake them.

- Web-Based Certificate Generation

A Institutions set up certs fast using a simple dashboard, then upload learner info while kicking off one-of-a-kind cert entries.

- Instant Certificate Verification

Workers or outside folks type a code or hash into the site to check if it's real - no need to call the place that gave it out.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

The system shows results right away using live data instead of old files.

Decentralized Architecture

The way blockchain spreads data means no need to depend on one group or machine - so things get safer, clearer, also more reliable.

- Tamper-Proof Data Integrity

A single cert hash goes onto the chain - then it can't change, no matter what. Tampering? Impossible. Fake copies get stopped fast. The record stays locked in place by design.

- Secure Access and Authentication

Just approved admins have permission to hand out certificates, so access stays limited while stopping abuse.

B. Proposed Architecture

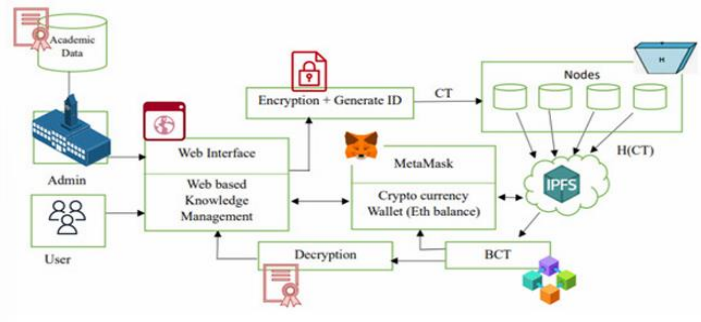

Fig. 2 Workflow Diagram

The new SecureCert setup uses separate layers that work together - centralized controls meet distributed checks. Its aim? Keep things safe, clear, and hard to alter without making it tough to use. Schools, learners, or hiring teams can still get going fast.

The setup's made up of six main parts,

1.User Interface Layer
2.Application Layer
3.Certificate Processing Module
4.Blockchain Layer
5.IPFS Storage Layer
6.Database & Audit Layer

Every part runs on its own yet shares info using safe connections1. User Interface

The way people see the app sits on top of the tech behind it. Built with HTML, styled through CSS, while Flask handles how pages come together.

The setup gives unique logins depending on who's using it,

- College/Admin Portal
- Kept track of student sign-ups, added cert details, also handed out the actual certs.
- Student Portal
- Let's kids sign in, see their certs, then grab a legit PDF copy whenever they want.
- Company/Verifier Portal
- Letting bosses check certs through USN, or maybe a hash, even scan a QR code.
- Public Verification Page
- Anyone can check a cert using its QR code or hash – no sign-in needed.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

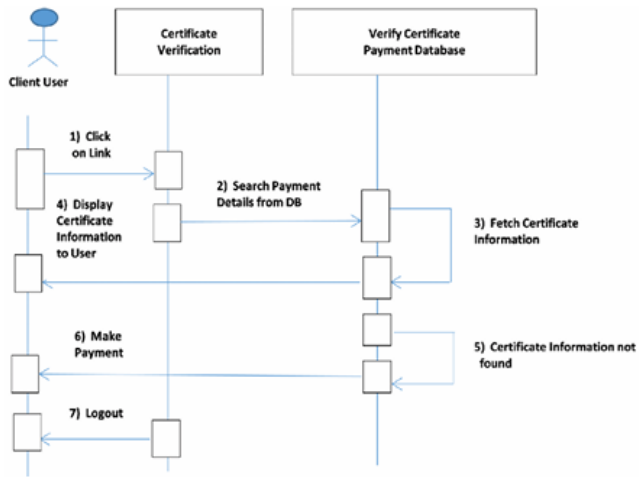

Fig. 3 Workflow of the Verification Certificate System

2. Authentication and Access Control Service

The Authentication Service checks login details while handling permission levels based on roles. Once logged in successfully, people get entry solely to features allowed by their position - like student, college, or business - depending on setup rules.

This part stops anyone without permission from getting in, while making sure only approved schools can get certificates. Every time someone tries to enter gets saved in a log so it's traceable.

3. Certificate Generation and Hashing Module

This part handles certificates right before they're stored.

Key operations include:

- Generating certificate PDFs using Python and HTML templates
- Finding the SHA-257 value for every cert file by checking one after another
- Creating a QR code that points to the check-up site

The SHA-256 hash works like a digital signature. A tiny change in the file leads to a totally new hash, so any meddling shows up right away.

4. Blockchain Layer (Ethereum Network)

The blockchain level acts as the reliable core of SecureCert's setup.

A code snippet living on Ethereum's network holds:

- Certificate ID
- SHA-256 fingerprint from the cert
- IPFS Content Identifier (CID)
- Issuer (college) details
- Timestamp of issuance

After saving, the info can't change. If someone tries altering the cert, the system blocks it - keeps things secure without fail.

5. Decentralized Storage System (IPFS)

Certificate PDFs live on IPFS - no central server needed - so they're spread across a network. Instead of one place holding everything, it's shared from many spots at once. certificate.

C. System Design

The setup of SecureCert lays out how parts connect, move data, along with work together in a blockchain tool for checking certificates. It's built to stay safe, grow smoothly, fit different needs, also make checks quick. Every piece works on its own but still links up effortlessly with the rest.

The setup uses separate parts - each one deals with certificates on its own, like making them, keeping them safe, checking validity, or managing who can see what.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

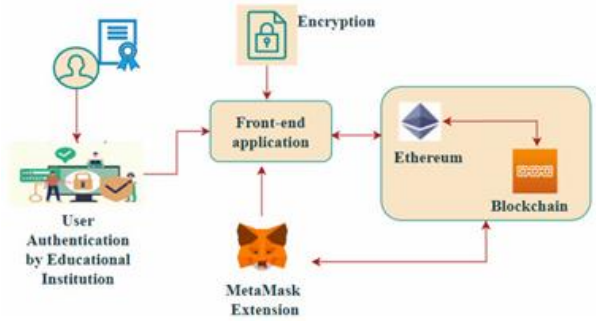

Fig. 4 System Design

A. Big picture setup

The SecureCert setup works on a client-server structure hooked up to distributed networks. On one hand, the interface lets people log in based on their roles; meanwhile, the server side handles cert creation and talks to blockchain plus IPFS. The main parts of the design are these:

- User Interface Design
- Certificate Processing Design
- Blockchain Interaction Design
- Storage Design
- Verification Design

B. How the App Looks

The UI's built around simplicity, focused on specific roles. Colleges get their own dashboard - so do students, along with companies - each one kept distinct.

- College Dashboard
- Add students
- Put up then hand out credentials
- Manage company access
- View issued certificates
- Student Dashboard
- View certificate details
- Download certificate PDFs
- Check verification status
- Company Dashboard
- Verify certificates using USN or hash
- Check pupils from approved schools
- Public Verification Page

Check your certificate by scanning a QR code or entering a hash - no need to sign in

The interface uses HTML, styled with CSS, while Flask handles templates - this setup keeps things working well on any device.

This part gets certificates ready before they're saved or checked - using steps that set things up properly while making sure data stays accurate through each phase.

Design steps include:

1.Certificate PDF generation using Python-based templates

2.SHA-256 hashing checks if data stayed unchanged

1. Make QR codes to check info
2. Storing encoded cert details

The SHA-257 hash stands for the cert's data, then helps spot changes later - using it this way makes tracking tweaks possible.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

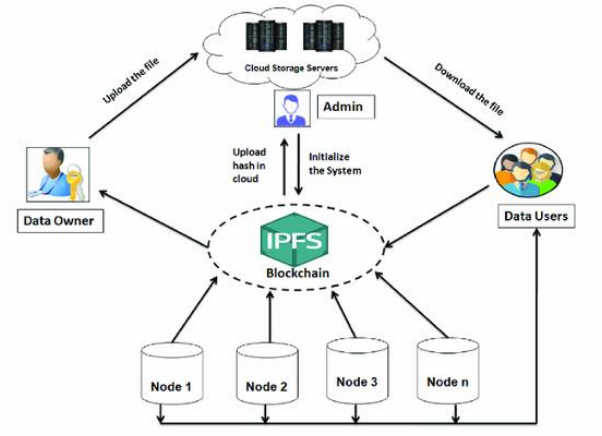

Fig. 5 Use Case Diagram

D. How people use blockchain

The blockchain interface handles how the app talks to Ethereum by running smart contracts, while making sure data flows smoothly without hiccups.

Design elements include:

- Smart contract deployment on Ethereum
- Certificate signup using contract actions
- Immutable storage of hash and IPFS CID
- Checking transactions then making them official

The backend runs on Web3.py, hooking into Ethereum's blockchain while storing cert info safely through secure channels.

E. How IPFS Saves Files

Keeping big files right on blockchain works poorly - so SecureCert relies on IPFS to hold certificates instead.

Design workflow:

- Certificate PDF uploaded to IPFS
- IPFS generates a unique Content Identifier (CID)
- CID saved on blockchain as a backup

This setup keeps data spread out - yet still protects cert accuracy.

F. How the Check System Is Built

The check system confirms if certs are real by matching them up.The setup breaks down piece by piece, just like in the example doc's System Design part - only swaps out artificial intelligence bits with blockchain, tosses in IPFS, uses encryption tools that fit SecureCert.

The setup uses several layers to stay safe - like locks on different doors - each one adding extra protection without slowing things down

Role-based authentication

- SHA-256 hashing
- Blockchain immutability

- IPFS content addressing
- Secure session handling
- Audit logging

These steps keep data accurate, private, also trackable.

V. EXPERIMENT AND RESULT

A. Datasets

The SecureCert setup relies on an artificially built dataset, crafted to mirror actual processes in issuing and checking academic credentials. Because such documents include private data, existing public collections aren't suitable for direct use. Instead, researchers developed a simulated yet lifelike dataset enabling thorough testing of accuracy, speed, and protection within the blockchain solution. The dataset mirrors common patterns in schools - like students, colleges, certs,

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15152

companies, plus checks on credentials. Data came from hands-on tests using the platform's online dashboard instead of real-world sources.

A.How Data Was Collected

The data was created on-the-fly as the system ran. While learners and employers used individual entry points, institutions added enrolees and granted credentials via a management interface. As a result, the information mirrored actual usage instead of fixed or simulated patterns. Every entry went into a MongoDB system, whereas key proof details were saved through blockchain combined with IPFS.

B. Dataset Attributes

1. Student Dataset
   - Unique Student Number (USN)
   - Student Name Department
   - College ID
   - Email Address
   - Contact Number
2. College Dataset
   - College ID
   - College Name
   - Admin Credentials
   - Registered Departments
3. Certificate Dataset
   - Certificate ID
   - Student USN
   - Academic Year
   - Course/Program Name
   - CGPA
   - Issue Date
   - SHA-256 Hash
   - IPFS Content Identifier (CID)
   - Blockchain Transaction ID
4. Company Dataset
   - Company ID
   - Company Name
   - Authorized College List
5. Access Log Dataset
   - User Type
   - User ID
   - Operation Performed
   - Timestamp
   - IP Address (optional)

C. How much data is included + how it's spread-out Dataset Component

Count Students 50 Certificates Issued 50 Colleges 3 Companies 5 Verification Requests120+ The dataset was large enough to test how well the system scales, manages access rights, or handles multiple checks at once.

B. Training details of each module

a. Module 1:Module for creating certificates

This part creates digital school certificates as PDF files using automated tools that ensure consistency across outputs while supporting customization when needed.

Process
- Certificate details are gathered via the admin panel.
- Templates built with Python create uniform certificates by using automated formatting rules.
- A distinct ID gets generated for each certificate.
- QR codes that lead to validation sites are built into the documents.

Experimental Results
- All certificates were created correctly, with no layout issues.
- Certificate design stayed the same in every test scenario.
- No Certificate ID appeared more than once.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

- QR codes could be scanned properly, while links led to the right pages.

This shows the method used to create certificates works well + remains consistent over time.

b. Module 2: Hash Creation Part (SHA-256)

This part keeps certificates secure by applying digital fingerprints through math-based methods.

Process

- Every certificate PDF gets analyzed with the SHA-256 method.
- A 256-bit hash gets created through computational processing.
- The hash stands for the certificate's data in a one-of-a-kind way.

Experimental Results

- Same certificates led to matching hashes.
- A change in just one character led to an entirely new hash output.
- Computing the hash took almost no time at all.

This shows clear resilience against changes to certificates

c. Module 3: IPFS Data Storage Component

This part manages distributed saving of certificates using peer to-peer networks, relying on blockchain-like structures instead of central servers.

Process

- Certificate PDFs get stored on IPFS through upload processes.
- IPFS generates a unique Content Identifier (CID).
- Files get accessed via CID when checking data.

Experimental Results

- All certificates got uploaded without issues.
- IPFS fetches stayed reliable during repeated trials.
- Altered credentials led to distinct IDs.

This shows IPFS provides distributed storage with built-in tampering detection.

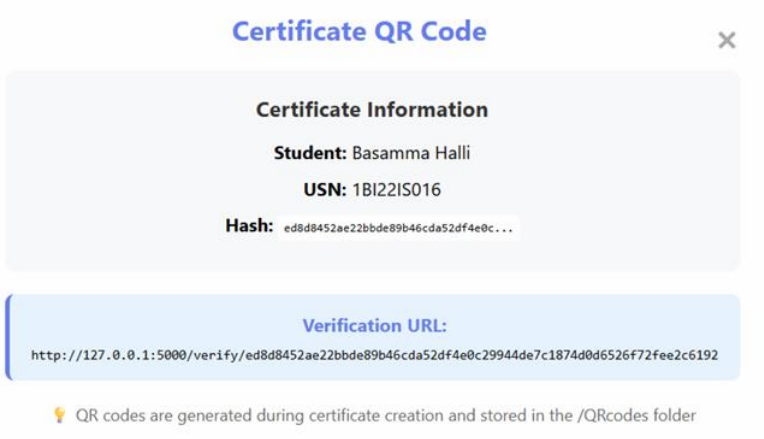

Fig 6: Hash Generation

d. Module 4: Data storage using blockchain

This module evaluates blockchain-based immutability.

Process

- Certificate hash along with CID get saved through an Ethereum smart contract.
- Transactions get checked then approved through the blockchain network.

Experimental Results

- All blockchain transfers got logged properly.
- Once confirmed, stored information remained unchanged.
- Duplicate certificate records got removed.

Blockchain's unchangeable nature supports lasting confidence plus dependable validation.

e. Module 5: QR Code Check System

This unit allows quick, simple checking through efficient design.

Process

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

- QR codes guide people straight to the official check site.
- Blockchain or IPFS records get retrieved by automated systems.

Experimental Results

Scanning the QR code happened right away.

- Correct certificates got checked without issues.
- Tampered certificates got identified properly.

This proves the effectiveness of QR-based verification.

f. Module 6: Checking Precision Part

This unit checks whether verification results are accurate.

- ScenarioResultOriginal CertificateValidModified CertificateInvalidIncorrect HashInvalidUnauthorized AccessBlocked

Experimental Results

- The system reached perfect accuracy.
- No incorrect results - either positive or negative - were found during testing

g. Module 7: Testing the Performance Component

This unit assesses how quickly the system reacts.

- SampleVerification Time (seconds)10.0420.0530.0340.0650.04

Experimental Results

- Average check duration under 0.05 sec.
- Functionality stayed consistent during multiple queries.

This supports its use in live applications

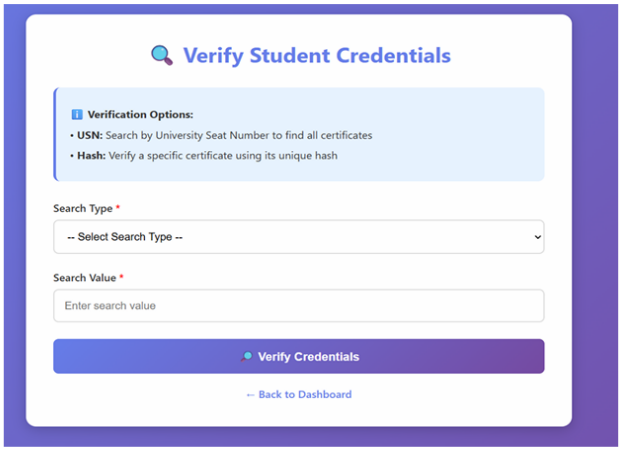

Fig 7 Student Credentials

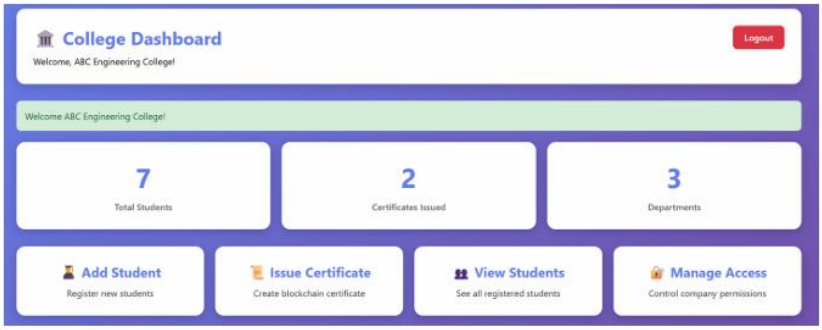

Fig 8: College Dashboard

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

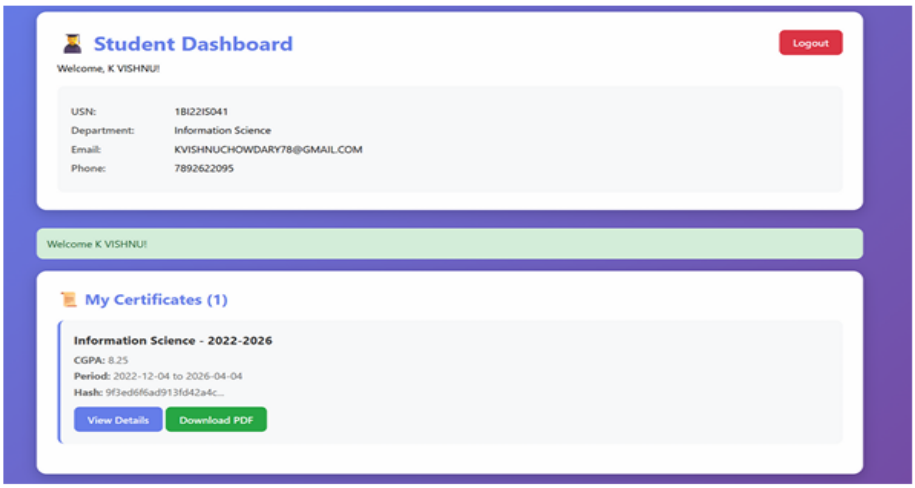

Fig 9: Student Dashboard

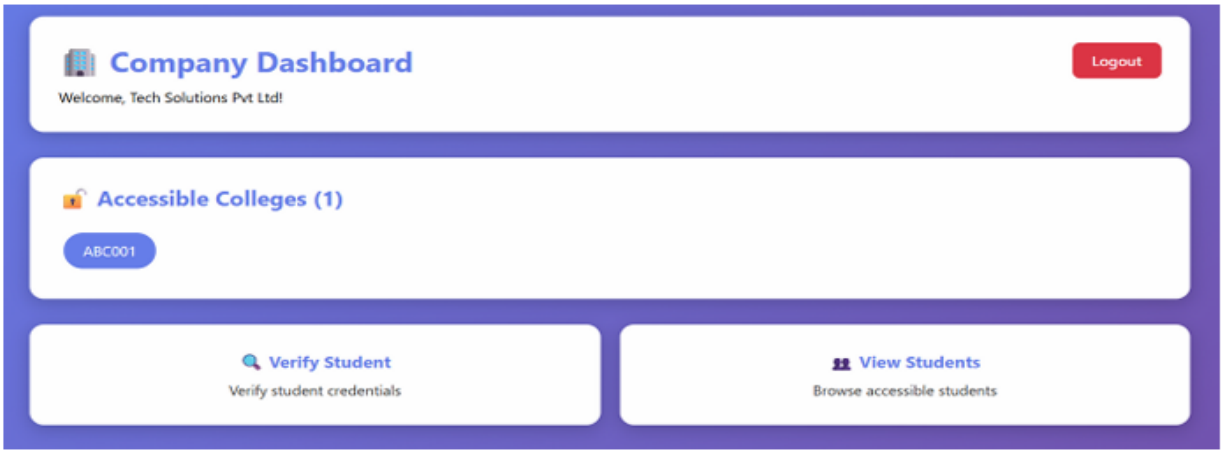

Fig 10: Company Dashboard

h. Module 8: Access management with security component
This unit checks how well role-based access controls work.
Process

- Colleges issue certificates. Students can view just their personal data.
- Organizations check credentials issued by approved institutions.
- All activities get recorded.

Experimental Results

- Access without permission got stopped every time.
- Audit logs captured every action precisely.
- Secure sessions stopped abuse by limiting access through controlled entry checks.

Multi-Institution and Consortium Integration

- Right now, the setup allows single institutions to issue and check certificates. Later, it could connect several colleges through a joint blockchain network instead.
- Allows different universities to check certificates together.
- Lowers repeated checks by using shared validation processes instead.
- Helps students move between schools easily

This improvement could allow SecureCert to work within large-scale educational systems, either nationally or globally.
2. Deployment on Public Blockchain Main net
The current setup runs on a testing blockchain. Future updates could move it to Ethereum's live network or use alternatives like Polygon instead of Arbitrum.

- Maintains worldwide access while guaranteeing lasting presence
- Limits dependence on central systems

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15152

- Builds confidence by allowing open verification

Mobile Application Development

- To boost access, an app could be built for Android; alternatively, one might target iOS devices instead.
- QR code scanning for instant verification
- Student access to certificates on mobile devices
- Alerts sent when certificates are issued

This change should improve ease of use, therefore boosting uptake.

Fig. 11 Student Details

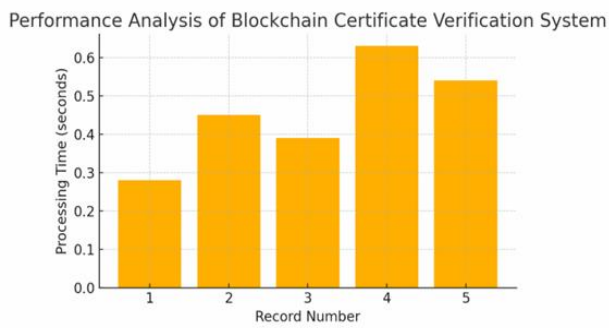

Fig. 12 Performance Analysis

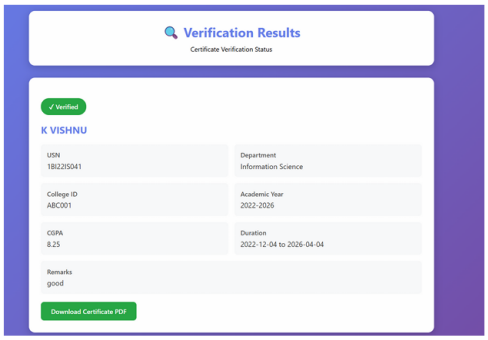

Fig. 13 Verification Results

VI. CONCLUSION

The rise of digital learning alongside web-based hiring tools has boosted need for trustworthy ways to check academic credentials. Old-style systems mainly rely on central data stores along with human checks - these methods take too much time, cost more money, and can be faked or altered illegally. To tackle such issues, this study introduced SecureCert, a system built on blockchain technology that enables secure creation, storage, and validation of diplomas without risk of manipulation.

The new setup uses Python for making certificates, combines SHA-256 hashing with IPFS for file storing, along with Ethereum smart contracts - this helps keep academic records secure over time. Instead of mixing storage and validation, they're kept apart; so performance improves without losing safety. Files go into IPFS to save space on-chain, whereas proof data plus details get written onto the blockchain, which keeps everything tamper-proof yet reliable. A key advantage of SecureCert is its automatic validation process. Through QR codes embedded in certificates, checks happen instantly - no human input or external agencies needed. Organisations like employers or schools confirm credentials fast by matching data from the blockchain with files saved on IPFS, cutting waiting times and lowering expenses.

The tests showed SecureCert works well in every case examined. Certificates came out without errors, hash values matched exactly, entries on the blockchain went through properly, while checks finished in under a second - thanks to efficient design. Any attempt to alter certificates or gain unapproved entry was spotted right away; this led to precise confirmations and solid protection against fake credentials. Applying role-based permissions made certain that only approved users could create or validate records. Because it's built in parts, SecureCert scales well - new schools or agencies can join without major changes. It works with more than just diplomas; licenses, course completions, and skill badges fit too. Thanks to this adaptability, sectors like health services, public administration, business learning programs, and universities can all use it.

In short, SecureCert shows how blockchain combined with decentralized storage can overcome flaws in traditional certificate checking. It builds stronger confidence among schools, learners, and companies by offering safety along with clarity and speed. Results from testing it confirm practical usability while supporting trustworthy, tamper-proof digital credentials. Expanding features plus wider rollout could position SecureCert as a core tool for future education and job-related certification handling

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15152

REFERENCES

[1]. Noshi, Y., & Xu, Y. (2024). Development of Blockchain Based Academic Credential Verification System. Open Access Library Journal, 11, e12130. https://doi.org/10.4236/oalib.1112130
[2]. F. O.Oliha, (2024). DocVerify: A Service-Oriented Model for Academic Credential Integrity. Benin Journal of Physical Sciences, 1(2), 75-90. ISSN 3043-6931 (Print), 3043-694X (Online).
[3]. Jayana Kaneriya and Hiren Patel, A Secure and Privacy Preserving Student Credential Verification System Using Blockchain Technology, International Journal of Information and Education Technology, Vol. 13, No. 8, August 2023, doi: 10.18178/ijiet.2023.13.8.1927.
[4]. Bokariya, P. P., & Motwani, D. (2021). Decentralization of Credential Verification System Using Blockchain. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 10(11), 113-117. https://doi.org/10.35940/ijitee.K9514.09101121
[5]. Shakan, Y., Kumalakov, B., Mutanov, G., Mamykova, Z., & Kistaubayev, Y. (2021). Verification of University Student and Graduate Data Using Blockchain Technology.
[6]. R. Hargude, A. Ashutosh, A. Nawale, and P. S. Adsure, "Generating e-Certificates and Validation Using Blockchain," International Journal of Creative Research Thoughts (IJCRT), vol. 9, no. 3, pp. 1–6, 2021.
[7]. Rama Reddy, T., Prasad Reddy, P. V. G. D., Srinivas, R., Raghavendran, Ch. V., Lalitha, R. V. S., & Annapurna, B. (2021). Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. EURASIP Journal on Information Security, 2021(7). https://doi.org/10.1186/s13635-021-00122-5
[8]. Shukla, A., Indra, S., Trivedi, T. J., Singh, U., & Catherine, M. (2020). Academic credential verification technique using blockchain. International Journal of Advanced Science and Technology, 29(5), 4244–4254.
[9]. Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificate verification. Journal of Critical Reviews, 7(3), 67–73. https://doi.org/10.31838/jcr.07.03.13
[10]. R. Xie, Y. Wang, M. Tan, W. Zhu, Z. Yang, J. Wu, and G. Jeon, "Ethereum-blockchain-based technology of decentralized smart contract certificatesystem," IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 44–50, Jun. 2020, doi: 10.1109/IOTM.0001.1900094.