D.K.T.E. Society’s Textile and Engineering Institute, Ichalkaranji.

(An Empowered Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

Department of Artificial Intelligence and Data Science

2025-2026

Project Synopsis On

AI-Powered Certificate Authentication System for Recruitment

Under The Guidance Of

Mr. S. P. Pise

Submitted By:

Sr.	PRN	Name
1.	22UAD008	Nitin Anna Borase
2.	22UAD020	Ekanath Ramesh Ghasti
3.	22UAD026	Kuldeep Balsao Kamble
4.	22UAD043	Harshal Mahesh Mehtar
5.	22UAD060	Pranav Shrikant Shelar

Mr. S.P.Pise	Prof. (Dr.) T.I.Bagban
Project Guide	**Head of Department**

INTRODUCTION

The project was based on Artificial Intelligence (AI) and Blockchain-based Document Authentication Systems. In today’s digital recruitment world, most applicants submit resumes and digital certificates to highlight their skills and qualifications. However, with the rise of digital document sharing, the manipulated or fraudulent certificates has become major challenge. Ensuring the authenticity of certificates is important for maintaining trust and efficiency in recruitment and academic validation process.

In today’s recruitment and academic validation process, multiple challenge are observed. Fake certificates have become common, misleading recruiters and organizations into accepting fraudulent credentials. Manual verification of documents is not only time-consuming but also prone to human errors, making process inefficient. Another major issue is skill mismatch, where resumes often list skills but it not supported by authentic certificates, ultimately leading to fraudulent recruitment and hiring unqualified candidates.

To overcome above challenges, the integration of advanced technologies such as Artificial Intelligence (AI) and Blockchain offers solutions. AI-powered tools can automatically analyse certificate data and extract relevant information. Blockchain technology ensures certificates are tamper-proof and transparent, enabling secure and decentralized validation. Additionally, embedding QR codes or digital link in certificates allows system to verify their authenticity instantly. Automated system ensure that only genuine and validated certificates consider during recruitment.

The applications of such a system extend across multiple domains. Recruitment systems and corporate HR departments can leverage it to authenticate applicant certificates efficiently. Universities and educational boards can issue blockchain-verified certificates that remain secure and universally valid. Government agencies can adopt this system for validating academic or professional documents at a national scale. Job portals can integrate certificate authentication features, enhancing trust and credibility for both employers and job seekers. Overall, these applications make the system highly beneficial across industries where authenticity and transparency are critical.

RELATED WORK

Paper 1 : Anti-Counterfeit Framework of Electronic Certificate Based on QR Code and Seal Watermark (Springer, 2024)

Summary of work : This paper proposes a QR code + digital watermarking approach for electronic certificate authentication. Each certificate embeds a digitally signed QR code containing encoded verification data, along with a visual watermark (seal). The QR can be scanned by verifiers to validate certificate authenticity, while the watermark helps prevent visual forgery.

Limitations :

1. Lacks decentralization relies on a centralized verification server.
2. Vulnerable if the QR code itself is tampered with or redirected.
3. No support for certificate revocation or updates.
4. Scalability is limited when verifying across multiple institutions.
5. No interoperability with modern standards like W3C Verifiable Credentials.

Paper 2 : Certificate Authentication System Using Blockchain (Springer chapter, 2023/2024)

How it tackles Paper 1's limitations : Unlike Paper 1's reliance on a centralized QR check, Paper 2 introduces blockchain-based verification. Certificates are hashed (SHA3-512) and stored on-chain via smart contracts, creating a tamper-evident record. This addresses the authenticity, auditability, and decentralization gaps of Paper 1.

Summary of work : Proposes a blockchain-based certificate authentication workflow: institutions generate a hash of each digital certificate (SHA3-512), anchor it on-chain via "sealed" smart contracts, and expose a verification process for employers. The aim is to make verification faster, transparent, and cost-efficient compared to traditional manual checks.

Limitations :

1. Limited details on scale/performance (costs, throughput, time-to-verify) across many issuers.
2. Unclear handling of revocation/updates (e.g., name changes, rescinded awards).
3. Interoperability with standards like W3C Verifiable Credentials and DIDs isn't specified.
4. Privacy/PII strategy is not elaborated (on-chain vs off-chain storage).

Paper 3 : The Decentralized Smart Contract Certificate System Utilizing Ethereum Blockchain Technology (ScienceDirect, 2025)

How it overcomes Paper 2's limitations : This work moves beyond verification to cover the full lifecycle—issuance, holding, verification—on Ethereum, clarifying roles (issuer/holder/verifier) and operationalizing decentralized checks. By formalizing issuance flows, it can better support revocation and status, and provides a clearer path to scalability and real-world deployment than a verification-only concept.

Summary of work : Proposes an Ethereum-based system where issuers publish certificate proofs on-chain, holders present them, and verifiers check authenticity without relying on a central authority. The goal is tamper-resistance and trust less verification for digital credentials. Abstract indicates decentralized issuance and verification; full text specifics may include smart contracts and off-chain storage.

Gap Analysis of all research papers:

Lacks of standardization, privacy-preserving mechanisms, and cross-platform adoption, real-world adoption and integration with AI.

Scope for modification and implementation :

1. Interoperability: adopt W3C Verifiable Credentials + DIDs to work across wallets/issuers, add revocation registries and status lists.
2. Scalability & cost: move to L2 rollups (Optimistic/ZK), batch transactions, or store only hashes on-chain with IPFS/cloud for artifacts.
3. Privacy: use selective disclosure/zero-knowledge proofs so applicants reveal only needed claims, keep PII off-chain with encrypted references.
4. UX & adoption: QR-code deep links for instant verify, issuer onboarding portal, admin analytics, webhook/API for HRIS/ATS integration.
5. Security & compliance: formalize smart-contract audits, key management for issuers, GDPR/DPDP-compliant data handling.

PROBLEM DESCRIPTION

In today's recruitment process, companies face a growing challenge of verifying the authenticity of certificates and resumes submitted by applicants. Fake certificates and fraudulent claims of skills are increasingly being used to secure jobs, putting organizations at risk of hiring unqualified candidates. Fake certificates and fraudulent claims of skills from certificates are increasingly being used to secure jobs, putting organizations at risk of hiring unqualified candidates. The manual verification of documents is time-consuming, inefficient, and prone to errors, especially when dealing with a large number of applications. Additionally, the absence of a universal or standardized system for certificate validation further complicates the process, leaving recruiters dependent on inconsistent or unreliable methods.

As a result, organizations struggle with ensuring that skills and qualifications mentioned in resumes are genuinely backed by authentic documents. This leads to skill mismatch as per job requirement and even risks for companies. The lack of transparency in traditional verification processes further increases the chances of fraud going undetected. With the rise of digital certificates, there is also a growing need for systems that can authenticate QR codes or links embedded in certificates in real time and also if no any link or QR available to authenticate.

Therefore, there is a strong need for an automated, secure, and reliable system that can authenticate certificates, validate applicant credentials, and assist recruiters in making hiring decisions. By leveraging technologies such as Artificial Intelligence, Blockchain, and QR code verification, companies can ensure more transparency, accuracy, and trust in the recruitment process.

PROBLEM STATEMENT

Design and develop an AI-powered Certificate Authentication System using blockchain technology, capable of verifying the authenticity of applicant certificates through QR codes, embedded links, and decentralized validation mechanisms to ensure secure, transparent, and tamper-proof recruitment processes.

OBJECTIVES

1. To develop an AI-powered certificate authentication system that can validate the authenticity of submitted certificates.

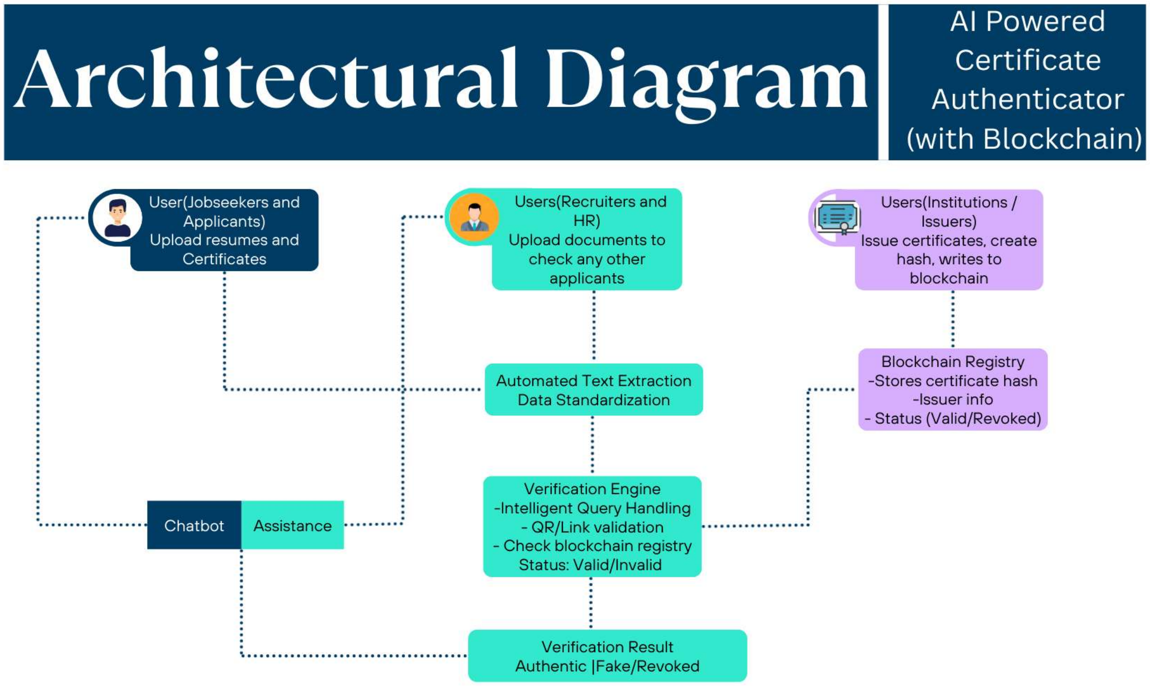
2. System will ensure that only genuine documents are accepted during recruitment process.

3. To build a secure and decentralized certificate repository using blockchain technology.

4. To achieve high accuracy, efficiency, and scalability in the authentication process.

5. Ensuring that large volumes of certificates can be verified in real-time with minimal errors and delays.

METHODOLOGY


Architectural Diagram
AI Powered Certificate Authenticator (with Blockchain)
User(Jobseekers and Applicants) Upload resumes and Certificates
Users(Recruiters and HR) Upload documents to check any other applicants
Users(Institutions / Issuers) Issue certificates, create hash, writes to blockchain
Automated Text Extraction Data Standardization
Blockchain Registry -Stores certificate hash -Issuer info - Status (Valid/Revoked)
Chatbot
Assistance
Verification Engine -Intelligent Query Handling - QR/Link validation - Check blockchain registry Status: Valid/Invalid
Verification Result Authentic |Fake/Revoked

Modules of project :

1. User Authentication & Access Control
2. Certificate Upload & Parsing Module
3. Blockchain Certificate Registry
4. Verification & Validation Engine
5. LLM Support Layer (AI Assistance & Automation)

Description of modules :

1. User Authentication & Access Control :

This module ensures that only authorized users can access the system. It provides secure login and registration functionalities for three primary roles: Applicants (job seekers), Employers/Recruiters, and Institutions/Certificate Issuers.

- Applicants can create profiles, upload resumes, and submit certificates for verification.
- Employers can access verified candidate details and download authenticity reports.
- Institutions can issue new blockchain-backed certificates and revoke fraudulent ones. Authentication is implemented using JWT (JSON Web Token) or OAuth2.0 to provide secure, role-based access control.

2. Certificate Upload & Parsing Module :

In this module, users (applicants or institutions) can upload certificates in PDF or image formats. Once uploaded, the system processes these certificates using OCR (Tesseract / Google Vision API) and NLP techniques to extract key data such as:

- Candidate’s Name
- Issuing Institution
- Skill Certified
- Issue Date & Expiry Date
- Certificate ID or QR Code (if present)

The extracted information is normalized into a structured format and prepared for blockchain hashing and validation. This module forms the basis of ensuring that all data entering the system is machine-readable and ready for verification.

3. Blockchain Certificate Registry :

This is the core trust layer of the system. Once a certificate is uploaded and parsed, its cryptographic hash is stored on the blockchain (e.g., Ethereum, Hyperledger Fabric, or Polygon).

- Institutions issue certificates through a smart contract, which ensures immutability and tamper-proof storage.
- Each certificate gets a unique blockchain transaction ID and an associated QR code that can be scanned for instant verification.
- If a certificate is later revoked, the blockchain ensures that the revocation event is permanently recorded.

This module guarantees transparency, decentralization, and trust by ensuring certificates cannot be forged or altered once registered.

4. Verification & Validation Engine :

This module is responsible for validating the authenticity of uploaded certificates. It works in two main ways:

4.1 QR Code / Link Validation:

- If the certificate contains a QR code, the system scans it using a QR scanner and retrieves the verification link provided by the issuing institution.
- If the certificate has a direct validation link, the system checks whether the link is valid, active, and points to a trusted issuer’s portal.

4.2 Blockchain Validation:

- The certificate's details (or its hash) are cross-checked with the Blockchain Certificate Registry.
- If the certificate exists on the blockchain with matching details, it is marked as Authentic. Otherwise, it is flagged as Unverified or Fraudulent.

The final output is a verification status report (Authentic / Fake / Invalid Link) that can be accessed by recruiters or institutions.

5. LLM Support Layer (AI Assistance & Automation):

- Automated Text Extraction: Using DONUT model we can read scanned certificates or images (PDFs, PNG, JPG) directly and extracts text without using OCR.
- Data Standardization: Normalizes extracted text using Hugging face transformers(RoBERTa (Robustly Optimized BERT)). An improved version of BERT, trained on more data and without some training limitations and much better at context understanding, synonyms, and abbreviations.
  (e.g., "B.Tech AI&DS" → "Bachelor of Technology, Artificial Intelligence and Data Science").
- Intelligent Query Handling: We use Langchain and Google gemini API(2.5 pro) for manages workflow, adds agentic behavior, reasoning, and natural language understanding. This retrieves and explains results.
- Workflow Orchestration: Agentic AI can connect multiple modules (LLM Extraction → Blockchain → Verification → Chatbot Assistance) into an automated pipeline.
- Chatbot Assistance: Provides recruiters and applicants with real-time support by answering FAQs and explaining verification reports in natural language using the Gemini API(2.5 pro).

FACILITIES REQUIRED

1. **Personal Computer**

   - Minimum Specification: Intel i5/i7 processor or AMD equivalent, 8–16 GB RAM, 512 GB SSD storage, Windows/Linux OS.
   - Recommended: Dedicated GPU for AI/ML model training and faster processing.

2. **Application Development Tools**

   - Backend: Node.js / Express.js
   - Frontend: React.js
   - Database: MongoDB
   - Blockchain Framework: Ethereum/Hyperledger Fabric
   - QR/Barcode Libraries: Python qrcode, pyzbar or Node.js qrcode-reader
   - AI/NLP Tools: Python (Scikit-learn, TensorFlow, or PyTorch).

3. **Other Requirements**

   - Cloud Deployment Platform: AWS or Google Cloud
   - Version Control: Git/GitHub
   - Certificate Dataset (for testing): Sample academic and professional certificates with QR codes or verification links.
   - API Services: Blockchain APIs (e.g., Web3.js, Ether.js), QR scanning APIs if required.

REFERENCES

1. << Disha Wankhede, Vidya Gaikwad>>,”<< The Decentralized Smart Contract Certificate System Utilizing Ethereum Blockchain Technology >>”,<< Procedia Computer Science ScienceDirect>>, <<volume 230 Pages 923-934>>,<< 2023>>

2. << Murugan Sekar, A. Rajesh >>,”<< Certificate Authentication System Using Blockchain >>”,<< Integrating Blockchain and Artificial Intelligence for Industry 4.0 Innovations (Springer book chapter)>>,<< 2023>>

3. <<T. R. Sree>>,”<< Decentralized certificate issuance and verification system >>”,<< Presumably an article in ScienceDirect >>,<< 2025>>

4. << De Li, XiangJuan Ran, Xun Jin >>,”<< Anti-counterfeit framework of electronic certificate based On QR code and seal watermark >>”, << Volume 83>> ,<< Multimedia Tools and Applications>>,<< 2024>>

5. <<Dr. Shagufta, Md. S. Sheikh>>,”<< AI-Powered Resume Ranking System: Enhancing Recruitment Efficiency through Natural Language Processing>>”,<< Artificial Intelligence & Data Science, AISSMS Institute of Information Technology, Pune, India >>, << volume 10>>,<< 2025>>

6. <<Noshi, Yuan Xu>>,”<< Development of Blockchain-Based Academic Credential Verification System>>”,<< School of Software Technology, Dalian University of Technology, Dalian, China>>,<< 2024>>

7. <<Imane Khaouja, Mounir Ghogho>>,”<< A Survey on Skill Identification From Online Job Ads>>”,<< IEEE (Conference/Journal)>>,<< 2021>>

8. << Eduard, Martin Gaedke>>,”<< Building a Search-Based Architecture to Enhance Product Certificate Verification and Reducing Counterfeit,>>”,<< 20th International Conferences on WWW/Internet 2021 and Applied Computing 2021>>,<< 2021>>