



CERT-AI-CHAIN: Enhancing Certificate Authenticity and Management with AI and BlockChain

Gauranshi Gupta¹ | Anant Jain² | Rahul Johari³ | Deo Prakash Vidyarthi⁴

¹CSE Department, Guru Gobind Singh Indraprastha University, Delhi, India, gauranshigupta2000@gmail.com, 

²CSE Department, Guru Gobind Singh Indraprastha University, Delhi, India, ritujainanant2810@gmail.com, 

³SWINGER : Security, Wireless, IoT Network Group of Engineering and Research, University School of Automation and Robotics(USAR), Guru Gobind Singh Indraprastha University, Delhi, India, rahul@ipu.ac.in 

⁴School of Computer and Systems Sciences, Parallel and Distributed System Lab, JNU, Delhi, India, dpv@mail.jnu.ac.in, 

Abstract

This research delves into creating a certificate generation and management system using AI techniques like Optical Character Recognition (OCR) and Face Recognition with BlockChain technology. In this article, two novel algorithms, "Smart Contract Algorithm" and "Marksheet Data Extraction Algorithm" have been proposed for the first time. After the successful execution of the OCR technique, accurate data was extracted from eight sample marksheets of a university which included Name, Enrollment number, Year of Admission, Total Credits, and CGPA. The data was further used to generate candidate certificates which were then stored and retrieved using a BlockChain system facilitated by smart contract. To the best of our knowledge and belief, it is the first of its kind of work in such a direction.

KEYWORDS

Optical Character Recognition, BlockChain, Artificial Intelligence, IPFS, Smart Contract, Certificate System

1 | INTRODUCTION

With the increasing demand for skilled labor in the job market the need for higher education and specialized courses increases which subsequently opens the door to digital certificate fraud. This research focuses on solving this issue to streamline the process of digital certificate validation using AI and BlockChain technologies.

BlockChain technology offers unique features which provide a tamper-proof solution for storing digital certificates. Certificates once stored on an immutable ledger cannot be hampered by any unauthorized entity. BlockChain ensures the immutability of certificates through decentralized consensus mechanisms like Proof of Work (PoW) by distributing them across a decentralized network of nodes or entities which makes it extremely difficult for any single node to modify the data without detection.

For designing a robust certificate authentication system a Smart Contract is required to perform the functionality of storing the certificates on BlockChain and generating a unique hash. Smart Contracts are self-executing contracts that execute when certain conditions are met. They automate the entire process by executing functions and performing transactions. For issuing a certificate to the candidate the smart contract stores the hash of the certificate which is generated through IPFS (Interplanetary File System) on the BlockChain along with the receiver address and issuer information. Solidity is a popular programming language for creating smart contracts on Ethereum BlockChain, it is similar to C++ and Java languages.

IPFS can be understood as the decentralized storing and sharing system for files. The files stored on IPFS are not stored on a single server but distributed across a network of computers making them available even if some computers are offline. After storing the file on this file system it creates a unique public URL which can be used to access that file.

Machine Learning (ML) is a branch of Artificial Intelligence that trains a model to predict or forecast information based on provided information. ML techniques learn from data provided at the time of training to identify patterns and make decisions based on the data.

Facial recognition is a very popular application of Machine Learning that recognizes human faces in images or videos. It involves extracting facial features from an image or video frame, like the shape of the nose, the distance between the eyes, and

Abbreviations: ML, Machine Learning; OCR, Optical Character Recognition; IPFS, Interplanetary File System; URL, Uniform Resource Locator.

the shade of the face. The extracted features are then compared against a database of known faces to identify or verify individuals. In the case of identifying valid candidates for issuing certificates university can capture the facial features of candidates in real time and compare them with their existing database. Python library like Deepface is used to identify the candidate and validate whether he or she belongs to the institute or not.

Optical Character Recognition (OCR) is a Machine Learning technique that is used to extract information from any document or handwritten text. OCR analyzes the characters in documents and converts them into text which is in computer-readable format. In the certificate verification system, the OCR algorithm can read and extract relevant information from the student's marksheets and ID Card which can then be used to generate certificates for them. For OCR Pytesseract Python library can be used to read information for the documents.

For the sake of simplicity, the paper is divided into multiple sections and subsections, section 2 describes the Problem Statement, section 3 describes the Literature Survey, section 4 Methodology, section 5 provides two novel Algorithms proposed which explains the process involved in the ML model and the Smart Contract, section 6 Novelty, section 7 Results, section 8 Project Deployment and Simulation Guidelines, section 9 Conclusions, section 10 Future Work.

2 | PROBLEM STATEMENT

Certificate fraud happens when a person fakes the evidence of having some qualification which usually happens to grab a job offer. They create very realistic-looking certificates for any degree, diploma, or course. This problem is rising with the rise of photo editing tools, modern software, and high printing quality. Due to the lack of availability of a full-proof certificate validation system, many universities and organizations face challenges in identifying the originality of the certificate. This is a big issue that can lead to the loss of a company's reputation and waste of their time if they hire unskilled candidates. Due to unqualified staff, an organization may not fulfill customer's requirements and the company's reputation may suffer. This issue can be dangerous for health-related professions like medicine, food, and other industries where fake certificates can harm individuals leveraging these health services. Also, industries like construction businesses need to ensure that employees are qualified. According to the Association of American Medical Colleges (AAMC) in 2021, 20% of medical applicants faked their certificate credentials [13].

To overcome this issue organizations must adopt a system that offers a tamper-proof certificate validation system. Such a system must verify candidates for whom certificates will be issued and have a secure storage system to maintain traceability and immutability.

3 | LITERATURE SURVEY

In [1], authors told that BlockChain now expands beyond cryptocurrency into fields like government, healthcare, and supply chain, with countries like Australia and Japan integrating it for its decentralized, immutable storage capabilities which started with Bitcoin introduced by Satoshi Nakamoto in 2008.. Utilizing smart contracts, it eliminates the need for third-party involvement across sectors. This research systematically explores BlockChain in education, categorizing projects by service and technology, aiming to identify gaps by conducting a systematic survey on BlockChain-based digital certification and enhancing BlockChain's educational application.

In [2], authors critically examines the issuance of tamper-proof certificates that are essential for trust across academia, government, and industry. It uses a multi-dimensional framework for assessing security, cost, complexity, and scalability of various security models. It includes traditional and technologies like BlockChain and Zero-Knowledge Proofs. Their comprehensive analysis reveals each model's strengths and weaknesses. It also indicates that no single model offers the best balance across the metrics. The study concludes with some recommendations, guiding stakeholders towards informed decisions on using the most effective tamper-proof certificate issuance systems.

In [3], authors addresses the challenge of revocation management in Public Key Infrastructure(PKI) which is crucial for security yet strained by growing networks and the IoT. They proposed a BlockChain-based, decentralized solution enhancing certificate revocation and verification. By utilizing the X509 certificate extension field for revocation distribution using Bloom filters, storing bloom filter and revocation information on a public BlockChain, and implementing this system in Python and Namecoin BlockChain, their results shows superior efficiency and cost-effectiveness compared to traditional methods like OCSP and CRL, marking a significant advancement in secure, scalable revocation management.

In[4], authors discuss about Smart E-Learning, which utilizes information technology, especially artificial intelligence (AI), enhances connectivity, sharing, and flexibility in education which open the gates for online teaching, learning, and assessment. Despite its advantages, data privacy emerges as a major concern, which incur various challenges to the development of smart E-Learning applications. The integration of Blockchain technology with E-Learning aims to enhance the security within this digital education ecosystem. This paper discusses about the potential and challenges of applying AI and Blockchain in developing smart E-Learning applications in Vietnam. It suggests that the integration of AI and Blockchain with independent testing models into smart E-Learning system.

In [5], authors discuss that today's educational institutions face the critical challenge of maintaining the authenticity and secure exchange of digital student records. To safeguard against record manipulation, this study introduces a Blockchain-based framework for the secure storage, verification, and distribution of academic data. It also diminishes the reliance on third-party verification. It utilizes the Keccak-256 secure hash algorithm to generate a unique, consistent 256-bit hash for each student's record to ensure data integrity. This approach utilizes Blockchain's features such as immutability, transparency, and self-sovereignty to provide a reliable and secure method for data exchange. Therefore preventing unauthorized data alteration and fabrication.

In [6], authors explained that Blockchain technology can revolutionize education by providing cost-effective learning solutions and enhancing academic certificate verification. It includes reviews of 34 studies published between 2018 and 2022, using the PRISMA framework for identifying key themes and research gaps. Majorly, six themes emerged, and recommendations for future research and practical applications were provided to assist researchers, policymakers, and practitioners in leveraging Blockchain for educational purposes.

In [7], authors discuss about the risk associated with centralized storage of certificates by their universities such as hacking or data loss because documents are crucial for employment or further education. Verifying these certificates manually is also labor-intensive and tedious task. The rise of advanced software has increased the issue of credential forgery and replacing lost or damaged certificates is a lengthy process. A Blockchain-based solution offers a decentralized approach which ensures data integrity through cryptographic links and shared chains across the network. This proposed system aims to streamline certificate verification, counter forgery and speed-up the issuance process. It revolutionizes the current methodology of certificate management by developing a decentralized application (DAPP) to overcome the existing issues.

In [8], authors convey that academic credentials play a pivotal role for individual careers and societal advancement but suffer from inefficiency and fraud within the existing paper-based issuance, storage, and sharing system. The rampant issues, including diploma mills and forgery, underscore the urgent need for a Blockchain-based system which is indisputable and provides credential authenticity. Blockchain technology, offering transparency and verifiable ownership through decentralized storage and Public Key Cryptography (PKC) via Digital Signatures. This project employs the ECDSA algorithm for credential authentication and signing by various authoritative entities, including educational institutions and ministries. It enables credential verification for third parties, like employers, bypassing conventional verification hurdles.

In [9], authors discuss that digital education transformation requires a shift in how to validate and secure student data, especially online degrees. Blockchain technology provides immutable record-keeping and offers a secure alternative to traditional methods. It prevents data alteration and enhances data protection beyond password-secured directories. Its decentralized verification process, independent of central authorities, facilitates global recognition of credentials. This paper explores Blockchain's potential in e-learning to prevent identity fraud and securely store student information. It addresses challenges and opportunities for incorporating this technology in online and traditional educational settings.

In[10], authors discuss that the traditional degree verification process between universities and the Higher Education Commission (HEC) is highly complex as it involves manual checks and physical document submission. Blockchain technology offers a solution through HEDU-Ledger, a system that enables secure, quick, tamper-proof verification and tracing of academic records. This decentralized approach uses hyperledger fabric to ensure integrity and privacy, streamlining the attestation process by directly connecting HEC and universities. It overcomes language and administrative hurdles, offering enhanced security and privacy over existing methods.

In [11], authors combat the global issue of educational certificate fraud. This paper introduces a decentralized system utilizing Ethereum Blockchain and the InterPlanetary File System (IPFS) for securing and verifying academic credentials. All the transactions were carried out using the Ropsten Ethereum test network. IPFS facilitates decentralized storage of certificate files, while a smart contract developed in Solidity and deployed via the Remix IDE supports validation. Verification is simplified through a QR code scan, linking directly to the Ethereum network for immediate certificate authentication.

In [12], authors discuss about the limitations of traditional identity authentication methods as it relies on centralized entities, so it has chances for single points of failure and scalability. This article introduces a Blockchain based identity authentication scheme. Users create multiple identities to request certificates while the authorities distribute these certificates using ECDSA and RSA algorithms via smart contracts. This approach not only keeps the users' real identity information safe but also reduces the storage burden of managing numerous certificates. Their security and performance evaluation confirms the scheme's effectiveness and practicality in meeting rigorous security standards.

4 | METHODOLOGY ADOPTED

4.1 | Description

Below is a sequential flow of the entire proposed architecture as shown in FIGURE 2.

1. Documents storage: Candidates submit their documents including photo ID card, Marksheet, Aadhar, or any other sort of identity proof.
2. AI verification: The institute registered on the system does the AI verification of the candidate by Facial recognition using the DeepFace Python library and Optical Character Recognition (OCR) technique using the Pytesseract Python library.
3. Certificate Generation: The certificate will be generated with details fetched from OCR and Facial Recognition using the Python library Reportlab.
4. Issuing Certificate: The educational institute issues a unique certificate to each candidate.
5. Certificate Storage: The certificate will be stored on the IPFS (Interplanetary File System) which generates a public URL for that certificate.
6. Smart Contract interaction: The Smart Contract securely stores information about educational institutions and certificates on the Blockchain.
7. Accessing the Certificates: The certificates stored on the Blockchain can be accessed by any recruiting party or the student by entering the details about the student.

4.2 | Architecture Diagram

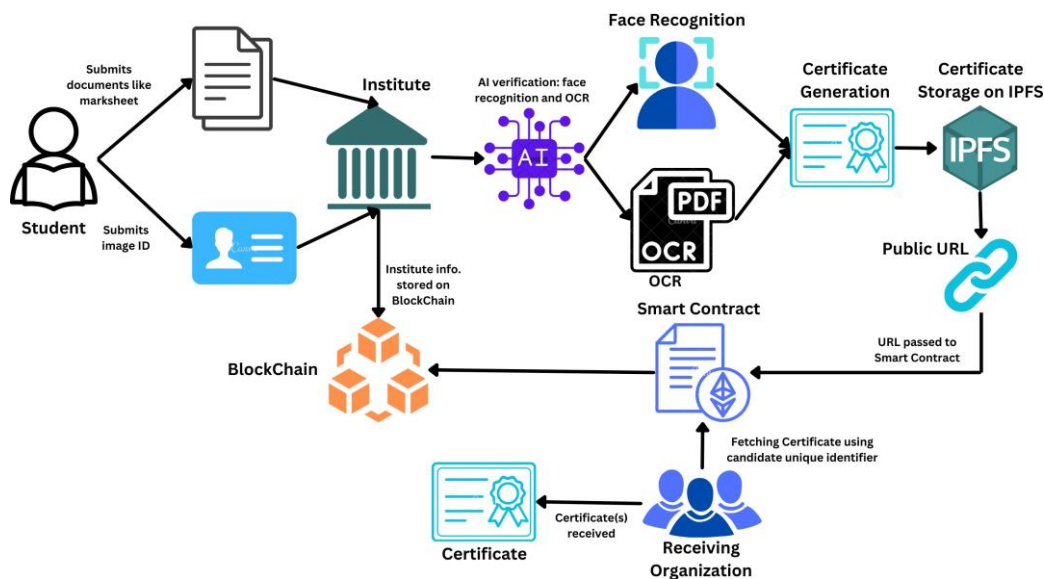


FIGURE 1 Architecture Diagram

FIGURE 1 explains the architecture of the proposed methodology. It starts with a student submitting documents that the university or institute uses to create and manage certificates. The institute details are stored on the BlockChain network to maintain traceability of records. AI algorithms like OCR and Face Recognition are utilized to validate candidates, then certificates are generated which are stored on BlockChain using IPFS and Smart Contract. These certificates are accessible to receiving organizations through candidate credentials.

4.3 | Flow chart

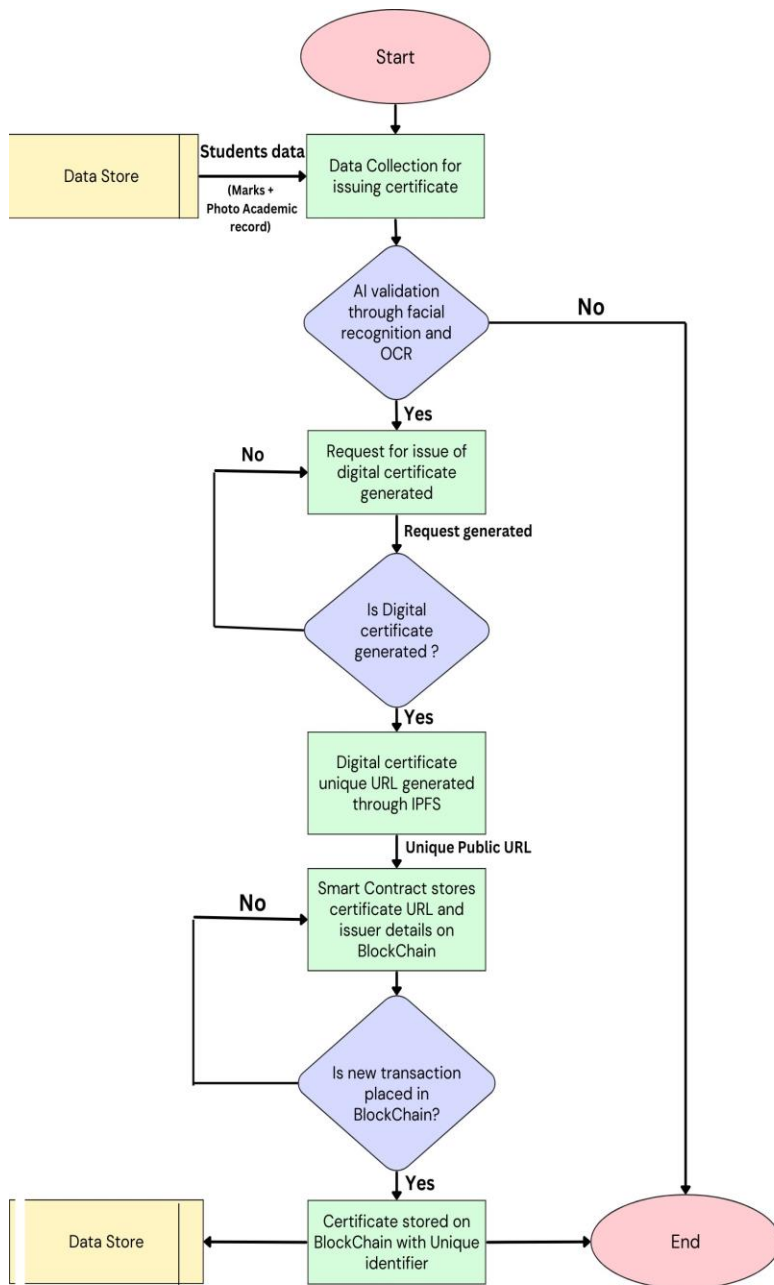


Fig 1.1

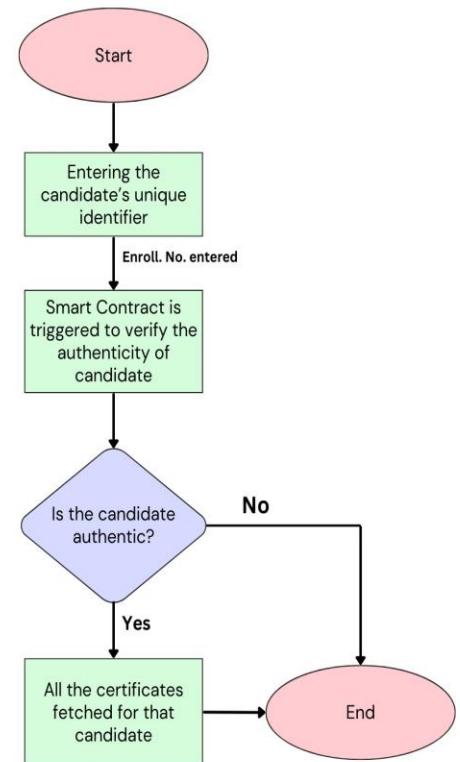


Fig 1.2

FIGURE 2 Flow Chart of the Certificate system

4.4 | Use Case Diagram

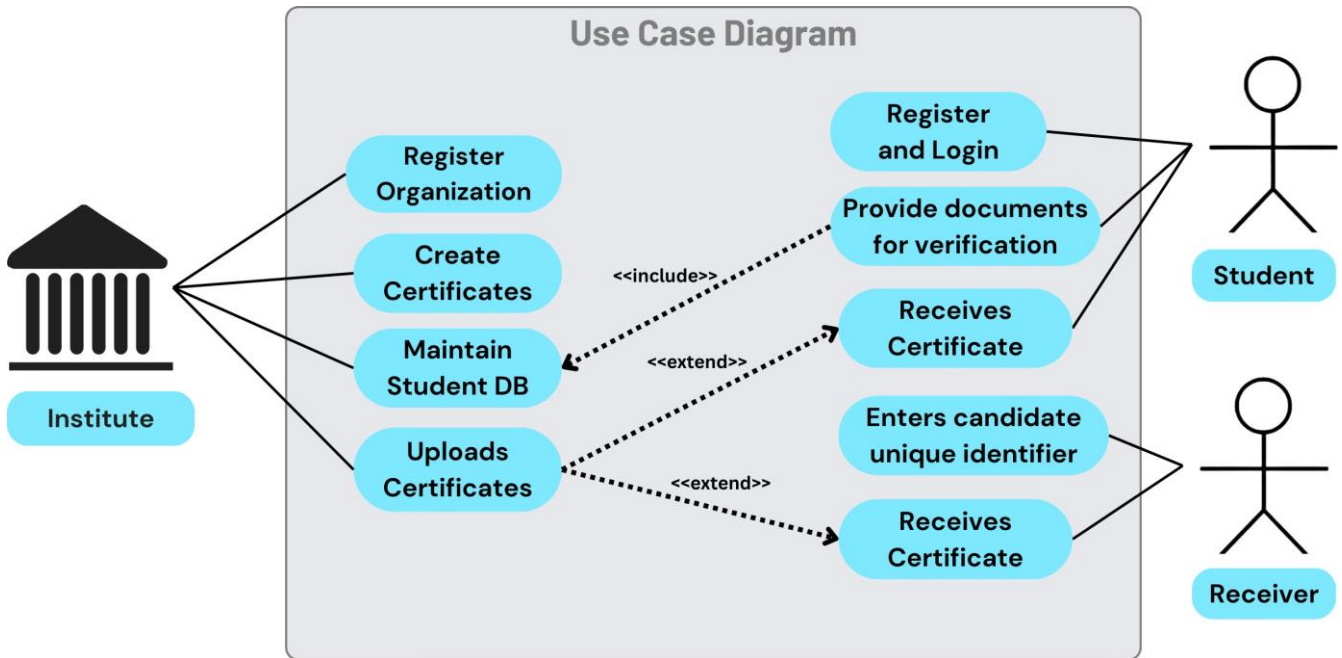


FIGURE 3 Use Case Diagram showing the roles of all the stakeholders in the system.

FIGURE 3 is a use case diagram that represents handling academic certificates. An institute has functions such as registering organizations, creating and uploading student certificates, and maintaining a student database. Students register, log in, and submit documents for verification to receive certificates. A receiver which may be an employer or another educational institution, can enter the student's unique identifier to receive and verify the student's certificate.

5 | ALGORITHMS

5.1 | Smart Contract

This algorithm outlines the operations of a smart contract for managing organizational registration, verification, token creation, and tracking of certificates on a Blockchain. Functions REGISTERORGANIZATION, ISORGANIZATIONVERIFIED, CREATETOKEN, CREATELISTEDTOKEN, GETORGANIZATIONCERTIFICATES, and GETUSERCERTIFICATES are defined to handle various aspects.

1. Registration and Verification: REGISTERORGANIZATION checks if an organization is already registered (IsVerified). If not, it registers and marks the organization as verified. ISORGANIZATIONVERIFIED simply checks the verification status.
2. Token Management: CREATETOKEN and CREATELISTEDTOKEN handle token creation. CREATETOKEN mints a new token and assigns it a unique ID and URI, while CREATELISTEDTOKEN associates the token with a receiver, facilitating its transfer.
3. Certificate Retrieval: GETORGANIZATIONCERTIFICATES and GETUSERCERTIFICATES retrieve all tokens associated with a specific organization or user, respectively, effectively listing the certificates each holds.

Algorithm 1 Smart Contract

```

1: Notation:
2: Org - Organization
3: Tkn - Token
4: RegNo - Registration Number
5: Pin - Pincode
6: URI - Uniform Resource Identifier
7: Addr - Address
8: IsVerified - Verification status
9: function REGISTERORGANIZATION(CompName, Loc, RegNo, Pin)
10:   if Org[Addr].IsVerified then
11:     print("Organization Already Registered")
12:     return
13:   end if
14:   Org[Addr] ← CreateOrganization(CompName, Loc, RegNo, Pin, True)
15:   emit OrganizationRegistered(CompName, Loc, RegNo, Pin)
16: end function
17: function ISORGANIZATIONVERIFIED
18:   return Org[Addr].IsVerified
19: end function
20: function CREATETOKEN(URI, Receiver)
21:   Increment TokenIDCounter
22:   TknID ← GetCurrentTokenID()
23:   MintToken(Addr, TknID)
24:   SetTokenURI(TknID, URI)
25:   CreateListedToken(TknID, Receiver)
26:   return TknID
27: end function
28: function CREATELISTEDTOKEN(TknID, Receiver)
29:   Tkn[TknID] ← CreateListedTokenStruct(TknID, Addr, Receiver, False)
30:   TransferToken(Addr, Receiver, TknID)
31: end function
32: function GETORGANISATIONCERTIFICATES(Org)
33:   Total ← GetTotalTokenCount()
34:   Count ← 0
35:   for i = 1 to Total do
36:     if Tkn[i].Creator == Org then
37:       Add Tkn[i] to OrgCerts
38:       Increment Count
39:     end if
40:   end for
41:   return OrgCerts
42: end function
43: function GETUSERCERTIFICATES(User)
44:   Total ← GetTotalTokenCount()
45:   Count ← 0
46:   for i = 1 to Total do
47:     if Tkn[i].User == User then
48:       Add Tkn[i] to UserCerts
49:       Increment Count
50:     end if
51:   end for
52:   return UserCerts
53: end function

```

5.2 | Machine Learning Model

This algorithm aims to extract marksheet information using OCR. It utilizes Python Image Library and Pytesseract to process and extract text from images. This algorithm uses regular expressions to match and extract relevant information such as the student's name, enrollment number, admission year, and CGPA from the OCR output. These patterns are based on the typical layout and formatting found in marksheet documents.

Algorithm 2 Image Processing and Data Extraction

```

1: Notation:
2: img - Input image file path
3: data - Extracted OCR data
4: pattern - Regular expression patterns for data extraction
5: function LOADIMAGE(image_path)
6:   img ← OPEN(image_path)
7:   return img
8: end function
9: function APPLYOCR(img)
10:  data ← TESSERACT(img)
11:  print data
12:  return data
13: end function
14: function EXTRACTDATA(data)
15:  Initialize patterns with regular expressions for name, enrollment, etc.
16:  Initialize extracted_data as empty dictionary
17:  for each pattern in patterns do
18:    match ← SEARCH(pattern, data)
19:    if match is not None then
20:      extracted_data[FIELDNAME(pattern)] ← CLEAN(match.group(1))
21:    end if
22:  end for
23:  return extracted_data
24: end function
25: function MAIN(image_path)
26:  img ← LOADIMAGE(image_path)
27:  ocr_data ← APPLYOCR(img)
28:  marksheet_data ← EXTRACTDATA(ocr_data)
29:  print marksheet_data
30: end function
31: Set the path to the Tesseract executable
32: Set the path to your image file
33: MAIN('./marksheets/anant.jpg')

```

6 | NOVELTY

The proposed certificate management system uses AI techniques like Face Recognition and Optical Character Recognition along with Blockchain functionalities which is a novel approach in the field of certificate management. The integration of these two technologies is a novel idea that distinguishes it from other research methodologies. This research focuses on explaining every

component of the architecture with a theoretical explanation as well as practical implementation shown in section 7. It also provides algorithms for Smart Contract and ML model in section 5 utilized in creating the certificate creation and management system.

7 | RESULT

The smart contract was successfully deployed on the Sepolia testnet, which can register institutes based on their unique ID, issue certificates to candidates, and allow fetching certificates by entering candidate credentials. FIGURE 4 is a screenshot of the institute's registration on the BlockChain portal. It shows how an organization can register itself on the portal by connecting its wallet and entering the Registration Number, Name, Address, and Pincode. Upon clicking the register button, Metamask prompts the user to sign the transaction ensuring security.

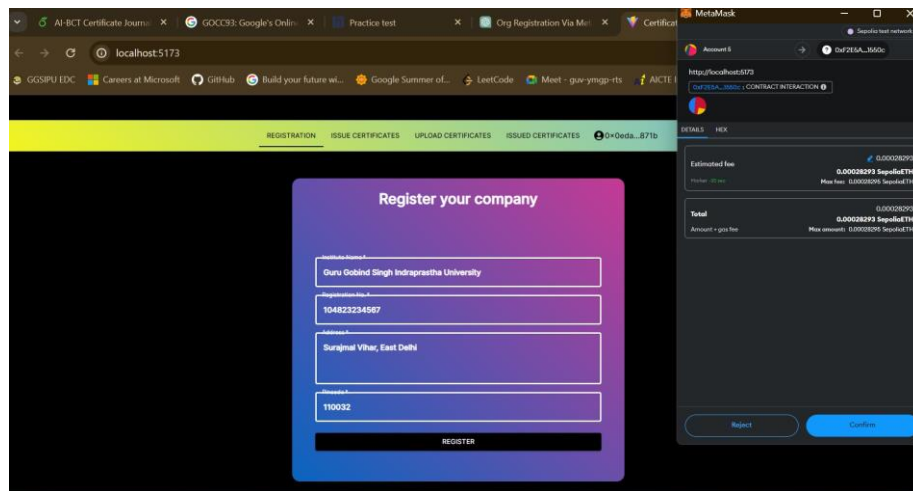


FIGURE 4 Registration of Institute

FIGURE 5 takes the receiver address and certificate file as input which is stored on the BlockChain. the uploaded certificate first gets uploaded on IPFS (Pinata here). The BlockChain then maintains the information about the issuer, the receiver, and the certificate URL (IPFS hash).

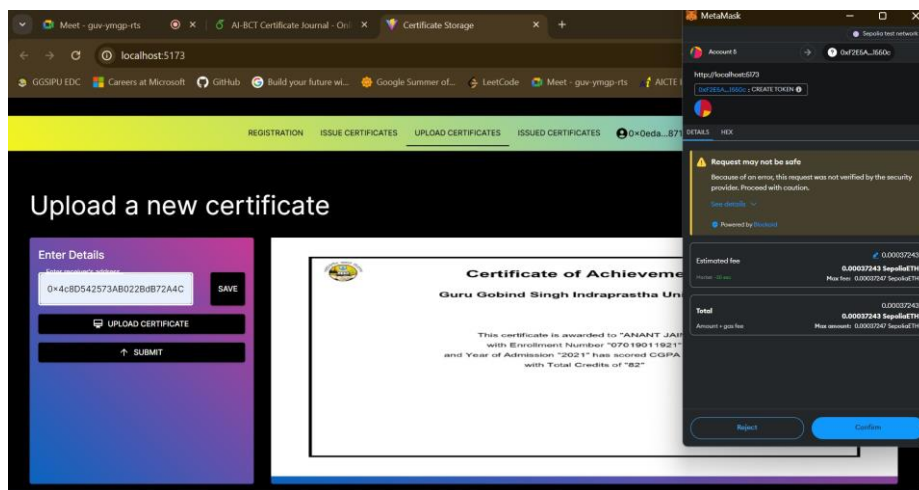


FIGURE 5 Issuing Certificate

FIGURE 6 shows the certificates fetched associated with the candidate whose credentials are entered. The IPFS public URL for the uploaded certificate is: <https://gateway.pinata.cloud/ipfs/QmaEw2d6ipHqgSsXZuJsbwGNoBhkTV81v87s6PwL1RF96>

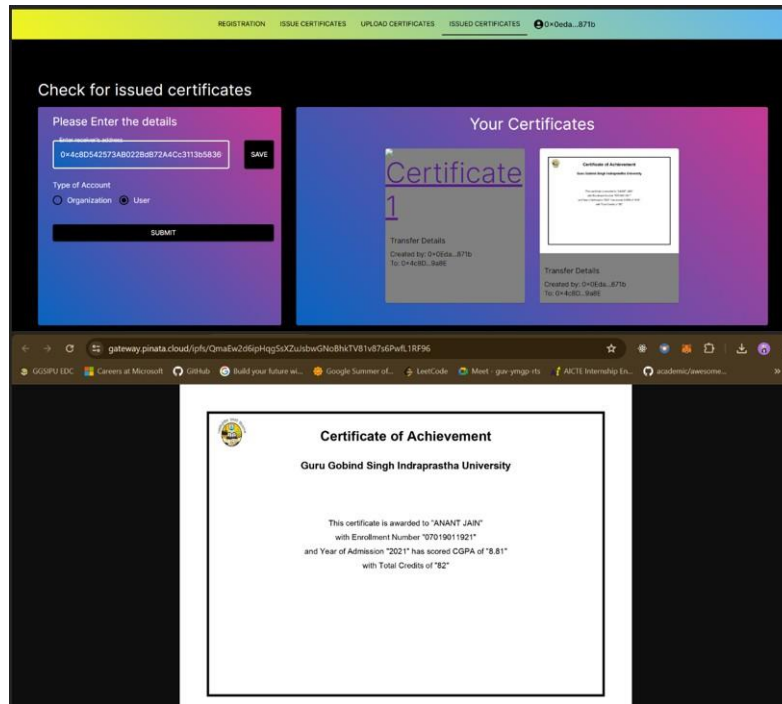


FIGURE 6 Fetched Issued Certificates

The ML model can fetch student data from the marksheet provided and create a certificate based on the fetched data. FIGURE 7 shows the marksheet and the certificated created on performing OCR using Pytesseract Python library.

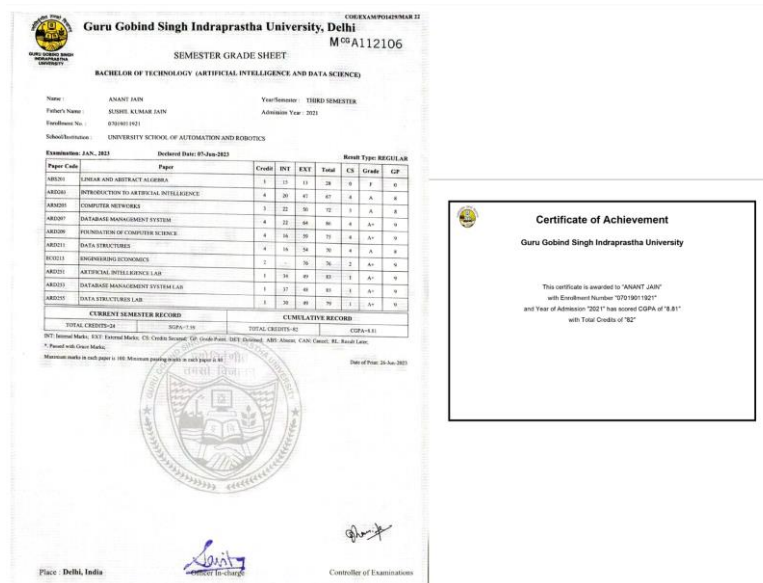


FIGURE 7 Snapshot of Marksheet and Certificate Created

8 | PROJECT DEPLOYMENT AND SIMULATION GUIDELINES

Deployed link of the certificate storage and verification system <https://certificate-generator-and-validator.vercel.app/>. It will allow users to register as an organization, upload certificates and fetch certificates. To simulate this project following are the software and hardware requirements of the device.

8.1 | Software Requirements

1. Metamask: It is necessary to have Metamask installed on the browser interface along with some accounts to register as an institute and receive certificates.
2. Sepolia Test network tokens: To sign the transactions and store the data on the BlockChain users must have some Sepolia tokens which can be achieved from [Sepolia Faucet](#)

8.2 | Hardware Requirements

1. Desktop or Laptop: The provided link works best on a bigger screen such as a Laptop or Desktop screen.

9 | CONCLUSIONS

In conclusion, the integration of Artificial Intelligence (AI) with BlockChain technology has demonstrated its effectiveness in establishing a secure, transparent, and efficient system for issuing, verifying, and retrieving certificates. This paper presents an end-to-end implementation of the system, starting with issuing certificates by academic institutions and access to certificates by recruiting parties candidate credentials. The integration of AI-like facial recognition and Optical Character Recognition (OCR) techniques enhances the verification process, ensuring the accuracy and reliability of candidate credentials. This innovative system overcomes the challenges with traditional certificate authentication methods and contributes to a more trustworthy certification process by providing a double verification process.

This implementation of certificate validation is not limited to academic institutions but any organization can store and fetch documents on the system.

AUTHORS CONTRIBUTIONS

1. **Anant Jain:** Literature Survey, Algorithm Formulation, Coding and Simulation, Writing - original draft.
2. **Gauranshi Gupta:** Methodology Adopted, Result, Coding and Simulation, Writing - original draft.
3. **Rahul Johari:** Supervision, Proof Reading and Editing, Project Administration, Writing - original draft, Literature survey.
4. **Deo Prakash Vidyarthi:** Supervision, Proof Reading and Editing, Project Administration

ACKNOWLEDGEMENT AND SUBMISSION

Sincere appreciation to Guru Gobind Singh Indraprastha University and Jawaharlal Nehru University for providing a conducive work environment, which has greatly facilitated our research efforts and the successful implementation of our proposed ideas. This paper is an expanded and extended version of the paper titled "Integration of AI with BlockChain towards Authentication of Testimonials and Transcripts In Academic Institutions" presented in the International Conference On Innovative Computing And Communication 2024 at Shaheed Sukhdev College Of Business Studies, University Of Delhi.

CONFLICT OF INTEREST

The authors declare no potential conflict of interest.

10 | FUTURE WORK

The future of the research will work on integrating the ML model within BlockChain system which will provide users with a single platform for creating, uploading, and accessing certificates securely. Work will also be done to improve the ML model to perform image analysis and validation capabilities, enabling to verification of student images in marksheets documents. This will ensure a more comprehensive verification process, enhancing the overall integrity and reliability of certificates issued through the system.

REFERENCES

1. Murugesan S, Lakshminarasaiiah MB. A survey on blockchain-based student certificate management system. In: Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance. 2021:44–50.
2. Mboma JGM, Lusala K, Matalatala M, Tshipata OT, Nzakuna PS, Kazumba DT. Integrating LLM with Blockchain and IPFS to Enhance Academic Diploma Integrity. In: 2024 International Conference on Artificial Intelligence, Computer, Data Sciences and Applications (ACDSA). IEEE. 2024:1–6.
3. Adja YCE, Hammi B, Serhrouchni A, Zeadally S. A blockchain-based certificate revocation management and status verification system. *Computers & Security*. 2021;104:102209.
4. Hung NQ, Phung TK, Hien P, Thanh DNH. AI and Blockchain: potential and challenge for building a smart E-Learning system in Vietnam. In: . 1022 of *IOP conference series: Materials Science and Engineering*. IOP Publishing. 2021:012001.
5. Akter F, Rahman MM, Haque R, et al. A Digital Certificate Forgery Prevention Using Blockchain Technology. In: International Conference on Big Data, IoT and Machine Learning. Springer Nature Singapore. 2023:893–909.
6. Rustemi A, Dalipi F, Atanasovski V, Risteski A. A systematic literature review on blockchain-based systems for academic certificate verification. *IEEE Access*. 2023.
7. Bokariya PP, Motwani D. Decentralization of Credential Verification System using Blockchain. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*. 2021;10(11).
8. Al Hemairy M, Abu Talib M, Khalil A, Zulfiqar A, Mohamed T. Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance. *Education and Information Technologies*. 2024:1–30.
9. Pfeiffer A, Bezzina S, Wernbacher T, Kriglstein S. Blockchain technologies for the validation, verification, authentication and storing of students' data. tech. rep., 2020.
10. Khan AA, Laghari AA, Shaikh AA, Bourouis S, Mamlouk AM, Alshazly H. Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Applied Sciences*. 2021;11(22):10917.
11. Jaafar RA, Alsaad SN, Al-Kabi MN. Educational Certificate Verification System: Enhancing Security and Authenticity using Ethereum Blockchain and IPFS. *Al-Mustansiriyah Journal of Science*. 2024;35(1):78–87.
12. Gao S, Su Q, Zhang R, Zhu J, Sui Z, Wang J. A privacy-preserving identity authentication scheme based on the blockchain. *Security and Communication Networks*. 2021:1–10.
13. Association of American Medical Colleges stats. <https://www.legicred.com/guide-to-prevent-certificate-fraud-in-education>; .