International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Block Chain-Powered Certificate Verification and Validation System

Prof. Chetan Padole
Guide from Department of Information Technology and Data Science
J D College of Engineering and Management, Nagpur, India
Mail...cppadole@jdcoem.ac.in

Prof. Rohan Kokate
HOD of Department of Master of Computer Applications
J D College of Engineering and Management, Nagpur, India
hodmca@jdcoem.ac.in

Achal Vighne
Student of Department of Master of Computer Application
J D College of Engineering, Nagpur, India
achalvighne8@gmail.com

Abstract: **In the digital world, each and everything is digitalized in which the certificate of SSLC, HSC, and academic certificate are digitalized in the educational institution and provided to the students. Students are difficult to maintain their degree certificates. For the organization and institution, verification and validation of certificates are tedious and cumbersome. Our project will help to store the certificate in the blockchain system and provide security. First, the paper certificates are converted into digital certificates. The chaotic algorithm is used to generate the hash code value for the certificate. Then the certificates are store in blockchain. And these certificates are validated by using the mobile application. By using blockchain technology we can provide a more secure and efficient digital certificate validation.**
Keywords: blockchain, digital certificate, hashing, a chaotic algorithm

I. INTRODUCTION

Blockchain was introduced in the year 2008 by Satoshi Nakamoto. Blockchain is one of the online ledgers which provide decentralized and transparent data sharing. In this project, we design an android application used to provide secure verification of our certificates. In nowadays, all Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should not be easily accessible to outside entities. Hence, there is a high need for an efficient mechanism, that can guarantee the information in such certificates is original, which means the document has originated from a reliable and authorized source and is not forged. Various systems have been designed to secure e-certificates for education institutions and to store them securely in cloud-based systems. Blockchain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also helps in eliminating the need for constant verification of certificates. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. Technologies that exist in security domains include digital signatures, which are used in digital documents to provide authentication, integrity, and non-repudiation. Also, with blockchain in play, the storage of certificates is more secure. With these technologies, an application created that facilitates the secure validation of digital certificates.

II. LITERATURE SURVEY

Jin-chiou et al [1] developed software in order to avoid counterfeiting certificates. Due to the lack of an anti-forge mechanism, the graduation certificate is to be forged. so, the decentralized application was designed based on Ethereum blockchain technology. First, generate the digital certificate for the paper certificate then hash value created for the certificate is stored in the blockchain system. Even it used to verify the authenticity of the certificate it required another scanning app to scan the certificate. The system saves on paper, prevent document forgery. But the QR-Code must be scanned with a smartphone and an internet connection is required.

Ze Wang et al [2] designed a blockchain-based certificate transparency and revocation transparency system. In this system, the certificate authority (CA) signed the certificate and the revocation status information of the respected certificates are published by the subject (Certificate Authority). Public logs are used to monitor the CAs operation. This system was implemented with Firefox and nogix. This system provided the trust but Certificate validation is delayed and a false sense of security.

Madala et al [3] used the Hyper ledger Fabric blockchain platform. In this system, the certificates are issued by CAs only by obtaining approval from the domain owner Certificate Transparency (CT) technique, invented by Google. The aim to prevent SSL/TLS CA from issuing certificates for a domain without visible to the owner of the domain. But there was low scalability and less transaction.

Ai song Zhang et al [4] designed a system based on consortium blockchain technology. They used a secret sharing scheme. It can validate the digital certificate to protect the user's information and also the property of the user. The digital certificate revocation lists have collaborated among the CAs.

The trust and reliable CRL (Certificate Revocation List) are more compared with the traditional system. If the user wants to verify the certificate, they only need to decrypt the signature with the public key. And the result will be compared with the hash operation of the original message. If the result is consistent, it proved that the digital certificate not tampered. But there is a false sense of security.

Macro Baldi etal [5] designed a system named certificate validation through public ledgers and blockchain. In this system, CRLs (Certificate Revocation List) were distributed through the use of a private blockchain, and it shared among CA (certificate authority). CAs are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs. The certificate revocation list was available and authentication was provided at any time for a certificate. The certificate revocation list for a set of the certificate was maintained by the same certification authority who issued the certificates. CA ecosystem is fragile and prone to compromise.

III. OBJECTIVES OF THE PROPOSED SYSTEM

By using the unmodifiable property of blockchain provide more security. Confidentiality is transparent with each transaction visible to all the peers. Our application runs in offline mode. The certificate is validated rapidly. Provide accurate and reliable information

IV. PROPOSED SYSTEM

A. Methodology

In this proposed system the academic, sports certificates are converted into digital certificates using sampling and quantization. Then the certificates are added with the hash values generated for the digital certificate and store it into the blocks. The chaotic algorithm used for generating the hash value. Each block consists of the hash value, timestamp, and hash value of the previous block. These blocks are linked together in the form of blockchain. The institution registers the student details in our interface (application) by providing details like name, email id and these are stored in the database. The certificate issued by the registrar is stored in the application and they form a blockchain. The employer or verifier can validate the certificate by entering the student details.

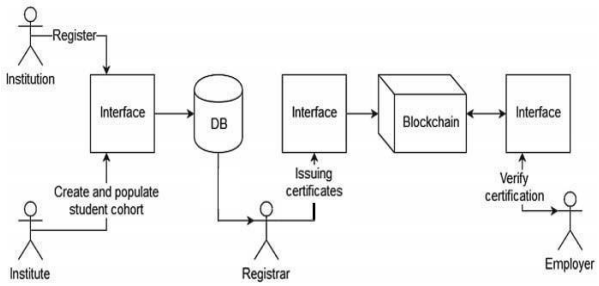

Fig 1: Architecture of the proposed system

B. Digital Certificate Creation

In this, the student certificates are converted into digital certificates. The academic certificate and sports certificate are issued by the institution are stored in the database. By using the analog image to digital image conversation method, the certificate can be converted into a digital certificate. The value 0's and 1's are created for each certificate. In a digital image, all the coordinates on 2-d function and the corresponding values are finite. Each value considered a pixel. By using admin login, the administrator login to our application to upload the student's certificate in the application then it will convert an analog image to digital image using sampling and quantization. The next page of the application shows the add student and add a certificate. If an admin tape the add student, the new student gets registered. If an admin clicks the added certificate, the student certificate is uploaded.

C. Hash Code Generation

The chaotic algorithm is used to generate the hash value for the certificate. This algorithm takes input in different size and produces the output in a fixed size. This algorithm needs to define the mapping scheme, initial condition, and parameters. Verifying process is started by using the same initial condition and parameters to generate the same output. When the certificate is uploaded, the hash value is created for the digital certificate. Compared to SHA-1, the chaotic hash function are collision- resistant.

D. Digital certificate validation

In this, the created digital certificate is validated. Certificates that are stored in the blockchain are validated by matching the hash value. The verification of the hash value of the certificate is used to avoid tampering. The employer or verifier can log in to the application using their login id and password. They can select and certificate type which they want to validate. Then tape the validate button in the application. If the certificate is original the output will be a valid certificate and success. If the certificate is not original or modified the output will be error and modified certificate.

E. Working of Application

In our application the first page is admin login, the next page consists of add student and certificate and last verifier page. The admin can log in to our application using the admin login id and password. Then the admin can add the student and their certificates by tap the add student and add certificate button. Next, the verifier can validate the certificate using the verifier login id and password. They provide the login id of the student and select the certificate type and tap the verify button. If the uploaded certificates are original then the result will be a success. Otherwise, the result will be error and modified.

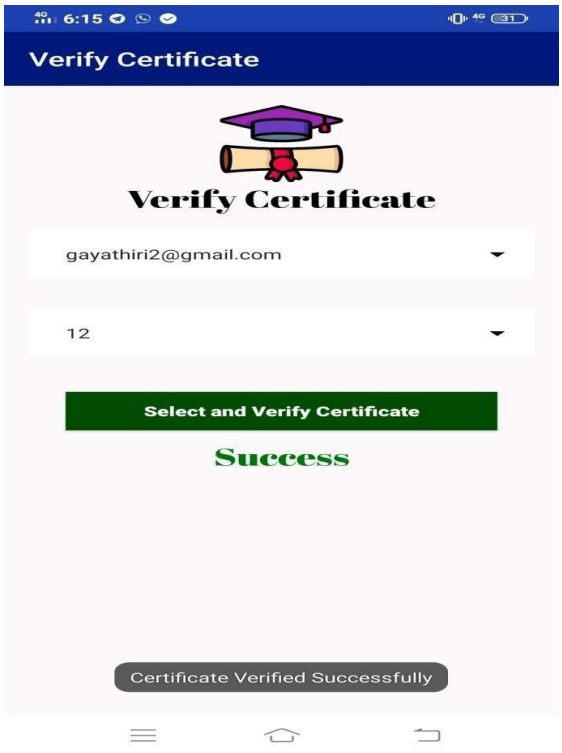

Fig 2: Blockchain successful verification of original certificate

D. SAMPLE CODE:

"""
Verify blockchain certificates (http://www.blockcerts.org/) Overview of verification steps
- Check integrity: TODO: json-ld normalizatio
- Check signature (pre-v2)
- Check whether revoked
- Check whether expired
- Check authenticity """
import json
from cert_core import to_certificate_model from cert_verifier import connectors
42

```
from cert_verifier.checks import create_verification_steps
import sys
def verify_certificate(certificate_model, options={}): # lookup issuer-hosted information
issuer_info = connectors.get_issuer_info(certificate_model) # lookup transaction information
connector = connectors.createTransactionLookupConnector(certifica te_model.chain, options)
transaction_info = connector.lookup_tx(certificate_model.txid) # create verification plan
verification_steps = create_verification_steps(certificate_model, transaction_info, issuer_info, certificate_model.chain)
verification_steps.execute()
messages = []
verification_steps.add_detailed_status(messages) for message in messages:
print(message['name'] + ',' + str(message['status'])) return messages
def verify_certificate_file(certificate_file_name, transaction_id=None,
options={}):
with open(certificate_file_name, 'rb') as cert_fp: certificate_bytes = cert_fp.read()
certificate_json = json.loads(certificate_bytes.decode('utf-8'))
certificate_model = to_certificate_model(certificate_json=certificate_json,
txid=transaction_id, certificate_bytes=certificate_bytes)
result = verify_certificate(certificate_model, options) return result
if __name____== "__main__":
if len(sys.argv) > 1:
for cert_file in sys.argv[1:]: print(cert_file)
result = verify_certificate_file(cert_file) print(result)
else:
result = verify_certificate_file ('../tests/data/2.0/valid. Son')
print(result)
```

F. Algorithm Description

Step 1: Certificate Creation by Issuing Authority

The process begins with an authorized institution (such as a university or professional body) generating a digital certificate for a student or professional. This certificate includes important details such as the recipient's name, certificate type, date of issue, and unique identification number. To ensure data privacy and security, the contents of the certificate are hashed using a cryptographic hash function (e.g., SHA-256). This hash uniquely represents the certificate without exposing its full content.

Step 2: Storing the Certificate Hash on the Blockchain

Once the certificate hash is generated, the issuing authority creates a blockchain transaction. This transaction contains:

- The hashed certificate data.
- Metadata such as the issuer's public key, timestamp,and certificate ID.

The issuing authority signs this transaction with its private key, ensuring authenticity. This transaction is then broadcasted to the blockchain network, where it is verified and stored in a block by participating nodes (miners). Once confirmed, the certificate's existence and authenticity are permanently recorded on the blockchain.

Step 3: Certificate Distribution and Access

The original digital certificate (in PDF or XML format) is either given to the certificate holder or stored securely on a decentralized storage platform (such as IPFS). A link or access token pointing to the stored certificate is

shared with the user. The blockchain's transaction ID or block reference is also associated with the certificate for future verification.

Step 4: Verification of Certificate

When a third party (e.g., employer or university) wants to verify the certificate, they are given access to both the digital certificate and the transaction ID on the blockchain. The verifier performs the following:

- They hash the received certificate using the same hash function.
- They retrieve the original hash from the blockchain using the transaction ID.
- They compare the two hashes:
  - If the hashes match, the certificate is verified as authentic and untampered.
  - If the hashes do not match, the certificate is considered invalid or altered.

Step 5: Result Generation

The system generates a clear verification result — either "Valid Certificate" or "Invalid/Forged Certificate" — based on the hash comparison. This ensures that only genuine, untampered certificates are accepted.

Benefits of This Algorithm

- **Tamper-Proof**: The immutable nature of blockchain ensures the certificate cannot be altered after issuance.
- **Decentralized Trust**: No central authority is needed for verification; trust is distributed across the blockchain network.
- **Real-Time Verification**: Any stakeholder can verify the certificate at any time using the blockchain.
- **Prevents Forgery**: Malicious actors cannot duplicate or alter certificates without being detected.

Result Representation:

- The implementation of blockchain technology in certificate authentication resulted in significant improvements in security, transparency, and verification speed. The key outcomes are as follows:
- **Improved Security**
  - Certificates stored on the blockchain were immutable and tamper-proof.
  - Cryptographic hashing ensured that any unauthorized modifications were easily detectable.
- **Enhanced Verification Process**
  - Verification time reduced from several hours/days (manual process) to a few seconds via blockchain lookup.
  - Third-party verification was no longer necessary, enabling direct and trustless validation.
- **Transparency and Traceability**
  - All issued certificates could be publicly verified without compromising private data.
  - A complete and transparent audit trail was maintained on the blockchain ledger.
- **Elimination of Forged Certificates**
  - Forgery attempts were unsuccessful due to the unique blockchain hashes.
  - Institutions and employers could easily distinguish between genuine and fake certificates.
- **Decentralized Control**

  - Authority over certificate issuance and verification was distributed, reducing dependency on a central body.

  - Multiple educational institutions or authorities could participate in a shared ledger system.

- **Scalability and Integration**
- The system was scalable and compatible with various blockchain platforms such as Ethereum and Hyperledger. API-based integration allowed seamless incorporation into isting institutional systems.

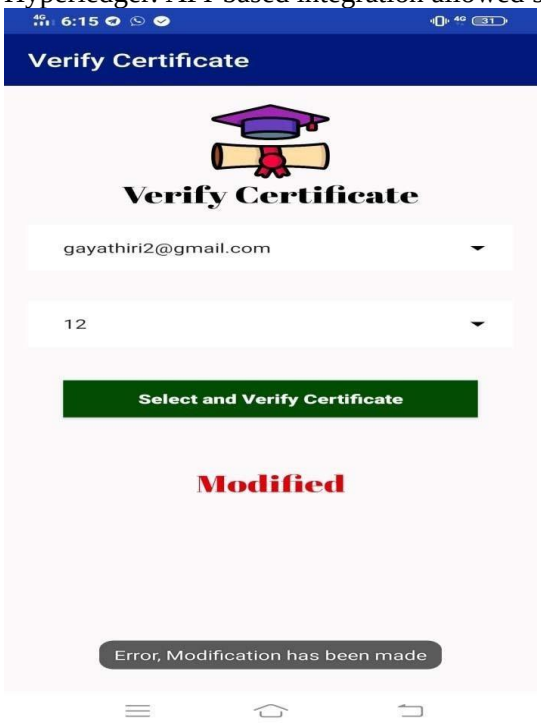

Fig 3: Blockchain successful verification of modified certificate

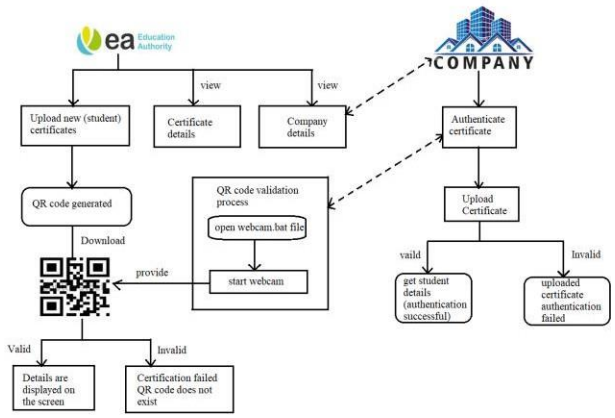

Fig.4: System Architecture Design

DATA FLOW DIAGRAM:

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.

2. The data flow diagram (DFD) is one of the most important modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.

3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied

as data moves from input to output.

4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

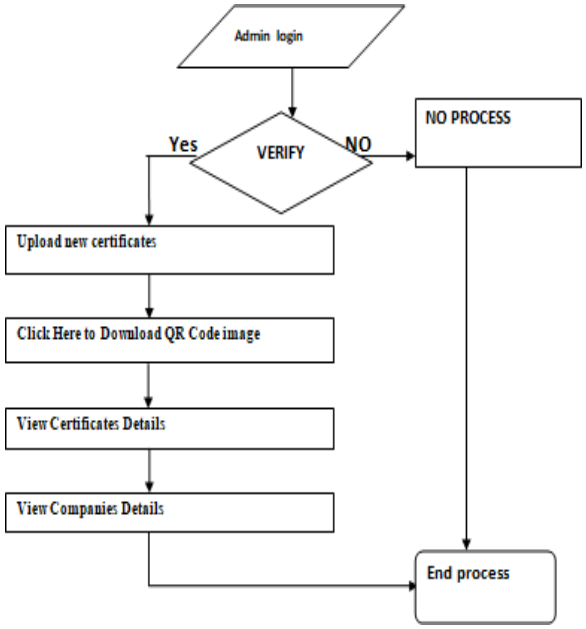

Fig.4: Data Flow Diagram

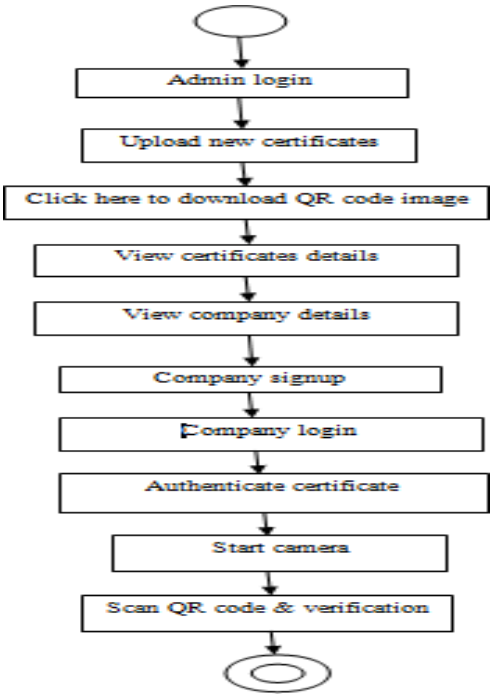

Fig. 5: Activity Diagram

V. CONCLUSION

In this paper, we proposed a solution to the problem of certificate forgery based on blockchain technology. Providing security to the data is very important. By using the unchallengeable property of blockchain, we can provide more security for data and reduce the certificate forgery. The application can allow the user to view and validate the certificate. This system guarantees information accuracy and security and easy for people to manage digital certificates.

REFERENCES

1. **Verifi-Chain: A Credentials Verifier using Blockchain and IPFS**
Rahman et al. propose a prototype for academic credential verification leveraging blockchain and IPFS to ensure tamper-proof and non-repudiable certificates.

2. **NFTCert: NFT-Based Certificates With Online Payment Gateway**
Zhao and Si introduce a framework that utilizes NFTs for certificate issuance, incorporating an online payment gateway to facilitate broader adoption.

3. **E-Certificate Verification Using Blockchain**
Singh and Chana discuss a secured academic certificate verification system using blockchain to prevent fraud and enhance trust.

4. **A Consortium Blockchain-Based Platform for Academic Certificate Verification**
Tran et al. present a platform that employs consortium blockchain for verifying academic certificates, aiming to streamline the verification process.

5. **Utilizing Blockchain Technology for University Certificate Verification System**
Oluwaseyi and Akinyede explore the implementation of blockchain technology to authenticate university certificates, addressing issues like fraud and inefficiencies.