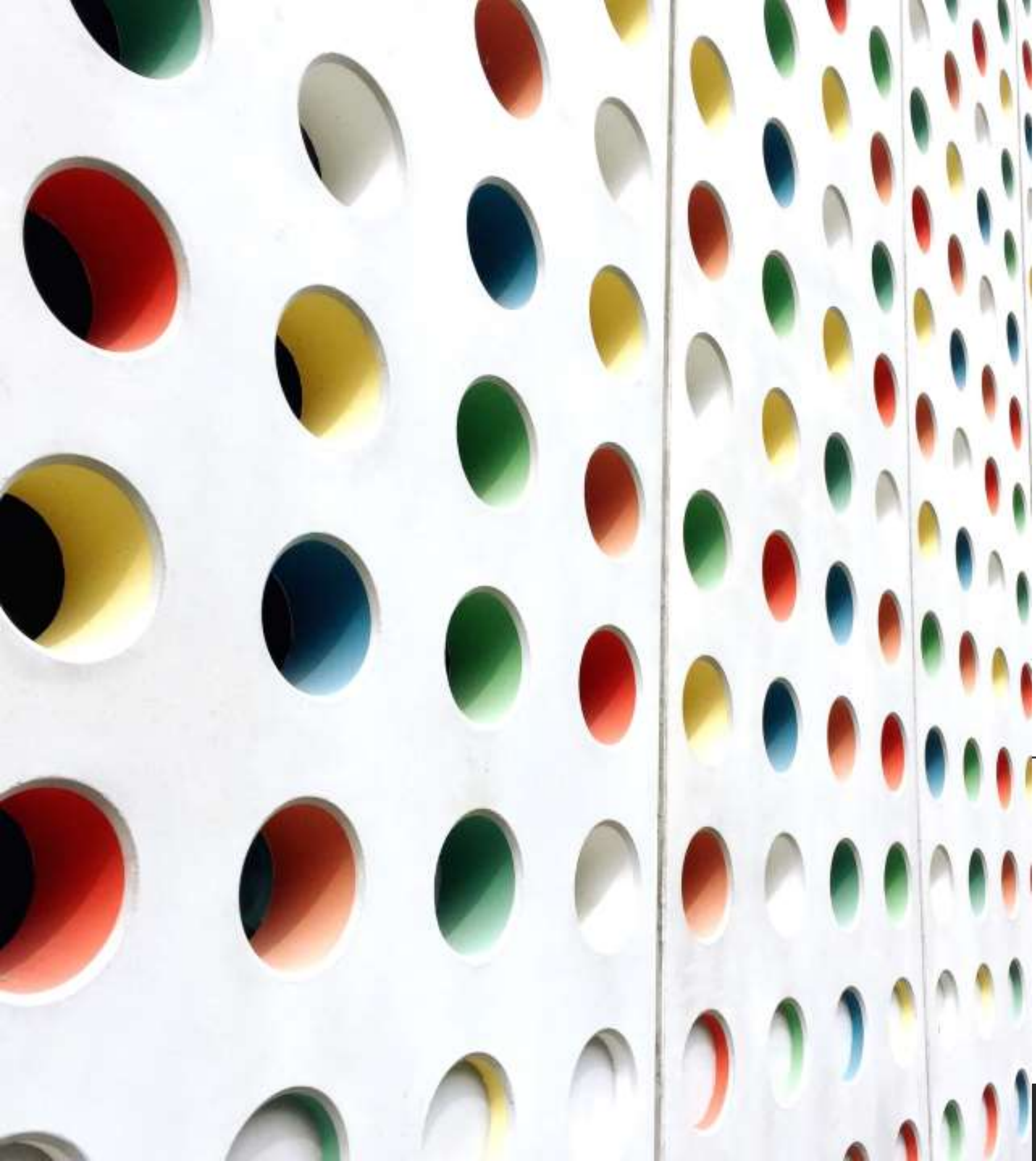


BLCOCKCHAIN BASED CERTIFICATE GENERATION AND VALIDATION

Submitted by,

NAME: KRISHNAVENI M

REG NO: 95072252018

Guide: J.Anciline Jenifer
MCA,M.Phil.(Ph.D)

ABSTRACT

Certificate verification system is a designed to computerize the process of adding certificates and verifying the certificates records using blockchain technology. Our project will help to store the certificate and provide security. The objective of the certificate portal project is to provide users with a streamlined and efficient platform for obtaining, managing, and verifying certificates. It has easy maintenance of information as well as time saving and reduction in operation. The system designed in HTML, CSS, JS and Python is interactive, backend php, it is a user friendly. It provides information about certificates. Most certificates operations are recorded and stored in the computer and retrieved at will. It ensures security as the user must login before and any certificate is added or printed.

EXISTING SYSTEM

The certificate are stored in centralized manner and verified manually. So it takes too much time to verify. There is no safety to the certificate that are given to any private sectors (banks). But the data may be changed, deleted or modified. Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates. There is no digitalized way to verify the certificate. Although there are some universities that store certificates in digital form but are also in a centralized network where there is a chance of tampering the certificate. This may increase the cases of fraud since there is no means of security and integrity of the data both in manual and in digital form.The employers verify the students credentials using third party lot of money and time consuming too.

PROPOSED SYSTEM

In this proposed system. Students login the portal and added our certificates. The consensus algorithm is used for generating the hash values. In the Blockchain, each block consists of hash value, timestamp, previous hash value and they connected together. The user verifies the certificates by using the login id and password of the student . Students can view their certificates by logging in to their account. we provide a platform to store and verify the student credentials using blockchain technology. With the help of the unique certificate ID, student can verify the certificate and also the company can verify whether the certificate provided by the student is authorized or not.. The SHA-256 algorithm is used for generating the hash value for the certificates. It accepts input in various sizes and produces a fixed size hash value. When the certificate gets uploaded, the hash value is generated.

LITERATURE SURVEY

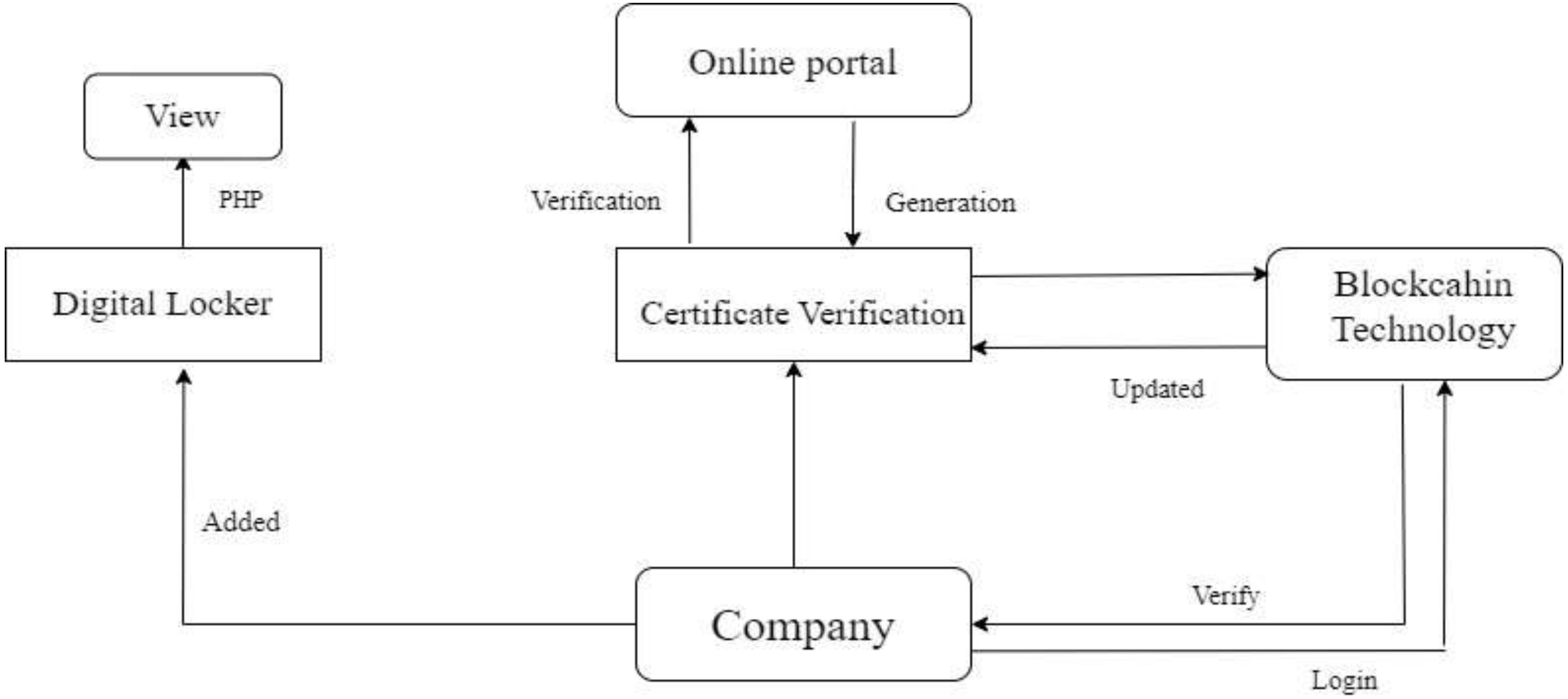
- **“AVNI RUSTEMI et.al.,[1]** This paper explores the transformative potential of blockchain in education, emphasizing its impact on learning methods and certificate verification. It reviews 34 key studies from 2018 to 2022, using the PRISMA framework.
- **Gayathiri, A., Jayachitra, J., & Matilda, S (2020).et.al.,[2]** In 2018-19, 26.3 million Indian students enrolled in higher education, with nearly 9 million graduates annually. Manual tracking and validation of numerous certificates pose challenge
- **A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, et.al.,[3]** The Indian Ministry of Education highlights the complexity and challenges in document verification due to the lack of an effective anti-forgery mechanism, leading to the frequent occurrence of forged graduation certificates.
- **Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and YiHua Chen(2018) et.al.,[4]** Blockchain's progress in recent years has the potential to transform education, offering cost-effective learning methods and reshaping teacher-student interactions
- **J. Clark and P. C. van Oorschot, “SoK: et.al., [5]** With one million graduates annually, compromised security in certificate issuance is a concern. Existing digital certificate systems, while introduced, still face security issues.

- **L. Zhang, D. Choffnes, D. Levin,et al.,[6]** The study emphasizes the importance of blockchain technology in securely recording and managing various types of information such as educational certificates
- **C.K. Wong and S, S. Lam et.al.,[7]** The Indian Ministry of Education highlights the complexity and challenges in document verification due to the lack of an effective anti-forgery mechanism
- **Shanmuga Priya R, et.al.,[8]** The rise of information technology, widespread Internet access, and mobile device usage have transformed human lifestyles. Virtual

RESEARCH METHODOLOGY

The web portal is authenticating a sure third party that validates all documents from the university, school, colleges, etc. Once with success verification has done from university, school, faculties it'll store information into the digital locker and same time it generates the certificate id or name code. Student upload our certificates in digital locker using own username and password. Organizations will submit id to the portal and pool the e-certificate of the various student and build the validation.

ARCHITECTURE DIAGRAM



MODULE DESCRIPTION

Module 1

I have created a portal where you can obtain certificates. In this portal, there is a description of how to receive our certificates. On the next page, you will find a list of available courses. After selecting a course, on the following page, you can fill in your name and other details to generate the certificate. You have the option to download the certificate, and you can also modify or delete it as needed.

Module 2

Now, let's move on to the next module. In this module, you can verify the certificates downloaded in Module 1. We use blockchain technology to ensure that the certificates are authentic. You can check whether the certificate is original or a duplicate, even if it has been received from another location, using this verification process.

Module 3

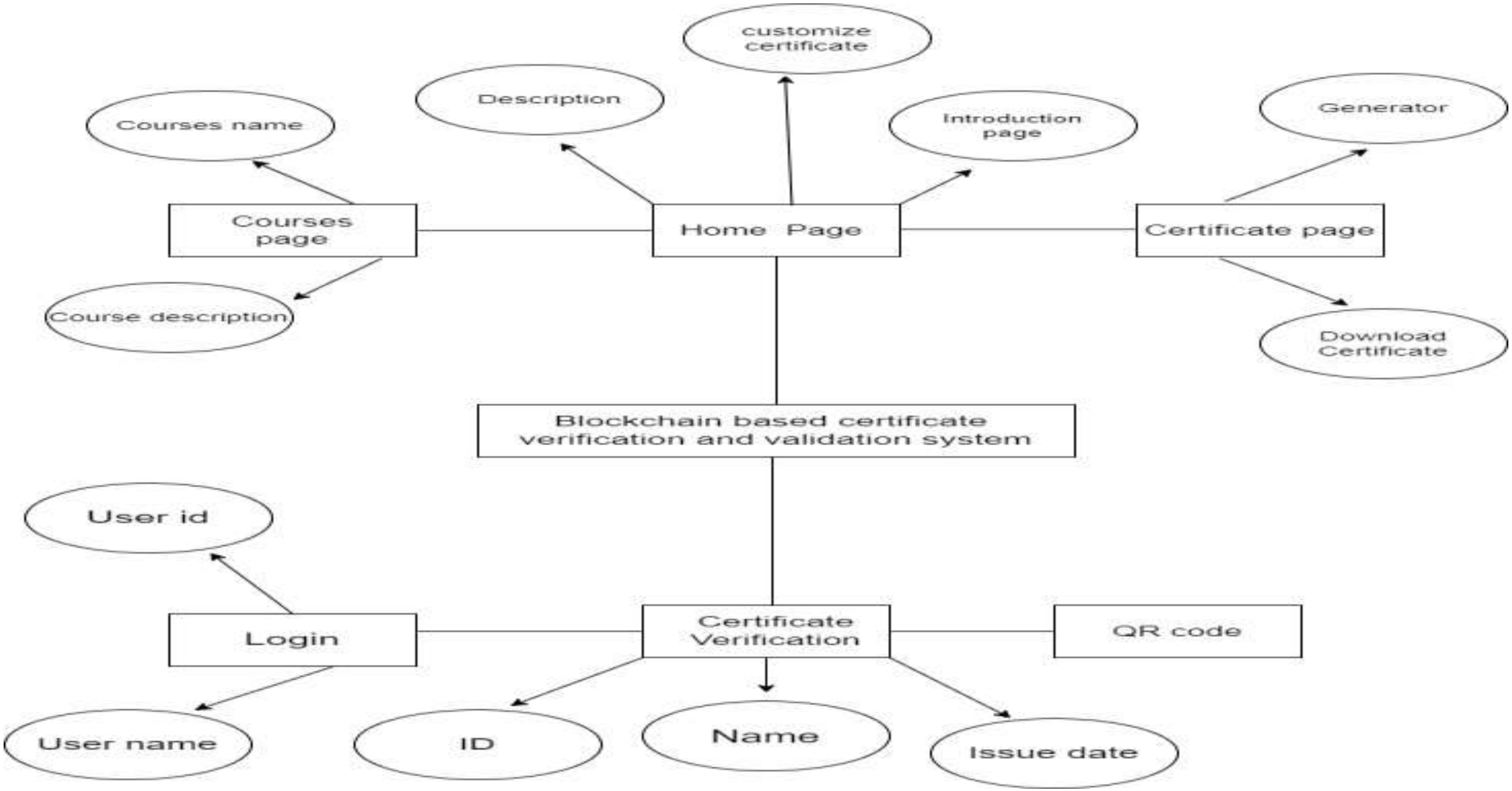
This is the final module description. In this module, I have created a digital locker. This means that I have set up a login page where you can enter your own username and password. Only we will have knowledge of this username and password. After logging in, you can view all of our certificates. Once you're done, you can log out and return to the external interface.

TABLE DESIGN

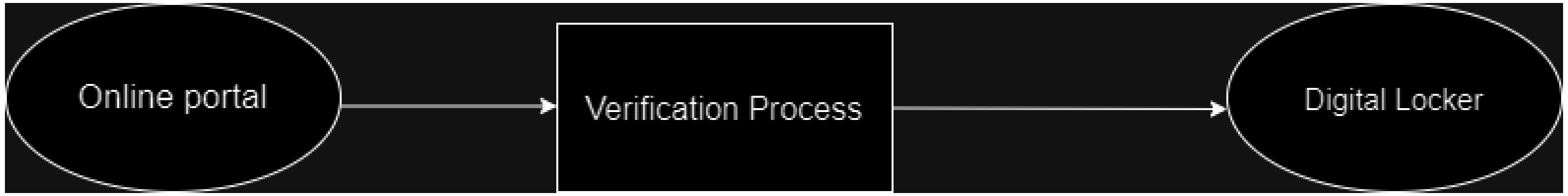
DATABASE NAME: test_db
TABLE NAME: images

S.no	Field name	datatype	constraints
1.	name	Varchar(50)	Not null
2.	id	int	Primary key

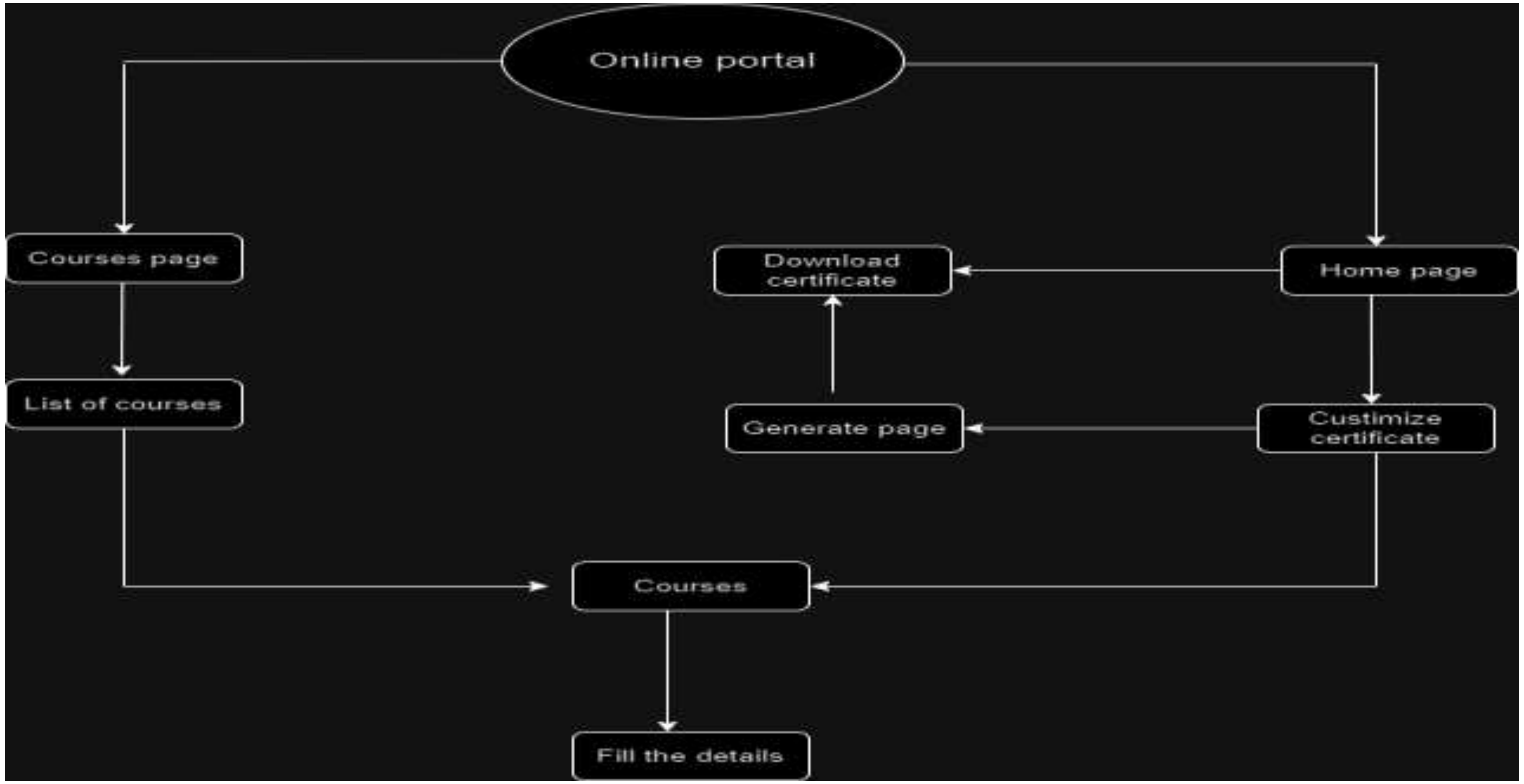
ER DIAGRAM


customize certificate
Description
Courses name
Introduction page
Generator
Courses page
Home Page
Certificate page
Course description
Download Certificate
Blockchain based certificate verification and validation system
User id
Login
Certificate Verification
QR code
User name
ID
Name
Issue date

DATA FLOW DIAGRAM

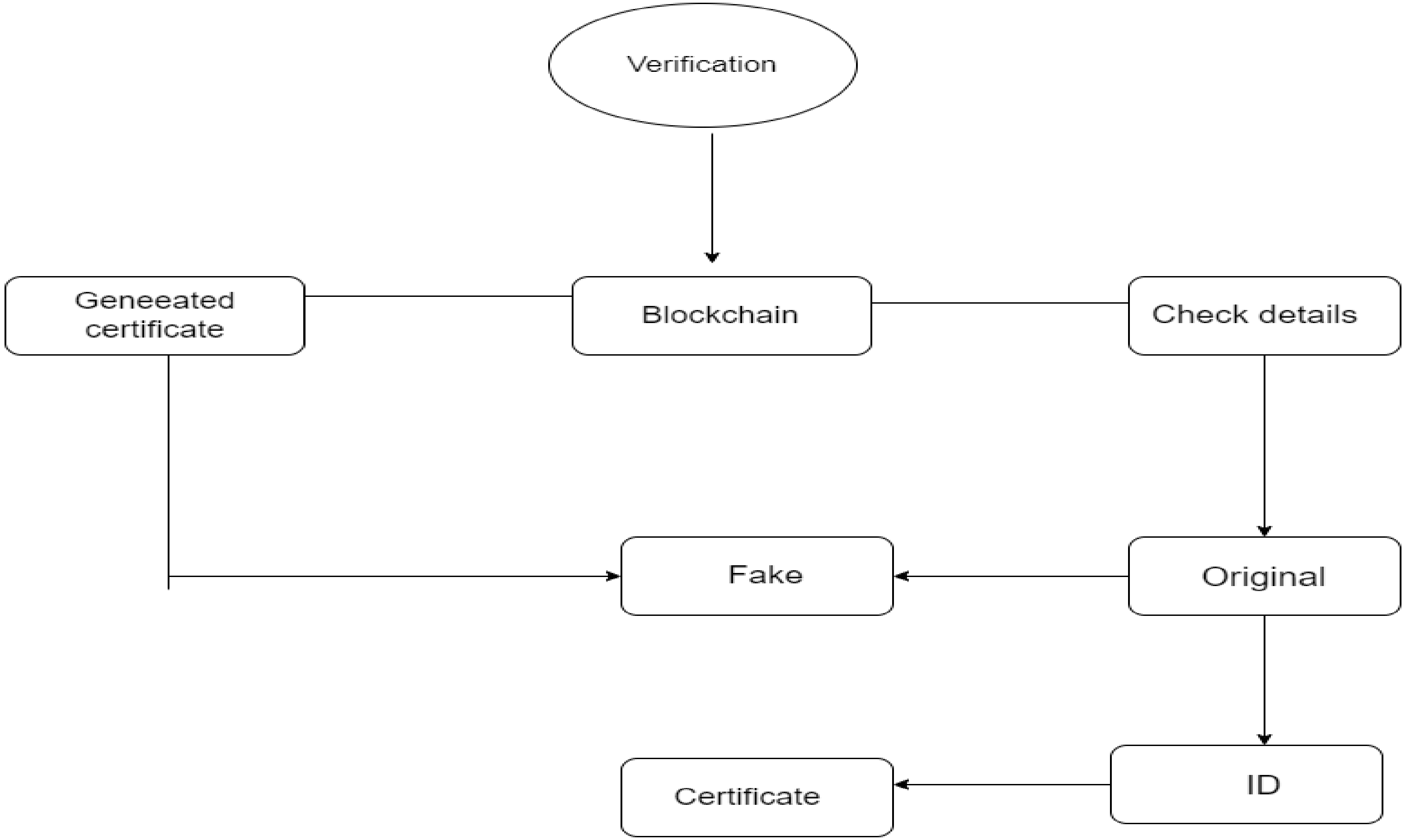


Level 0



Level 1

DATA FLOW DIAGRAM



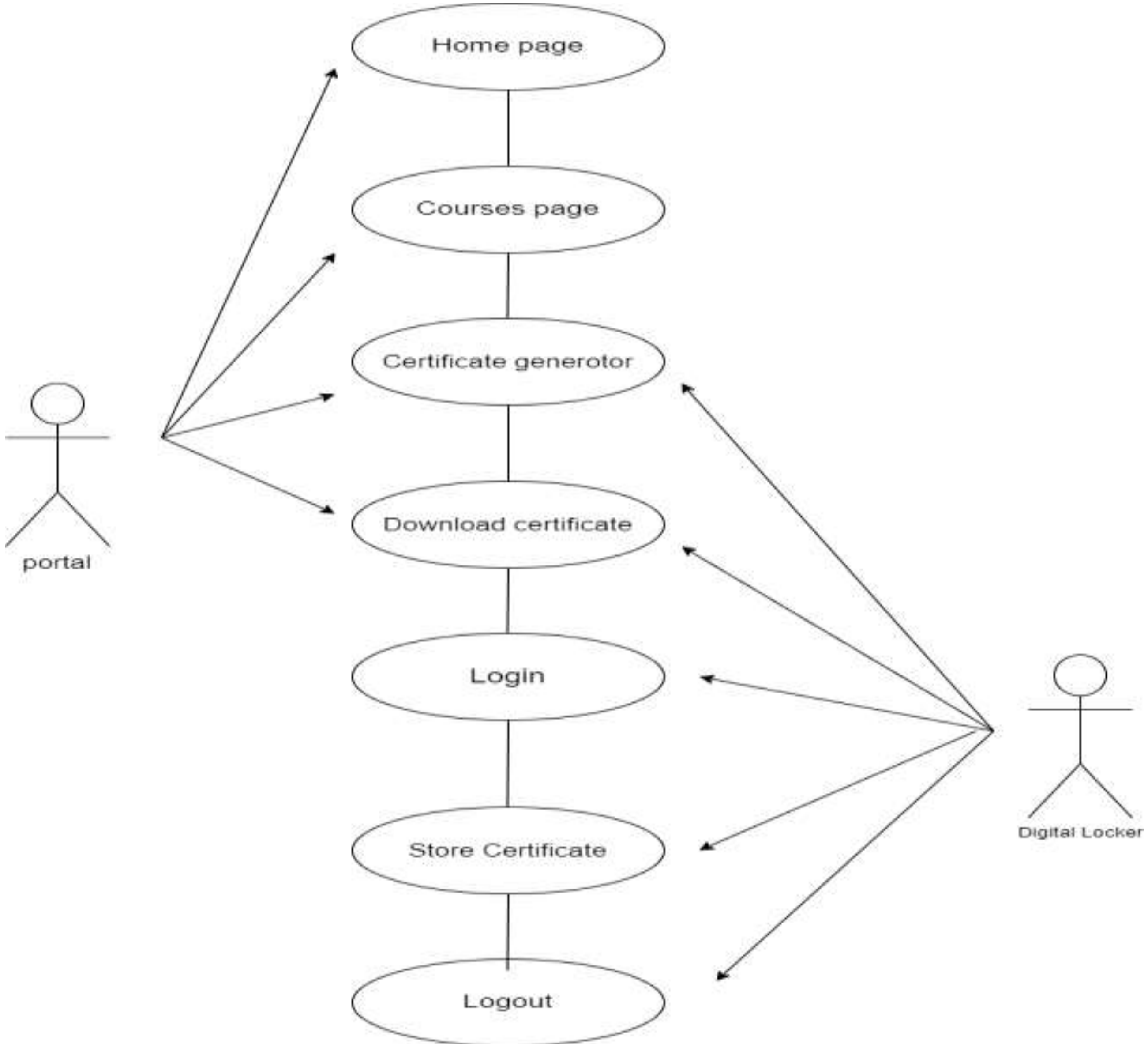
Level 2

DATA DICITIONARY

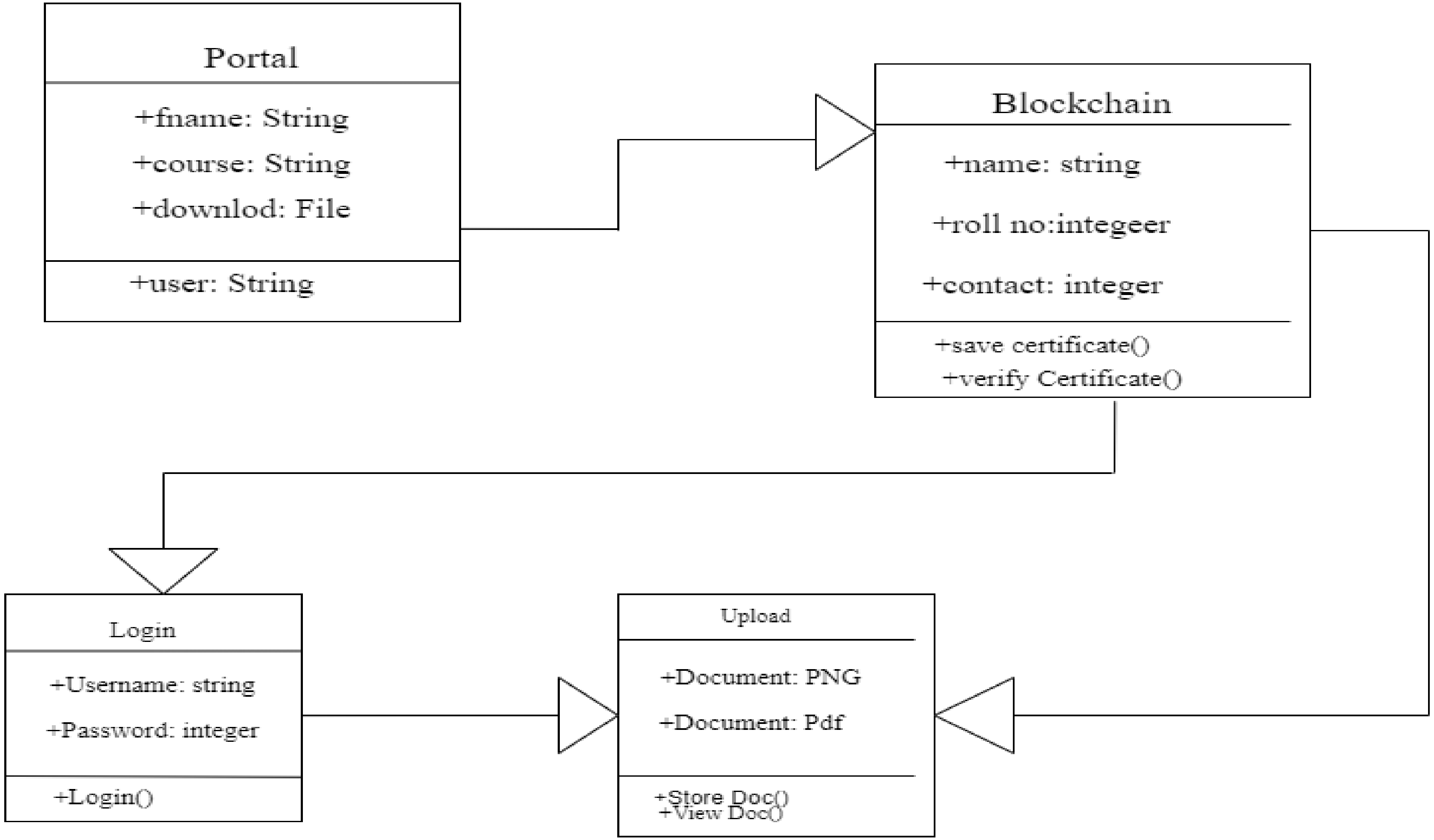
Table Name: test_db
Purpose: Used to view our certificates

Field	Type	Constraints	Description
username	Varchar	Not Null	Private username
password	Varchar	Not Null	Private password
Certificates_in_locker	Varchar	Not Null	Added certificates
Log_data	varchar	Not Null	Logut the data

USE CASE DIAGRAM



CLASS DIAGRAM



Portal

+fname: String
+course: String
+downlod: File

+user: String

Blockchain

+name: string

+roll no:integeer

+contact: integer

+save certificate()
+verify Certificate()

Login

+Username: string
+Password: integer

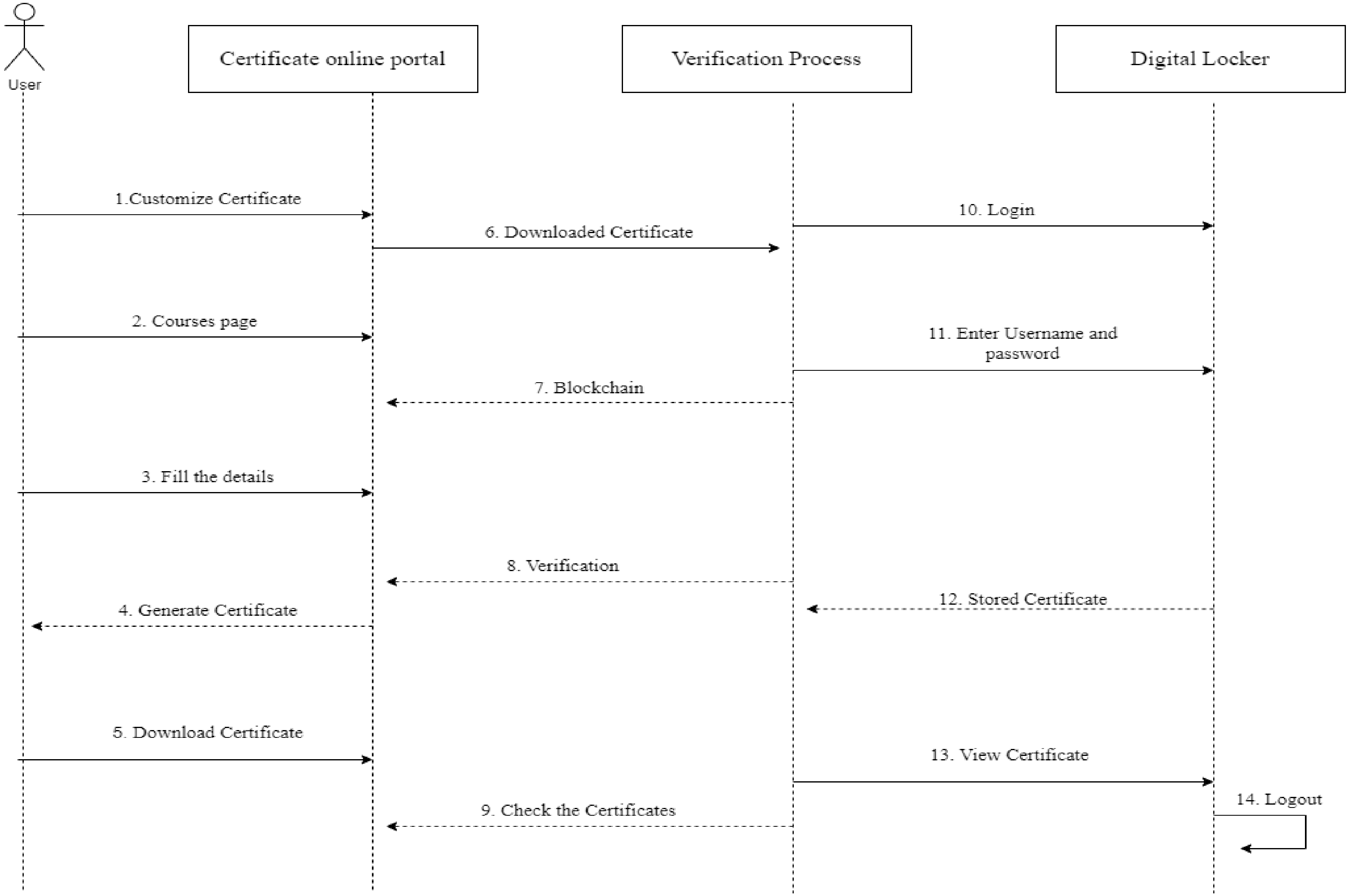
+Login()

Upload

+Document: PNG
+Document: Pdf

+Store Doc()
+View Doc()

SEQUENCE DIAGRAM



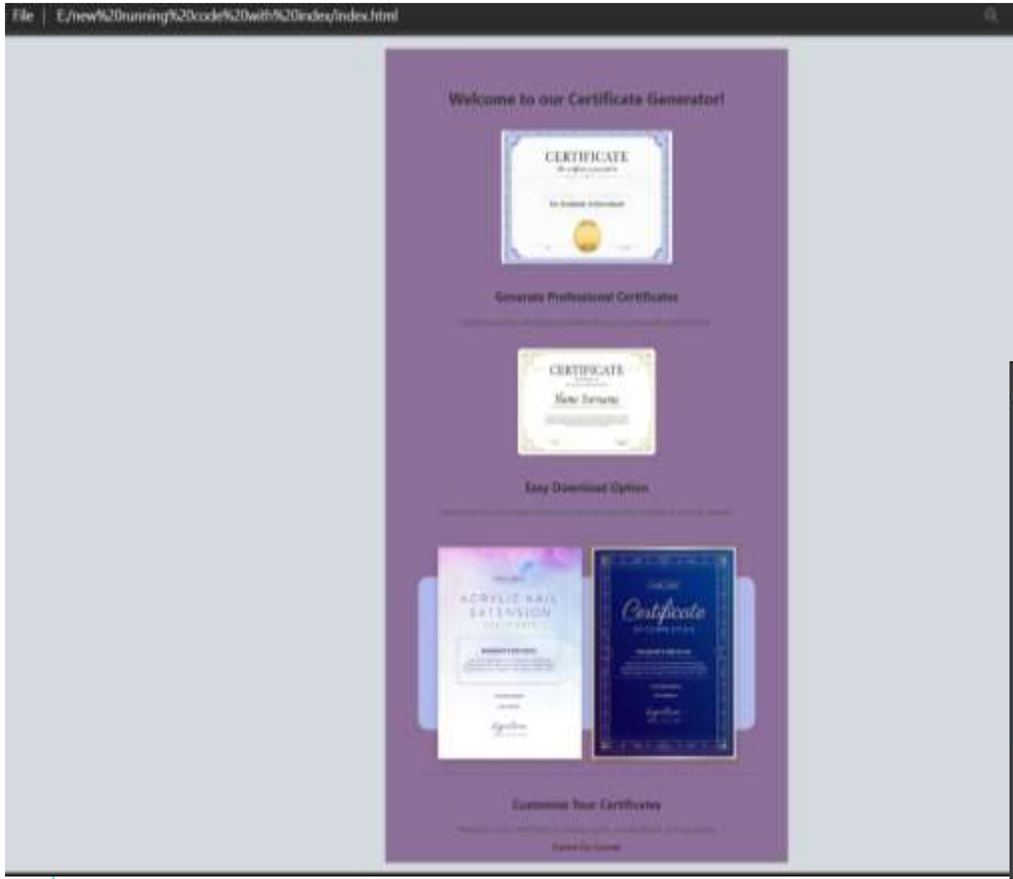
SAMPLE CODING

```
import tkinter as tk
from tkinter import messagebox, filedialog
from hashlib import sha256
import pickle
import os
class Blockchain:
    def __init__(self):
        self.chain = []
        self.transactions = []
    def add_block(self, block):
        self.chain.append(block)
    def add_transaction(self, transaction):
        self.transactions.append(transaction)
class Block:
    def __init__(self, index, previous_hash, transactions):
        self.index = index
        self.previous_hash = previous_hash
self.transactions = transactions
•           self.hash = self.calculate_hash()
```

```
def calculate_hash(self):
        return sha256(str(self.index).encode() + str(self.previous_hash).encode() +
str(self.transactions).encode()).hexdigest()
def save_certificate():
    filename = filedialog.askopenfilename(initialdir="certificate_templates")
    if filename:
        with open(filename, "rb") as f:
            bytes_data = f.read()

        roll_no = roll_no_entry.get()
        name = name_entry.get()
        contact = contact_entry.get()
filename = filedialog.askopenfilename(initialdir="certificate_templates")
    if filename:
        with open(filename, "rb") as f:
            bytes_data = f.read()
        digital_signature = sha256(bytes_data).hexdigest()
        for block in blockchain.chain:
            if digital_signature in block.transactions:
                messagebox.showinfo("Verification Successful", "Certificate is oriinal.")
                return
        messagebox.showerror("Verification Failed", "Certificate is fake.")
# Initialize the blockchain
blockchain = Blockchain()
# Create GUI
root = tk.Tk()
root.title("Blockchain Based Certificate Verification System")
root.geometry("600x350")
```

SAMPLE SCREENS



File | E:/new%20running%20code%20with%20index/index.html

Welcome to our Certificate Generator!

Generate Professional Certificates

[illegible]

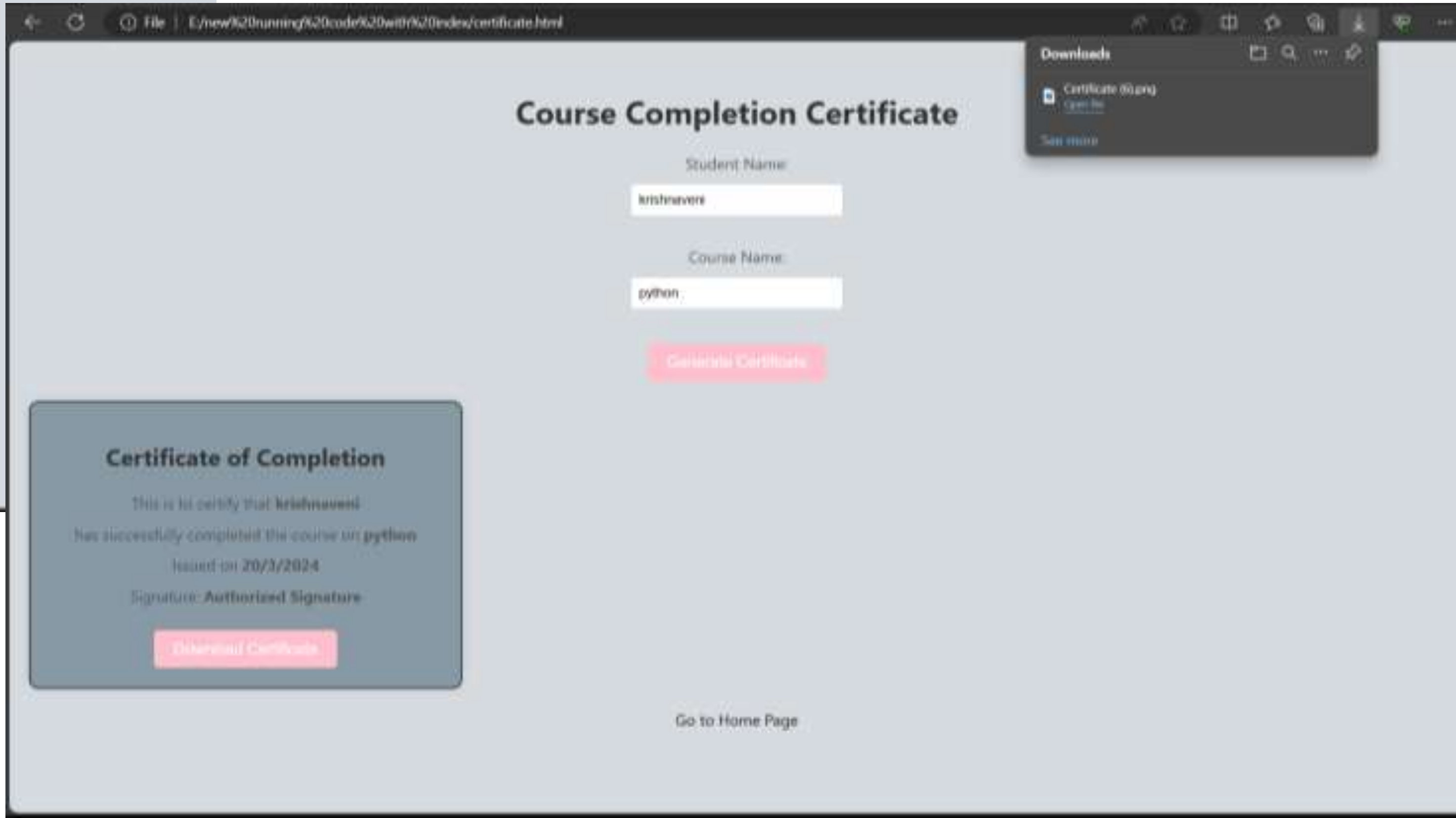
Easy Download Option

[illegible]

Customize Your Certificates

[illegible]

Home page



File | E:/new%20running%20code%20with%20index/certificate.html

Course Completion Certificate

Student Name:

krishnaveni

Course Name:

python

Certificate of Completion

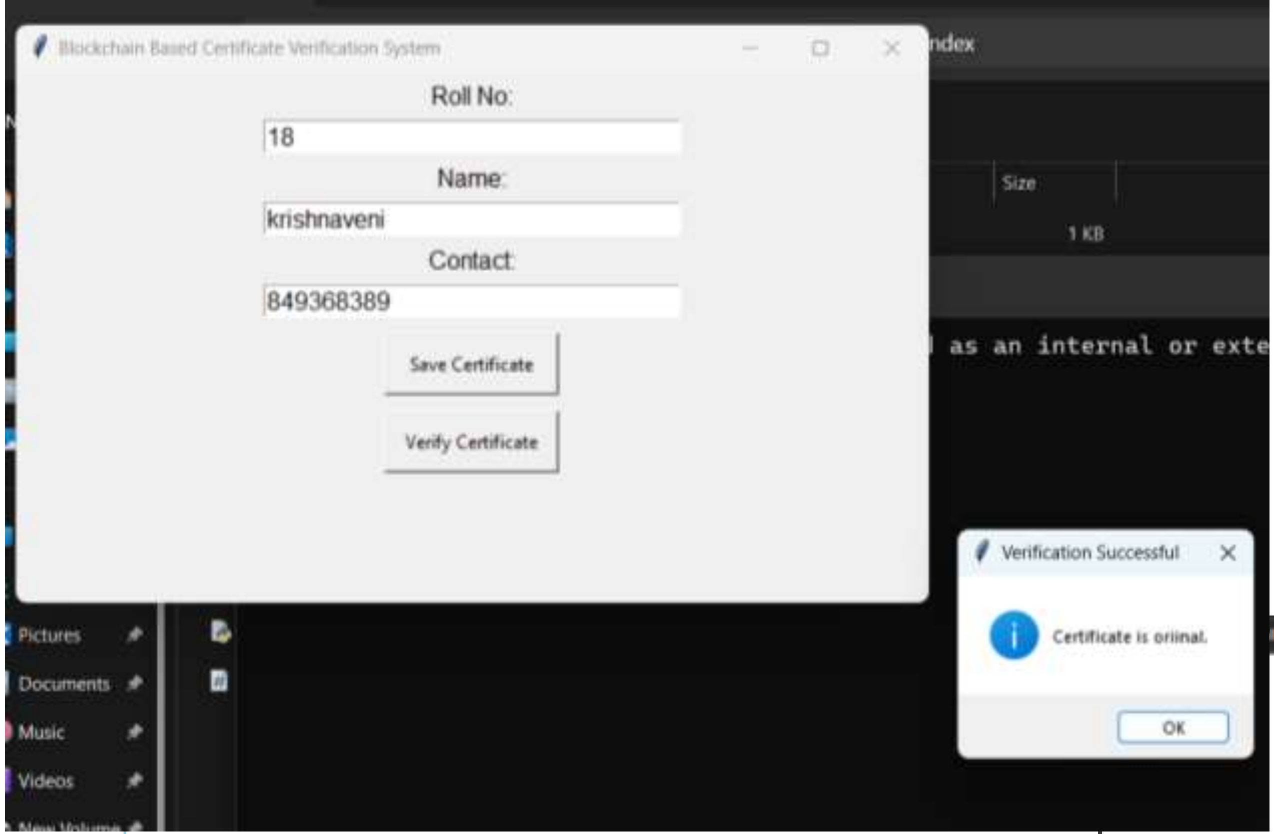
This is to certify that **krishnaveni**

has successfully completed the course on **python**

Issued on **20/3/2024**

Signature: **Authorized Signature**

Certificate generation page



Roll No: 18

Name: krishnaveni

Contact: 849368389

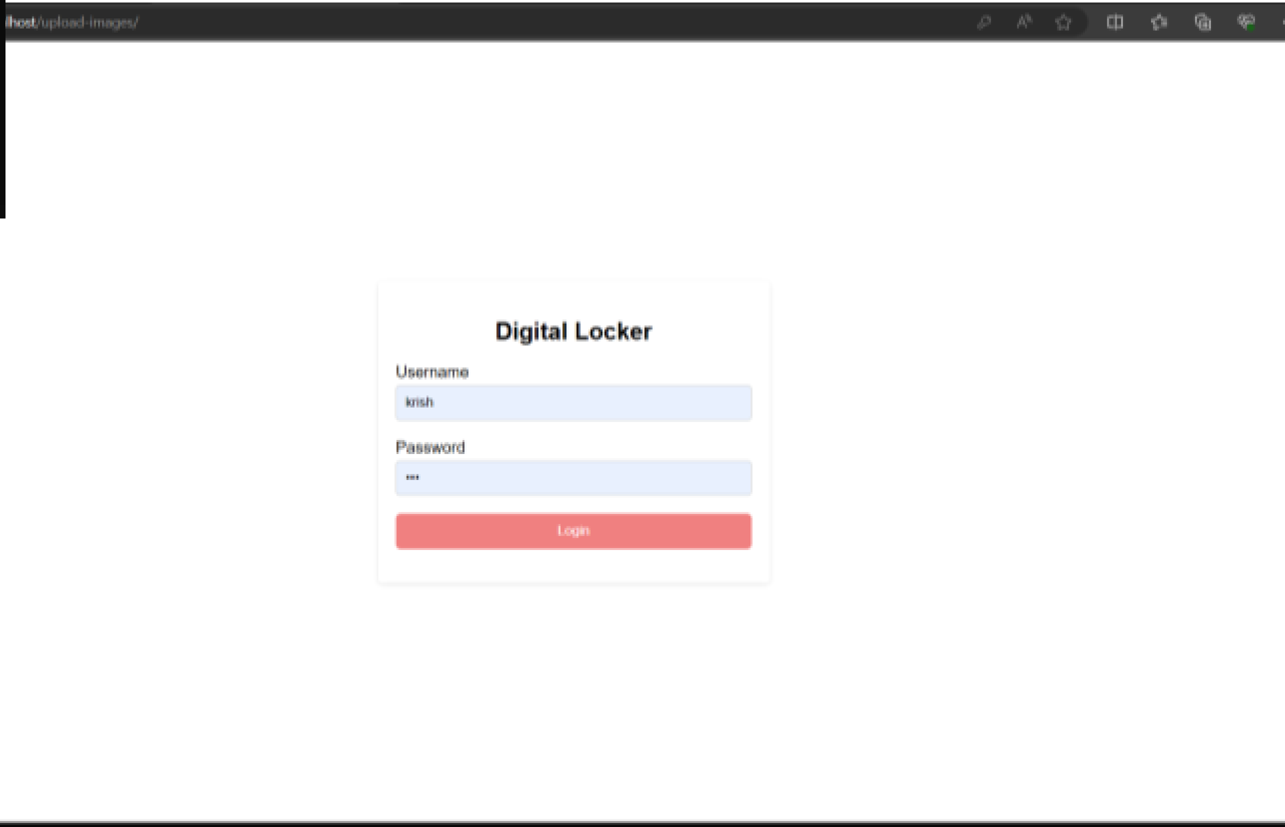
```
as an internal or exte
```

Verification Successful

Certificate is orinal.

OK

Check certificate page

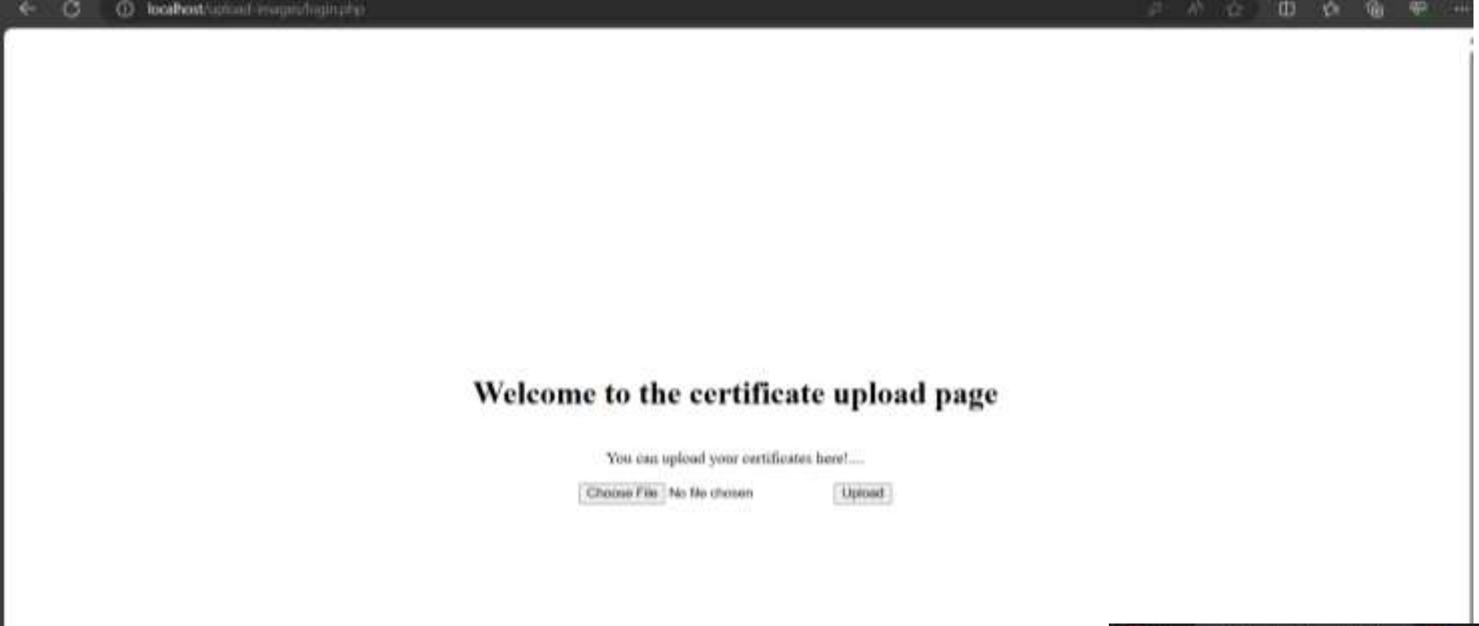


Digital Locker

Username: krish

Password: •••

User Login page

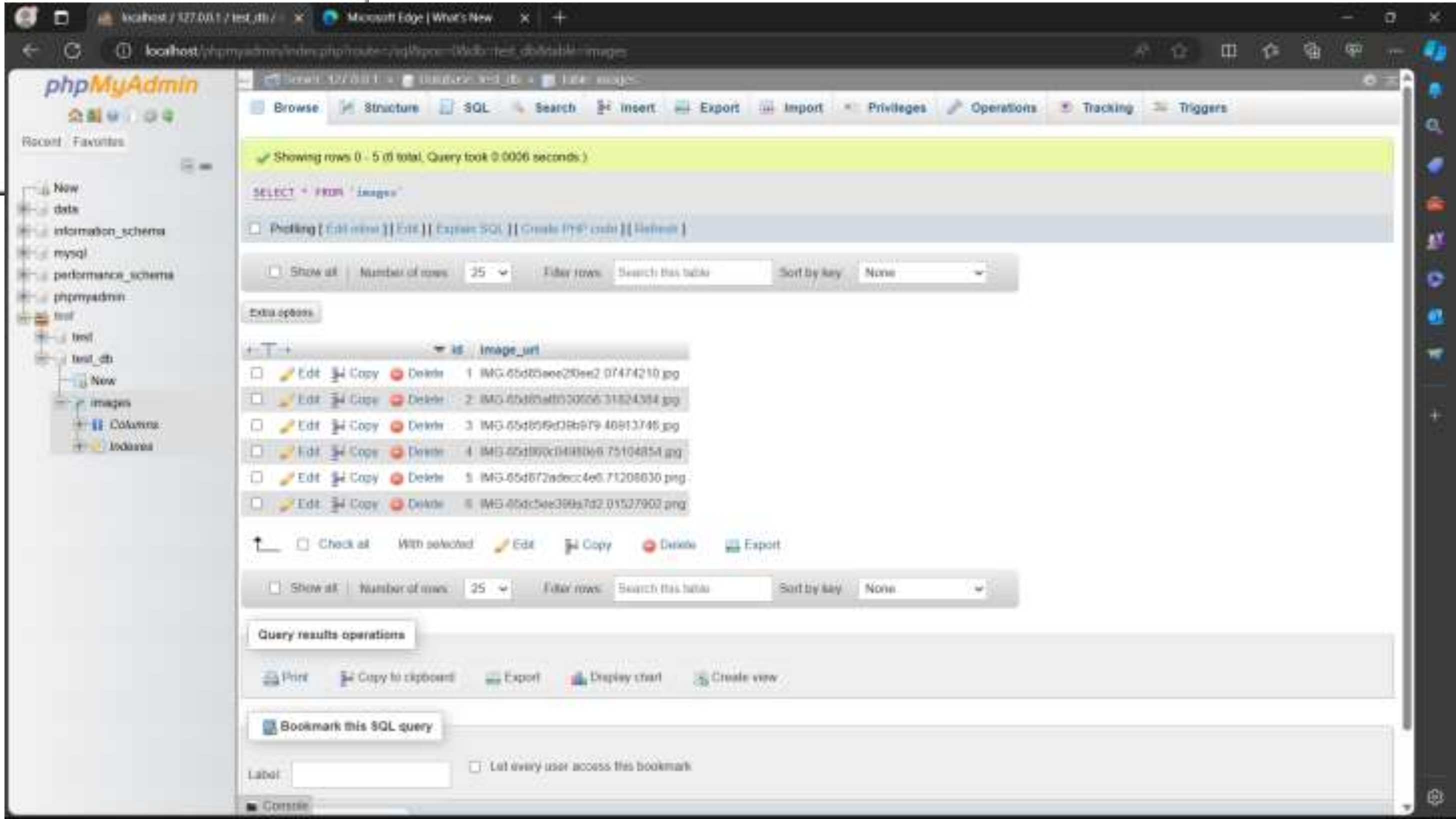


localhost/upload-images/login.php

Welcome to the certificate upload page

You can upload your certificates here!.....

Upload page



Showing rows 0 - 5 (6 total, Query took 0.0006 seconds.)

```
SELECT * FROM `images`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
Show all
Number of rows: 25
Filter rows: Search this table
Sort by key: None
Extra options

id	image_url
1	IMG-65d85aee2f0ee2.07474210.jpg
2	IMG-65d85af8530656.31824384.jpg
3	IMG-65d85f9d39b979.46913746.jpg
4	IMG-65d860c04480e6.75104854.jpg
5	IMG-65d872adecc4e6.71208830.png
6	IMG-65dc5ee399a7d2.01527902.png

Database page

ALL TESTING METHODS

Unit Testing:

- Test each individual component of the portal such as certificate generation, course selection, certificate modification, verification process, login/logout functionality, etc.
- Ensure that each component functions correctly and produces the expected output.

Integration Testing:

- Test the integration between different modules of the portal.
- Verify that data flows smoothly between the certificate generation module, verification module, and digital locker module without any loss or corruption.

Performance Testing:

- Test the performance of the portal under different load conditions.
- Evaluate the response time of various functionalities such as certificate generation, verification, login/logout, etc.

Black box testing

- Black box testing for this project involves verifying the functionality of the certificate portal without inspecting its internal workings.
- Testers interact with the portal as end-users, ensuring that they can easily navigate through the steps to obtain, generate, download, modify, and delete certificates.

White box testing

- white box testing involves scrutinizing the underlying code and database structure of the portal.
- Testers review the backend logic to ensure secure storage and handling of certificate data, proper authentication mechanisms for the digital locker, and robust error handling to prevent unauthorized access or data breaches.

CONCLUSION

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data.Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security. By integrating Blockchain technology, we will able to eradicate the problem of fake certificates . We can view our certificates from anywhere at any time. The application provides accurate and reliable information of digital certificates.

FUTURE ENHANCEMENT

In my project, I aim to automate all processes, including certificate generation, verification, and upload, as well as enhance the interactivity and user-friendliness of the website.On the course page, users will find a list of courses, and upon selecting a course, they will have access to its syllabus, videos, quizzes, and assignments. Furthermore, I will implement additional security measures to ensure high levels of protection.Additionally, I will customize the certificates to meet specific requirements.

PUBLICATION

- S. Rampriya; M. Krishnaveni; J. Anciline Jenifer; ”**Blockchain based certificate generation and validation**”, In conference proceedings of International Conference On Computational Intelligence and Communication (ICICIC, 5 April 2024) Organized by the Department of MCA and AI&DS, Francis Xavier Engineering College

REFERENCES

- [1] “AVNI RUSTEMI 1,2, FISNIK DALIPI 3“. A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification."
- [2] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, The Proposal of a Blockchain-based Architecture for Transparent Certificate Handling
- [3] Gayathiri, A., Jayachitra, J., & Matilda, S (2020). Certificate validation using blockchain. 2020 7th International Conference on Smart Structures and Systems (ICSSS).
- [4] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and YiHua Chen(2018) ‘Blockchain and Smart Contract for Digital Certificate
- [5] Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates."Elva Leka"
- [6] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy- preserving access control model based on blockchain technology in IOT,”

THANK YOU