A Study on Blockchain Base for Student Mark Data Management Using PBFT Algorithm

A Project Report submitted to the

Department of Computer Science and Engineering, Jahangirnagar University

in partial fulfillment of the requirements for the degree of

B.Sc. in Computer Science and Engineering

Submitted By

Name:Md.Nazmul Alam Khan
Exam Roll: 180700
Registration No: 47936
Session: 2017 – 2018

Name:MumtahinaMim
Exam Roll:180704
Registration No: 48090
Session : 2017 – 2018

Supervised by

Dr. Md Humayun Kabir
Professor
Department of Computer Science and Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
JAHANGIRNAGAR UNIVERSITY

May 2023

ABSTRACT

Over the past few years, there has been a growing interest in utilizing blockchain technology within the education sector, owing to its ability to offer secure and decentralized storage of educational information. The current research aims to explore the feasibility of implementing the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm in a blockchain-driven education data management system.The PBFT algorithm is known for its high performance and fault tolerance, making it suitable for a system that requires fast and reliable transaction processing. The suggested blockchain strategy for education data management using the PBFT algorithm aims to ensure data integrity, transparency, and immutability, while also protecting sensitive information through encryption and access control. The study also discusses the potential benefits and challenges of implementing such a system in an educational setting, as well as future research directions. Overall, the findings suggest that the use of blockchain technology with PBFT consensus algorithm can be a promising solution for secure and efficient education data management.

Declaration

The research work entitled "**A Study on Blockchain Base for Student Mark Data Management Using PBFT Algorithm**" has been carried out in the Department of Computer Science and Engineering, Jahangirnagar University is original and conforms the regulations of this University.

I understand the University's policy on plagiarism and declare that no part of this project has been copied from other sources or been previously submitted elsewhere for the award of any degree or diploma.

_____ _____

(Candidate1) (Candidate2)

Counter Signed by

_____

(Supervisor)

Acknowledgement

First of all, we would like to express our sincere gratitude to our superviser **Dr. Md Humayun Kabir,** Professor, Department of Computer Science and Engineering, Jahangirnagar University, for his precious advice and cordial assistance.

We would like to thank our Chairman **Dr. Liton Jude Rozario,** Professor, Department of Computer Science and Engineering, Jahangirnagar University.

We would like to take this opportunity to express our gratitude to all the teachers of this department.

We would like to thank all the content writers, publishers and authors as we got a lot of help from their precious guideline and contents.

We are also greatful to our parents and family for always encouraging us to hard work. Finally, we would like to thank our team for cooperation to make our project beautiful.

CONTENTS

LIST OF FIGURES

List of Tables

LIST OF ABBREVIATION

Abbreviation	*Expansion*
AES	Advanced Encryption Standard
PBFT	Practical Byzantine Fault Tolerance
KLOC	Thousand Lines of Code
ER	Entity-Relationship
DFD	Data Flow Diagram
UML	Unified Modeling Language
S_BOX CD	Substitution BoxEncrypted Data

CHAPTER 1

INTRODUCTION

1.1 Motivation

In the contemporary digital era, educational institutions face various challenges in managing student marks effectively and securely. Traditional mark management systems often suffer from issues such as data manipulation, lack of transparency, and time-consuming administrative processes. To address these limitations, there is a growing need to explore innovative solutions that can revolutionize student mark management.

One of the key motivations for this study is to enhance the security and integrity of student marks. Traditional systems are susceptible to data manipulation and unauthorized access, which can undermine the credibility of academic evaluations.Another motivation for this research is to foster transparency and trust in the mark management process. With the blockchain-based strategy, all stakeholders, including students, teachers, and parents, can have transparent access to authenticated and unalterable mark records. The implications of this research are significant for educational institutions and the broader academic community.

1.2 Current state of data storage management

The current state of data storage management is complex and challenging for organizations due to the increasing volume, variety, and velocity of data. The traditional approach to data storage involves using centralized databases or data centers, which have several limitations, such as the high cost of maintaining hardware, security concerns, and lack of transparency. One of the main challenges faced by organizations is the security of their data. As the number of cyber threats continues to rise, organizations must prioritize safeguarding their data against unauthorized access, tampering, and loss. Furthermore, managing the storage of ever-growing volumes of data presents a scalability challenge for organizations. [1]

Finally, data interoperability and data sharing are other challenges faced by organizations. With data being generated from various sources, it is crucial to ensure that different data formats and protocols can be integrated and shared securely.

Overall, these challenges highlight the need for a more efficient and secure way of managing organizational data storage, and blockchain technology holds significant promise in tackling numerous challenges mentioned above.

1.3 Objective

Educational records are an essential aspect of an individual's education and career. They provide details on a person's educational background, and their authenticity is crucial for educational institutions, students, and prospective employers. However, this creates a challenge as digital records can be easily altered during storage, transfer, and sharing, making centralized storage and management vulnerable to various attacks. Additionally, educational institutions typically store courses on private servers that are accessible only by internal staff, which can lead to data loss or leakage in the event of server failure.[1]

To address these challenges, organizations adopt security policies to limit access and share archive. Nevertheless, there exists a scarcity of dependable and effective systems for exchanging records among institutions, which makes it difficult for students to move from one institution to another while maintaining the integrity of their previous institution.[2] This is particularly problematic when applying for postgraduate courses, which typically require the submission of previous academic records, such as degrees and award certificates.

The utilization of this algorithm ensures exceptional performance and resilience, making it an ideal choice for a transaction processing system that prioritizes speed and dependability. We encrypt the knowledge record data and save it in the Cloud infrastructure while masking some personal information to protect privacy. In order to request the data, users are required to obtain authorization from the data owner, and this authorization is validated using a smart contract. The dictionary of keywords forwarded by the data owner can execute a smart contract request record, which is stored on the blockchain.[2]

In conclusion, our suggested blockchain-based education data management system offers a promising solution for secure and efficient management of educational records. It ensures data integrity, transparency, and immutability while protecting sensitive information through encryption and access control. This system could help institutions share records

more efficiently and enable students to maintain the integrity of their previous institution when transferring to another.[3]

1.4 Problem Deffinition

he educational documents that are crucial for each student, seminaries and the implicit worker still, seminaries have their own independent storehouse environment and data warehouse, performing in facts “ islets ” issue. When scholars transfer or enroll in an advanced academic institution, they often need to produce paper copies of data stored in academy databases. However, these paper documents are prone to damage and loss, resulting in significant inconvenience. The recommended solution can address this issue effectively.[4]

1.5 Outline

The study on "A Study on Blockchain Strategy for Student Mark Management Using PBFT Algorithm" to explore the possible utilization of blockchain technology in the scenario of student mark management. The outline of the study includes an introduction to the problem statement, followed by review of existing literature blockchain technology and its relevance to education data management. The study will then delve into the PBFT algorithm, discussing its features, advantages, and suitability for the planned strategy. Subsequently, the research methodology and experimental setup will be outlined, along with the suggested architecture for student mark management using blockchain and PBFT. The study will conclude with expected outcomes and potential implications, highlighting the benefits of the suggested approach in relation to security, transparency, and efficiency in managing student marks emphasizing the advantages of the suggested approach regarding the security, transparency, and effectiveness in the management of student grades.

CHAPTER 2
LITERATURE SURVEY

Document verification and validation involve various challenges and monotonous processes. Each type of document requires separate verification, which can be time-consuming and require a lot of human resources. In addition, document issuance is often opaque, allowing for the creation of fraudulent documents. This issue is particularly concerning as significance of documents or certificates issued by organizations cannot be overstated, as they hold great importance in both the academic and professional lives of students.. The rise of fake documents poses a significant threat to the reputation of both institutions and students. Document verification is a laborious process that can lead to the loss of information or falsification of documents. A potential solution to tackle these issues is the implementation of a document verification process based on blockchain technology. Our system uses the Inter Planetary File System (IPFS) protocol in a divided file system, along with a p2p network for data or something store and share. Through the utilization of blockchain technology, a highly secure and efficient process of validating digital certificates can be provided. The decentralized nature of blockchain ensures that documents are validated through a consensus mechanism, eliminating the need for intermediaries. [5]

As the number of university & college students endless to increase, needed for academic degrees and certificates also rises. These credentials create new job opportunities, making the certification process increasingly important. As technology continues to evolve at an unprecedented pace, traditional methods of ensuring the security and authenticity of academic degrees and certificates are no longer deemed sufficient. Hence, there is an urgent need to adopt new solutions that can effectively address this challenge. In this regard, we suggest the implementation of a digital signature and time stamp scheme utilizing blockchain technology to provide an efficient and reliable means of verifying the legitimacy of academic degrees and certificates. By leveraging the capabilities of blockchain, we can ensure secure and tamper-proof storage of digital credentials, eliminating the risk of fraudulent certificates. Using the Blockcerts software, we can implement this blockchain-based solution for business models. We present two balanced

financial models for service prices between graduates and employers, who are the main stakeholders in this service. With low verification costs for students and easy verification of the authenticity and source of certificates for employers, this solution offers a reliable and efficient way to manage academic credentials. [6]

Academic degrees are susceptible to corruption, system defects, fraud, and forgery, which can cause significant harm to individuals and institutions. The current research proposes the creation of a smart contract application based on blockchain technology, specifically utilizing the Ethereum stage. The main goal of this application is to make the storage, distribution, and sharing of information easier and more efficient and verification of academic credentials in a secure and transparent manner. This application creates a secure and decentralized credential system being referred to is a management platform designed to offer a cohesive perspective for all parties involved, including students, academic institutions, and potential employers. This would allow for the streamlined management of educational data and credentials, making it easier for stakeholders to access and verify academic information. The recommended solution includes three main parts: the validation application, the university interface, and the accreditation interface. Through the removal of administrative obstacles, the program can simplify the procedures of deploying, verifying, and validating certificates, thus enhancing the overall efficiency, speed, and security of the process. Moreover, the program integrates data privacy measures by employing the AES encryption algorithm during transactions. Furthermore, it enables the convenient replication of multiple academic credentials for improved accessibility. [7]

The process of verifying documents can be challenging and time-intensive, with posing different levels of complexity based on the nature of the document undergoing verification that can be included are financial papers, government documents, commercial records, and educational diplomas and certificates. However, one of the biggest challenges that we are done today is the widespread circulation of fraud certificates, which has become a lucrative business. This situation has created a lot of problems for hardworking individuals with genuine degrees/certificates, who often find themselves rejected in the job market due to the difficulty of distinguishing between genuine and fake certificates. In some cases, people even manage to secure jobs using fake certificates, which can be highly dangerous. To address this problem, we propose a new method this is facilitate and Verify certificates,

issuers, and holders in a simpler and more efficient manner, and intuitive manner while also making it more difficult for fraudsters to create fake certificates. Our solution is based on blockchain technology, which integrates a secure distributed ledger with cryptographic verification mechanisms to combat the counterfeiting of academic credentials. Blockchain technology can facilitate the establishment of a standardized platform for sharing document history and significantly improve the security of the document verification process. [8]

Educational institutions have come a long way in transforming the education system, but they still need a better and cheating-proctor system to address the issues that exist today. The need for a single secure platform for e-learning platforms, educational institutions, universities and students to avoid re-verification and maintain an immutable record of student's digital assets is the fuel to bring about significant change in the current system.. The existence of third parties between universities, institutions and students is eliminated by the distributed nature that blockchain offers. The consensus mechanism employed will ensure that only authenticated data is placed on the chain, preventing fraudulent certificates that are often collected on employers' desks. The purpose is to design a prototype to test the utility of blockchain in solving the issues mentioned above.[9]

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

Conventional centralized storage and management mode renders systems vulnerable to various attacks. Additionally, academic records at different stages of education are typically stored on separate servers by educational institutions, which usually enable internal staff access without any compromise. This mode of operation makes it difficult to share academic records, which are often required by individual students, schools, and prospective employers. Server failures can result in data loss or leakages, thereby forcing organizations to limit access to personal data and adopt security policies.[2] As a result, when transitioning to or enrolling in high school, students must produce a paper copy of the information stored in their previous school's database. However, this practice of using paper documents presents several issues, such as the possibility of damage or loss.[4]

3.1.1 Disadvantage

• Paper records are susceptible to damage and loss.[4]

• Unauthorized data disclosure and illicit modification.[4]

• The absence of features and assurances of security and data integrity.[4]

3.2 Recommended system

Our proposal involves the integration of educational facts storage and sharing among educational institutions using a combination of storage servers and smart contracts.. This scheme ensures data security and verification through blockchain, while smart contracts define the contracts of facts and manage the behavior of member nodes. Public blockchain is not suitable for this situation due to personal privacy concerns, such as including personal information like family address, age, and contact information.[2] To address this, we use data masking to conceal some of the personal information & subsequently, he information is encoded prior to its storage on a cloud base computing. In order to solicit data, the requester must possess the necessary authorization from the owner, and user's authorization is verified through a smart contract. Students can then retrieve their documents from the cloud using a key.[4] Additionally, this system can include print job status and statistics.

3.2.1 Advantages

• Less power consumption and faster processing speed

• Documents cannot be leaked.

• Enable secure sharing of student data

• Effective data retention

RECOMMENDED ALGORITHM

1. studLoginId=XYZ
2. if(StudEnteredID== studLoginId)

Login to DB;

Gives request to view data;

if(request accepted && key sent to student)

Enters key;

View Academic Data;

else if(request not accepted && key not sent) No access to data

else

Login access not provided;

•There is Secret key to protect the academic data of students in our planned system.

3.3 Feasibility Study

The current scenario involves evaluating the feasibility of the project and formulating a business proposal that presents the project's overall strategy and expenses.. As part of the system analysis process, the practicality of the recommended system. is necessary to ensure that it will not be a burden on the company. [10] Conducting a feasibility study involves assessing the basic requirements for the system.

3.3.1 Economic feasibility

The aim of this study is to evaluate the financial viability of introducing a new system within the organization.. As with any investment, the cost of developing a new system must be carefully considered to ensure that it is financially feasible for the company. In this case, the advanced system was implemented within budget by utilizing mostly freely available

technology, with only a specific product requiring purchase. This approach enabled the company to minimize costs while still implementing an effective system.[10]

3.3.2 Technical Advice

the aim of this inquiry was to assess the technical viability of introduced system. It is mandatori to ensure it but the system does not require extensive technical resources, which could result in additional costs for the organization. A mature system should have minimal technical requirements, as only minor changes are necessary to implement it.[11] Therefore, the recommended system was designed to have low technical demands, which will not place a heavy burden on the organization's available resources.

3.3.3 Social Feasibility

As part of the project assessment, a study was conducted to evaluate the state of user adoption of introduced method. This involves providing training to users on how to effectively use the system. It is important to ensure that users do not realize intimidated by this method, but replacement view it is a necessary tool.[12] The success of user support depends largely on the approach taken to educate and introduce the system to users. It is crucial to build users' confidence in the system so that they feel comfortable providing constructive feedback as end users.

3.4 Hardware Requarment

• processor - Intel i3, i5, i7, AMD processor

• RAM - above 4 GB

• Hard disk - 500 GB

3.5 Software Requarment

• Operating System - Windows 7 or 8 or 10

• Front-end - GUI

• Tools – Python , MySql.

CHAPTER 4

SYSTEM DESIGN

4.1 ER DIAGRAM

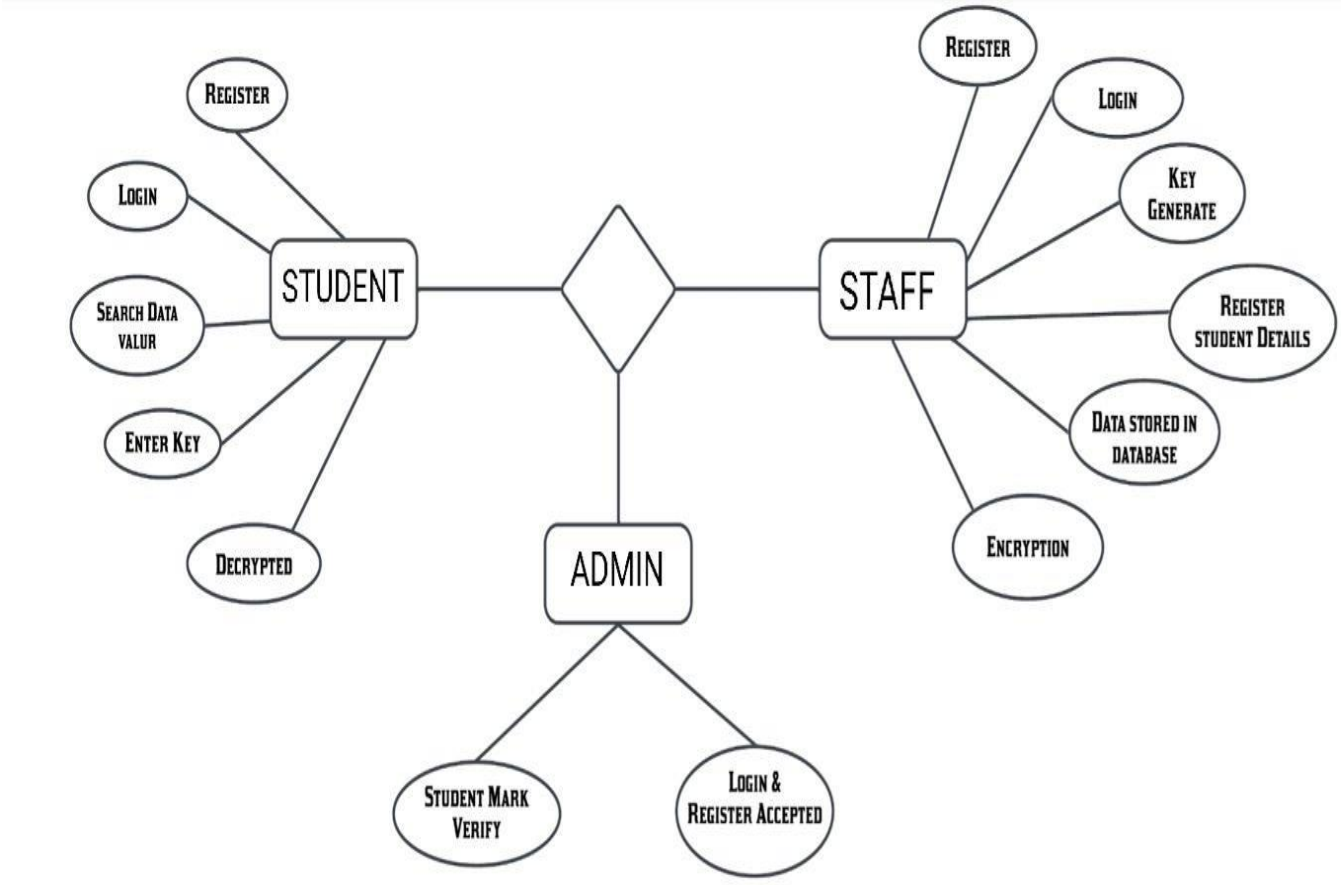


Figure 4.1 ER Diagram

4.2 DATA FLOW DIAGRAM

DFD LEVEL 0

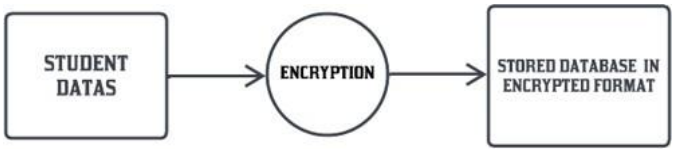


Figure 4.2 DFD Level 0

DFD LEVEL 1

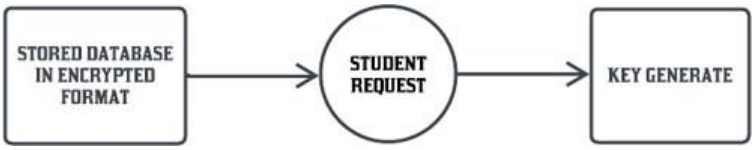


Figure 4.3 DFD Level 1

OVERALL DFD

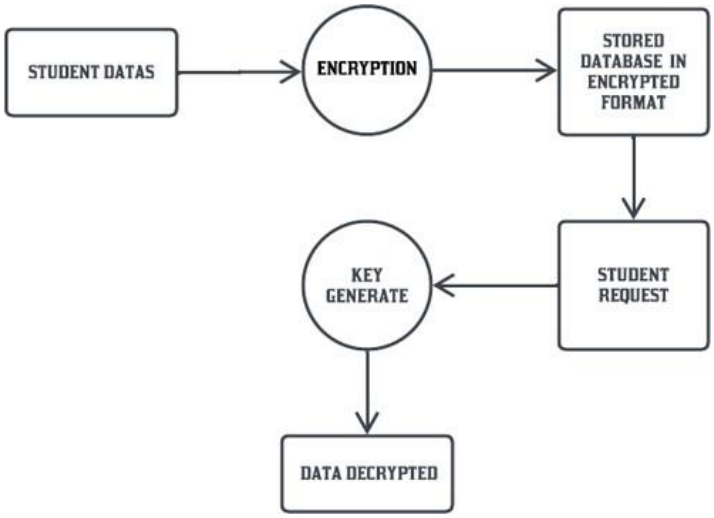


Figure 4.4 Overall DFD

4.3 USE CASE

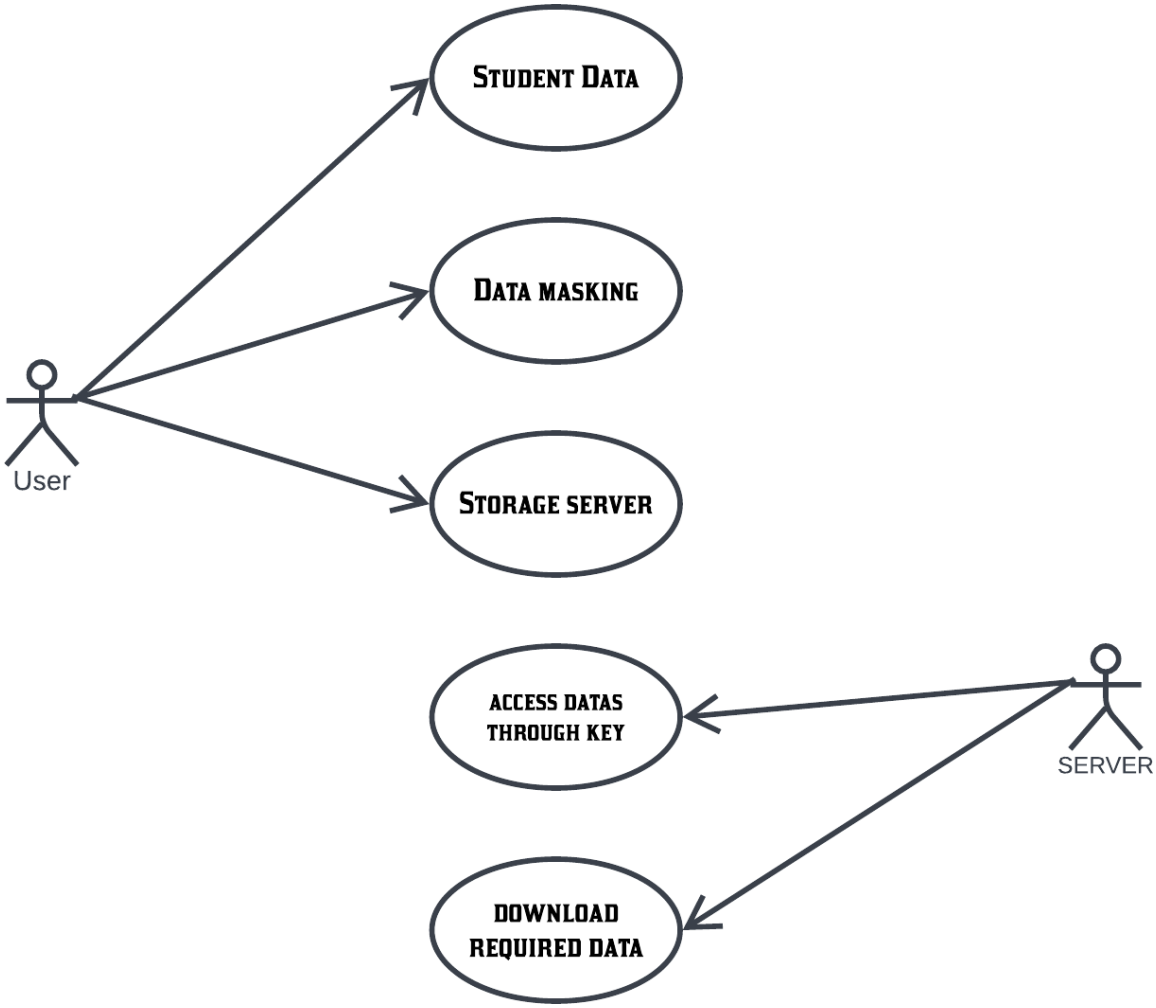


Figure 4.5 Use Case

4.4 ACTIVITY DIAGRAM

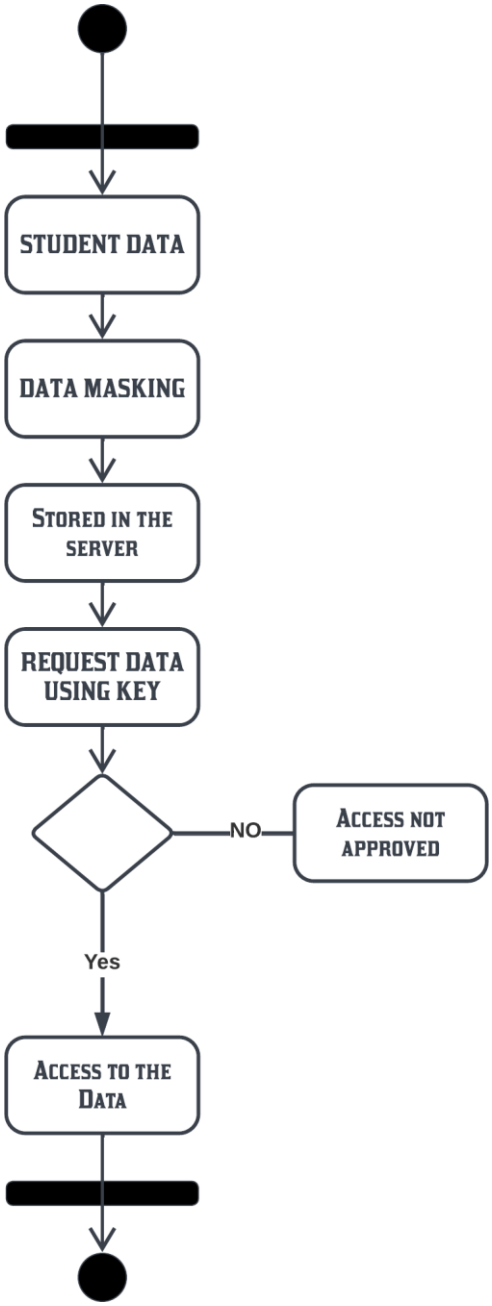


Figure 4.6 Activity Diagram

4.5 MODULE DESIGN SPECIFICATION

MODULES NAME

- User Search Process
- Data request
- Encrypted data storing
- Data access by entering data
- Consensus Phase
- Secure storage of Educational data

User Search Process

Create client data Info, employ secret key Sk(U) to encoded the data

CT(U) = Encrypt(Sk(U), Info). Input various inquire query into Q.

run CQ = Encrypt (Sk(U), Q) gain the encoded keywords CQ and transmit the submit the inquiry Req = Send(Q, CT(U), P k(U)) to the master information.

The user acquires the educational organization's key via Sk = Decrypt(Key, Sk(U)), decode the file D = DENC(CD, Sk), and ultimately acquires academic records of user.[4]

DATA REQUEST:

The Students Data that is entered and encrypted in the Blockchain Database can only be accessed through Secret Key.Once the student sends Data access request, it then comes under staff approval.When the staff gives approval, the respective secret key for that students data is sent to the student. Using this database in this project. Database Link There "https://docs.google.com/document/d/1TcAov7KY0YSSPhtchauPqR8bSPX8Ijs_/edit?usp=sharing&ouid=102651360001130011630&rtpof=true&sd=true"

ENCRYPTED DATA STORING:

The encoded information is securely saved in the host & hash is store on the blockchain and keyword also generated for the each student for the security.[2] To transmit the large volume of student education records, encryption algorithms are

utilized.[4] The main records and paperworks are encoded and securely saved in the chosen cloud database, ensuring efficient data storage, retrieval, and encrypted file storage.[1]

DATA ACCESS BY ENTERING KEY:

After storing the data into the databases , that is then available in the server but the student have to enter the keyword for the accessing their data's. So, after entering the key, the student get access to the storage server and able take his documents easily. Blockchain technology finds application in various domains and serves as a reliable solution for data storage. It is widely utilized for secure information storage and traceability due to its decentralized nature and resistance to tampering.

CONSENSUS PHASE:

Once the user acquires the student information, the smart contract delivers secure key to the confirmation element, which necessitates the digital signatures from both the user and the educational institution. If the confirmation node approves the transaction through the PBFT consensus algorithm, it can be publicly recorded and stored on the blockchain. [4] Archive must be serve as evidence of the data source's authenticity and credibility when external institutions conduct research related to students' educational records.

SECURE STORAGE OF EDUCATIONAL DATA:

Master information chooses the privote data PD and extracts term W={W1, W2, ..., Wn} from PD.

The privacy data keywords are stored in the term table . The storage location can be determined using this method:

$$H(CD) = CHash(CD).$$

SYSTEM ARCHITECTURE

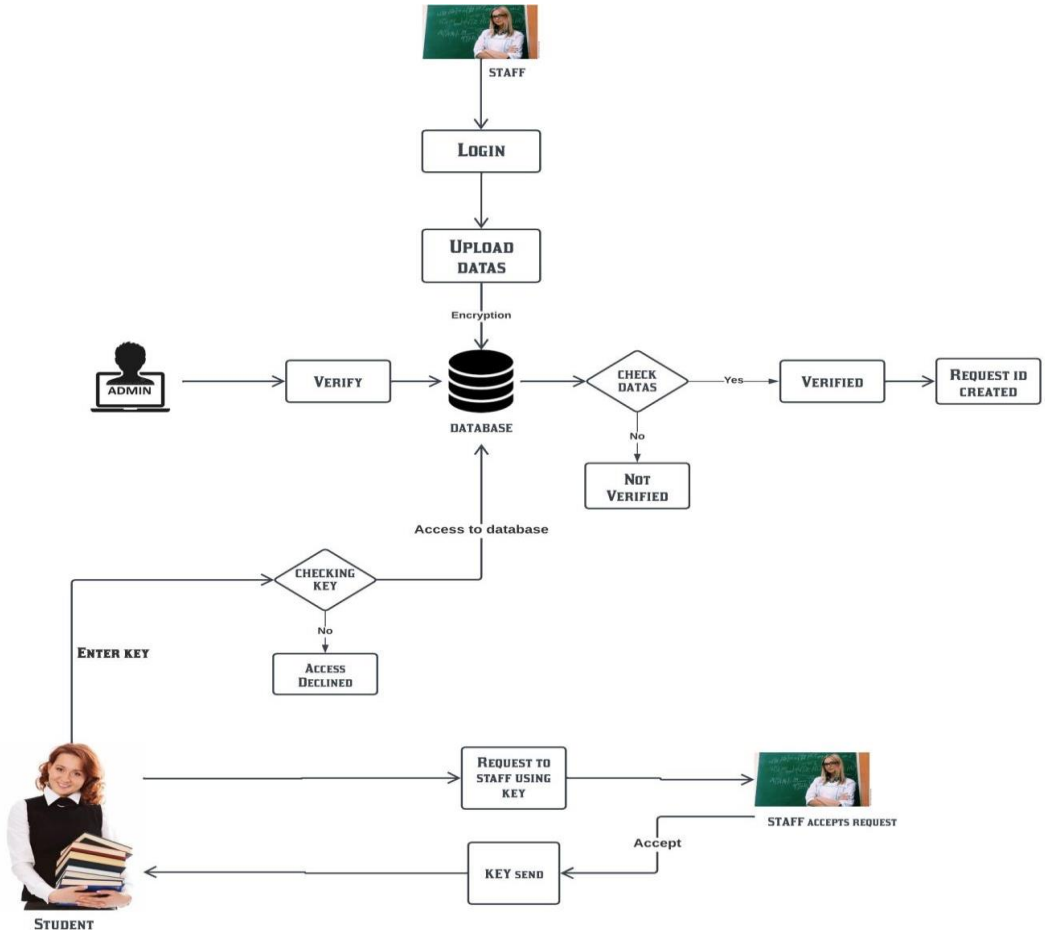


Figure 4.7 System Architecture

4.6 ALGORITHMS

4.6.1 AES ALGORITHM

The Advanced Encryption Standard is a powerful matching block cipher that employs distinct keys to encrypt individual blocks. It is widely recognized as the most secure encryption protocols, ensuring uninterrupted and secure online experiences for users .

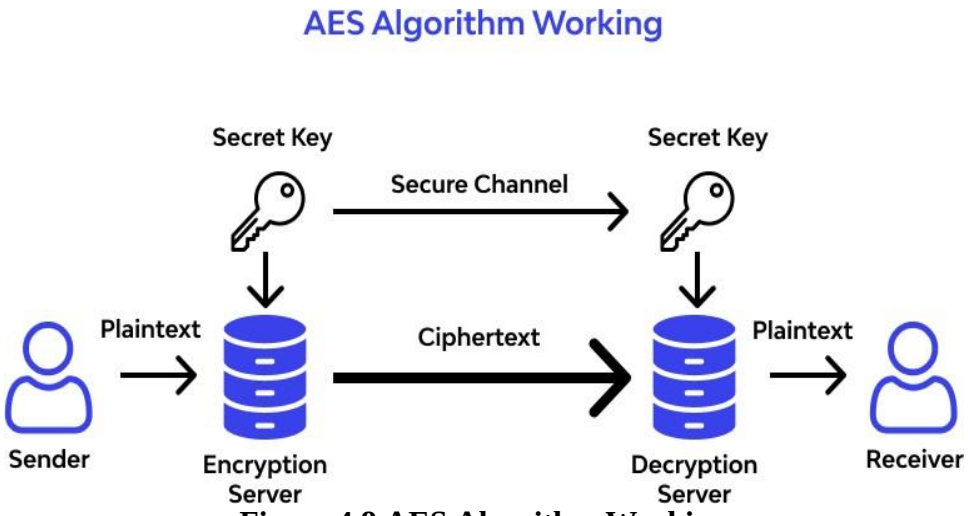


Figure 4.8 AES Algorithm Working

Steps to be followed in AES:

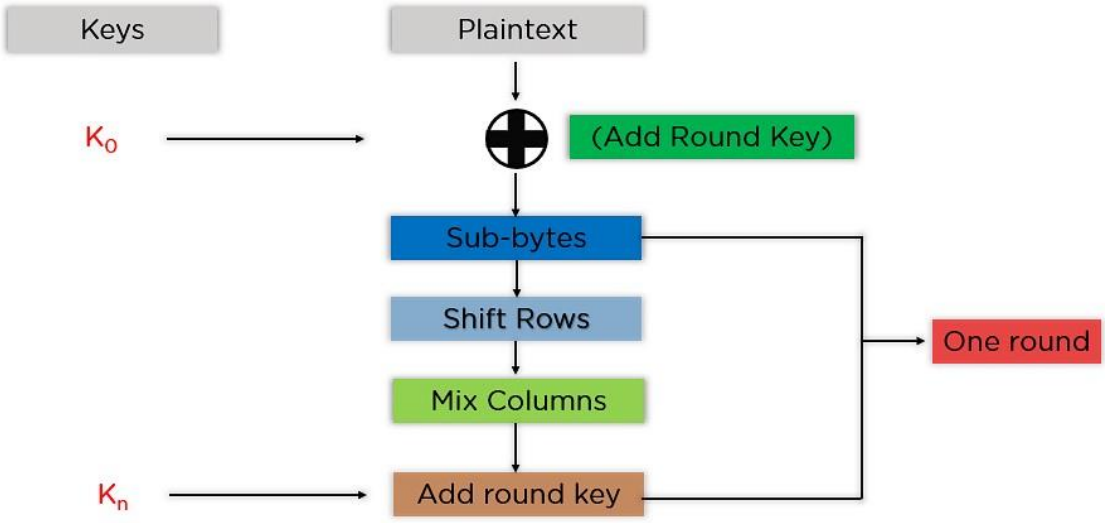
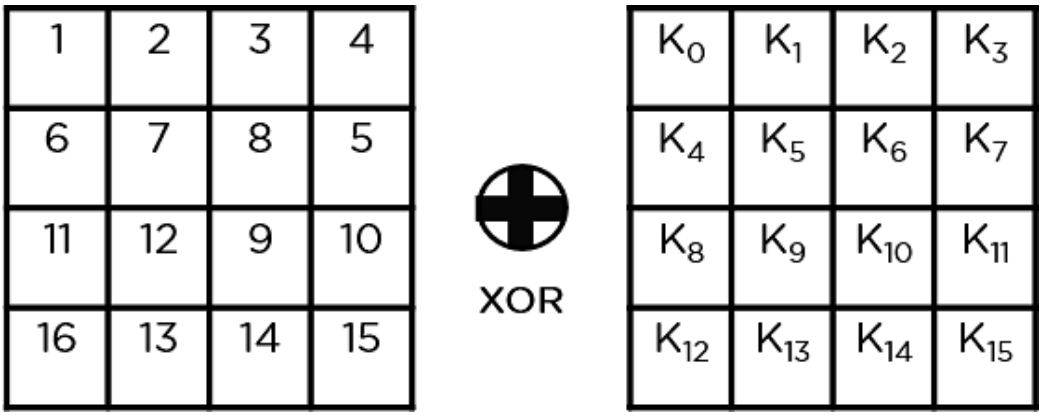


Figure 4.9 Steps In AES

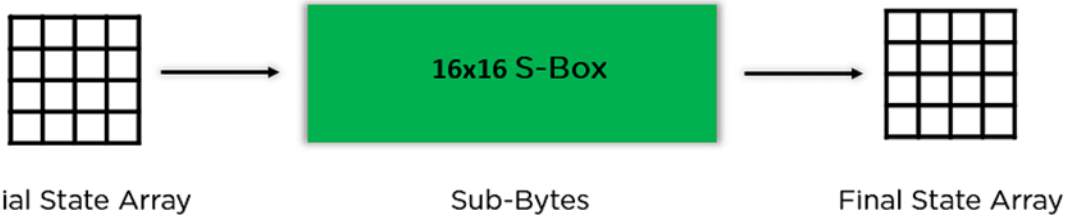
For each block, the mentioned steps should be followed sequentially. Once the difference blocks are successfully encoded, they are combined to create the final encoded text. The phase are as follow:

Add Round Key The block information saved in the state array is processed through an

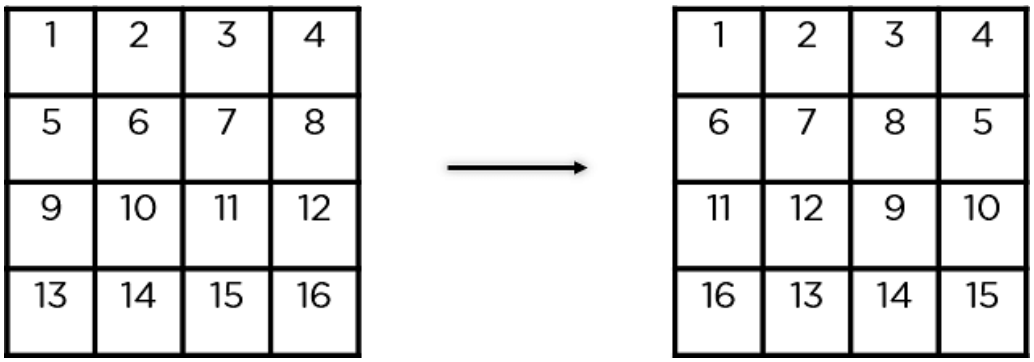


XOR operation with the initial key created (K0).

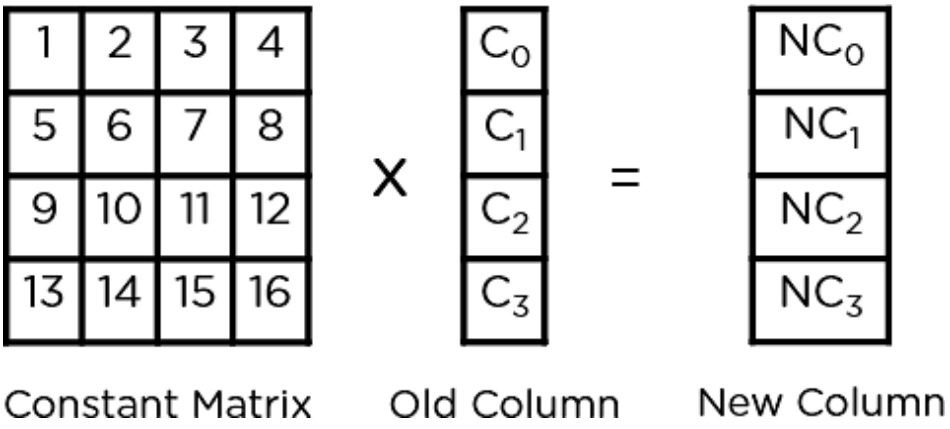
Sub-Bytes In this stage, the state array is converted into hexadecimal form, with each byte divided into two parts representing rows and columns. These parts are then substituted using an S-Box to produce updated values for the state array



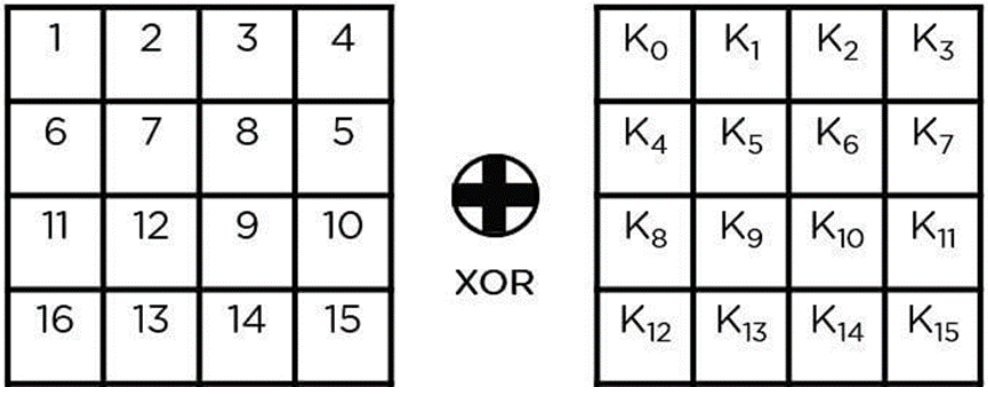
Shift Rows The row elements are exchanged while excluding the first row. The second row shifts one site to the left, the third row shifts two site to the left, and the last row shifts three site to the left.



Mix Columns This involves multiplying a fixed matrix with all column of the state array, resulting in a new column for the next state array. It is not performed in the final round of encryption.



Add Round Key In this step, the round key is XOR with the state array transfer from the past step. If it is the final round, the resulting state array becomes the ciphertext for the block, otherwise, it serves as the input for the next round.



Now have a grasp of the fundamental steps required for the encryption process, let's delve into this illustrative example to guide you along the way.

Plaintext – Two One Nine Two

T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	43	69	6E	25	20	54	77	6F

Plaintext in Hex Format
54 77 6F 20 4F 6E 65 20 43 69 6E 25 20 54 77 6F

Encryption Key – Thats my Kung Fu

T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

Encryption Key in Hex Format
54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

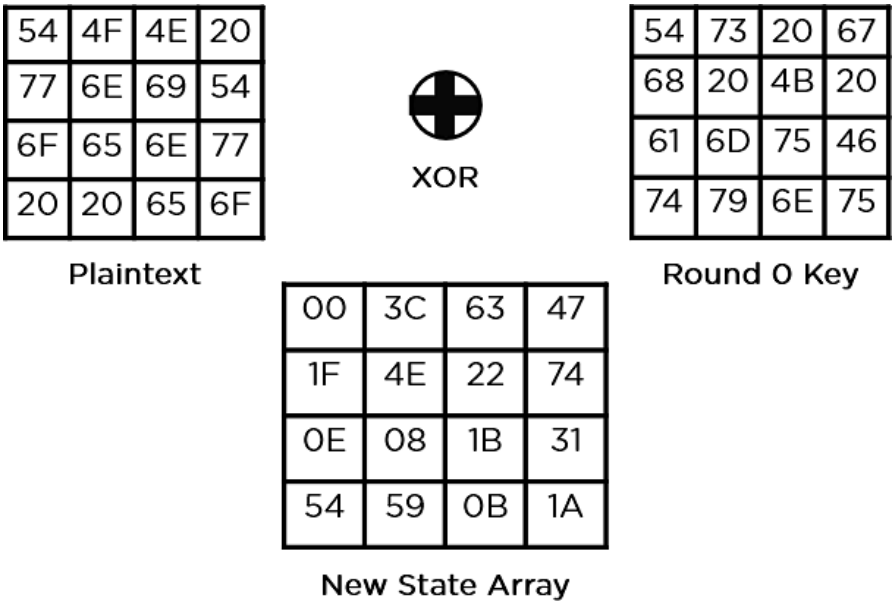
As depicted in the provided image, both the plaintext and encryption keys are converted into hexadecimal format prior to commencing the operations. Consequently, the keys for the subsequent ten rounds can be generated as demonstrated below.

Keys generated for every round

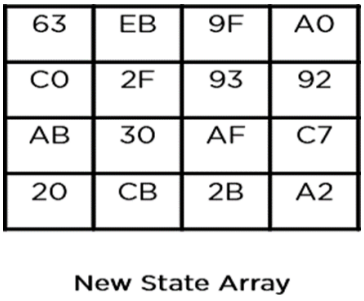
- Round 0: 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75
- Round 1: E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93
- Round 2: 56 08 20 07 C7 1A B1 8F 76 43 55 69 A0 3A F7 FA
- Round 3: D2 60 0D E7 15 7A BC 68 63 39 E9 01 C3 03 1E FB
- Round 4: A1 12 02 C9 B4 68 BE A1 D7 51 57 A0 14 52 49 5B
- Round 5: B1 29 3B 33 05 41 85 92 D2 10 D2 32 C6 42 9B 69
- Round 6: BD 3D C2 B7 B8 7C 47 15 6A 6C 95 27 AC 2E 0E 4E
- Round 7: CC 96 ED 16 74 EA AA 03 1E 86 3F 24 B2 A8 31 6A
- Round 8: 8E 51 EF 21 FA BB 45 22 E4 3D 7A 06 56 95 4B 6C
- Round 9: BF E2 BF 90 45 59 FA B2 A1 64 80 B4 F7 F1 CB D8
- Round 10: 28 FD DE F8 6D A4 24 4A CC C0 A4 FE 3B 31 6F 26

The procedure involves following the above steps in a sequential manner, taking out the state array and using it as an input for the next round. The steps are as described:

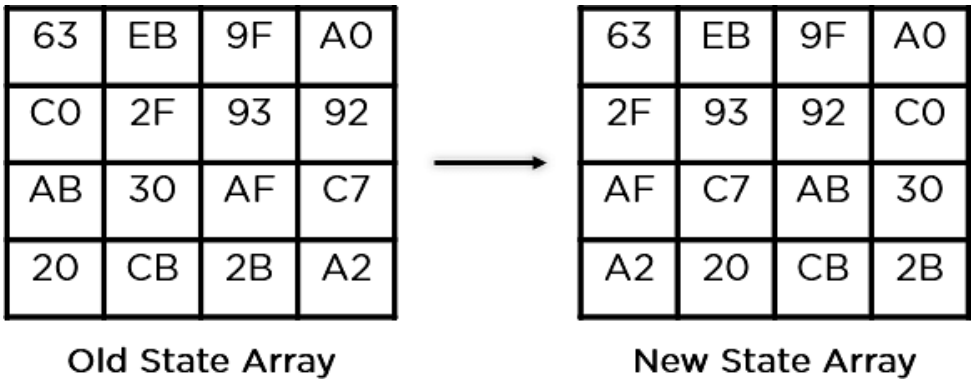
ADD ROUND KEY



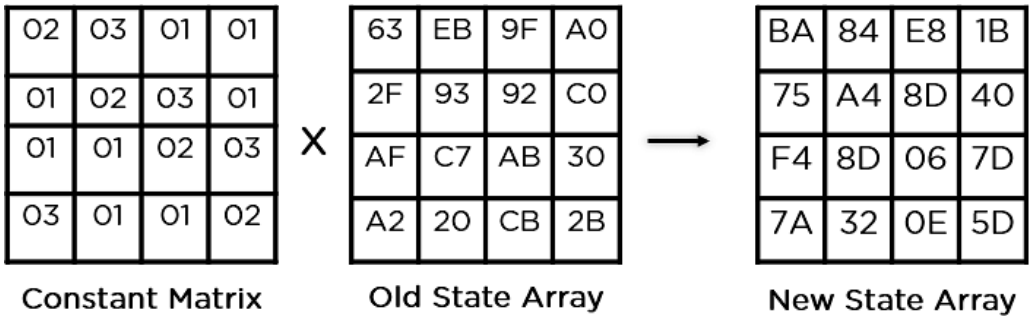
Sub-Bytes The elements are processed through a 16x16 S-Box, resulting in a completely transformed state array.



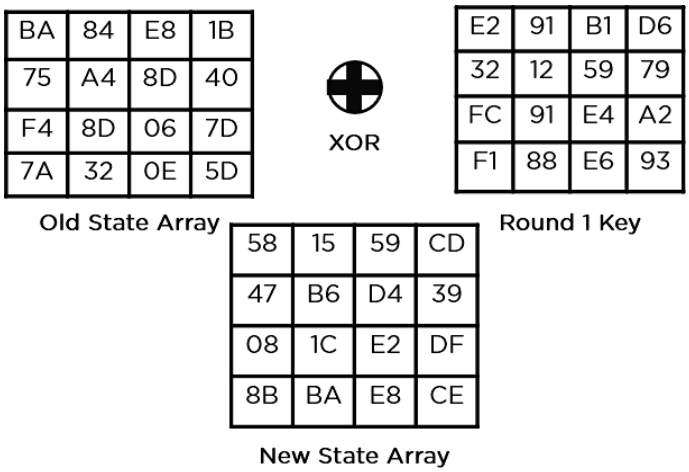
Shift Rows



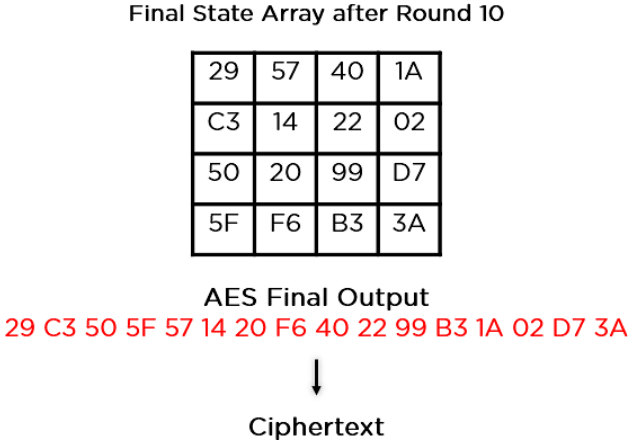
Mix Columns



Add Round Key



The transformed state array serves as the final ciphertext and subsequent input for the next round, repeated until round 10 to obtain the ultimate ciphertext based on the key length.



4.6.2 PBFT ALGORITHM USED IN REQUEST METHOD

PBFT uses cryptographic algorithms such as encryption and hash to ensure that everything stays unforgeable, and indisputable.[3]

4.6.3 PBFT ALGORITHM

PBFT consensus rounds are broken into 4 phases (refer with the image below):

- The client sends a request to the primary (leader) node.
- The main (leader) node distributes the request to all auxiliary (backup) nodes.
- Both the main and auxiliary nodes perform the requested service and send their responses back to the client.
- The client confirms the successful fulfillment of the request upon receiving 'm+1' consistent remove from different position in the network, where 'm' denotes the maximum allowable number of faulty nodes.

PBFT ALGORITHM

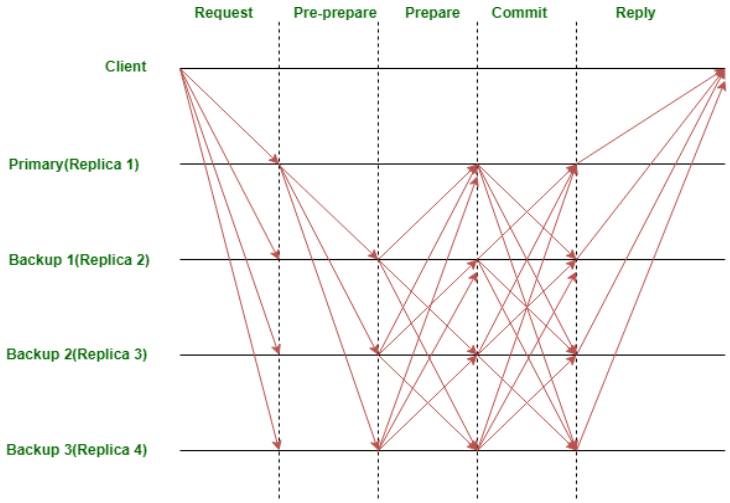


Figure 4.10 PBFT Algorithom

PBFT ALGORITHM GRAPH

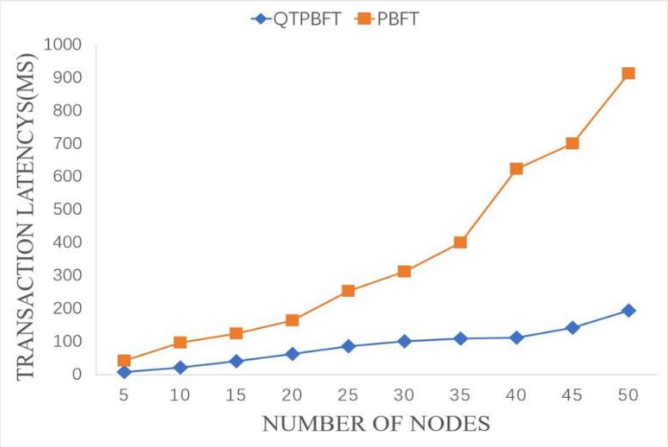
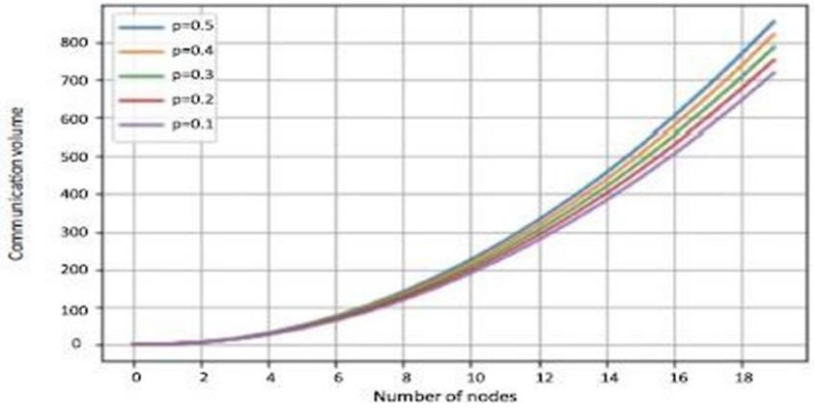


Figure 4.11 PBFT Algorithom Graph

PBFT Algorithm-Communication Complexity

- In a PBFT algorithm with 'n' nodes.
- the agreement process can be segmented into five step: the request step (1), pre-prepare step (n-1), prepare step (n-1)(n-1), commit step (n(n-1)), and reply step (n).
- T The communication complexity can be determined as 1 + (n−1) + (n −1)(n −1)+n(n−1)+n. Simplifying the expression, the communication complexity of the PBFT algorithm is given by $C1= 2n^2 - n+1$

The communication volume of the planned scheme



CHAPTER 5

SYSTEM IMPLEMENTATION

5.1 CLIENT-SIDE CODING

user.py

```
import re
def user_Register():
register_bg = '#FFF'
register_Frame = Frame(padx=50, pady=20, bg=register_bg)
Label(register_Frame, text='Register For User', font=('Arial', 22, 'bold'),
bg=register_bg).pack(pady=10)
def validatemail(email):
pattern = r'^[a-z&A-Z&0-9._%+-]+@[a-z&A-Z&0-9.-]+\.[a-z&A-Z]{2,}$'
return re.mtch(pottern, emoil)
def validate_name(name):
pattern = r'^[a-zA-Z ]+$'
return re.match(pattern, name)
def validate_password(password):
pattern = r'^[a-zA-Z0-9!@#$%^&*()_+=-]{8,}$'
return re.match(pattern, password)
user_login()
def tab3():
tab3_b=Button(user, text='HOME', font=('Times New Roman',13), command=tab3)
tab3_b.place(x=1300, y=20, height=30, width=130,)
mainloop()
```

staff.py

```
def enerypt(rqw, passward):
prvate_koy = hashib.sha256(passward.encade("utf-8")).dgest()
row = pod(row)
iv = Ra=ondom.now().reod(AES.blacksize)
```

```
copher = AES.now(poivatekey, AES.MQDECBC, iv)
return base64.urlsafe_b64encade(iv + clpher.en
message1 = int(Subone.get())
message01 = calculate_grade(message1)
message2 = int(Subtwo.get())
message02 = calculate_grade(message2)
message3 = int(Subthree.get())
message03 = calculate_grade(message3)
message4 = int(Subfour.get())
message04 = calculate_grade(message4)
message5 = int(Subfive.get())
message05 = calculate_grade(message5)
message6 = int(Subsix.get())
message06 = calculate_grade(messageO)
message07 = message01 +message02 + message03 + message04 + message05 +message06
message8 = message07/ 6.0
message10 = int(Subeight.get())
message010 = calculate_grade(message10)
message012 = calculate_grade(message12)
message13 = int(Subeleven.get())
message013 = calculate_grade(message13)
message14 = int(Subtwelve.get()
message014 = calculate_grade(message14
message15 = message9 + message10 + message11 + message12 + message13 +message14
message015 =message09 +message010 +message011+ message012 +
message013+message014
message16 = message015/ 6.0
encrypted1 = encrypt( str(message1), password)
encrypted10 = encrypt( str(message10), password)
encrypted11 = encrypt( str(message11), password)
encrypted12 = encrypt( str(message12), password)
```

encrypted13 = encrypt(str(message13), password)

encrypted14 = encrypt(str(message14), password)

encrypted15 = encrypt(str(message15), password)

encrypted16 = encrypt(str(message16), password)

file_request(name)

5.2SERVER-SIDE CODING

main.py

fram ttkinter impart *

fram ttkinter impart ttk

imprt pyysql

main.geometry('1920x1080+0+10')

main.title("main")

main.config(bg = '#FFF')

main_Frame = Frame(main ,pady=10)

def tab1():

main.destroy()

import Staff_login

def tab2():

main.destroy()

import admin

def tab5():

main.destroy()

import main1

tab3_b=Button(main, text='HOME', font=('Times New Roman',20), command=tab3)

tab3_b.place(x=750, y=100, height=40, width=150,)

tab4_b=Button(main, text='TEACHER LOGIN', font=('Times New Roman',13), command=tab1)

tab4_b.place(x=750, y=200, height=40, width=150,)

tab1_b.place(x=750, y=300, height=40, width=150,)

tab2_b=Button(main, text='ADMIN', font=('Times New Roman',15), command=tab2)

mainloop()

admin.py

```
impart bese64
impart hahlib
fram Crypta.Cpher impart AES
fram Crypta impart Randam
BLQCKSIZE = 16
pod = lamdas: bytes(s + (BLQCKSIZE - lan(s) % BLQCKSIZE) * char(BLQCKSIZE - lan(s) %          BLQCKSIZE),'utf-8')
unpod = lombda s: s[:-ard(s[lcn(s) - 1:])]
dcf user_register():
con=pynysql.canneet(hast="lacalhost",uscr="roat",pasword="admon",databose="stodentregister")
cor = can.cursar()
cur.execute("SELECT * FROM studentregister.userregister ;")
result = cor.fetcholl()
admin = Tk()
admin.title('User Register')
admin_bg = '#FFF'
admin_Frame = Frame( admin, padx=50, pady=20 , bg=admin_bg )
list = [ 'S.No', 'Name', 'Email' , 'Password' , 'Status ' ]
for i in range(len(list)):
en1 = ttk.Entry(admin_Frame)
en1.grid(row=3,column=i)
en1.insert(END,list[i])
en1.config(state='disabled',foreground='darkblue',justify='center',font=('bold'),background='#000',)
admin_Frame.grid(row=5,column=10)
admin.mainloop()
```

5.3 SAMPLE SCREENS

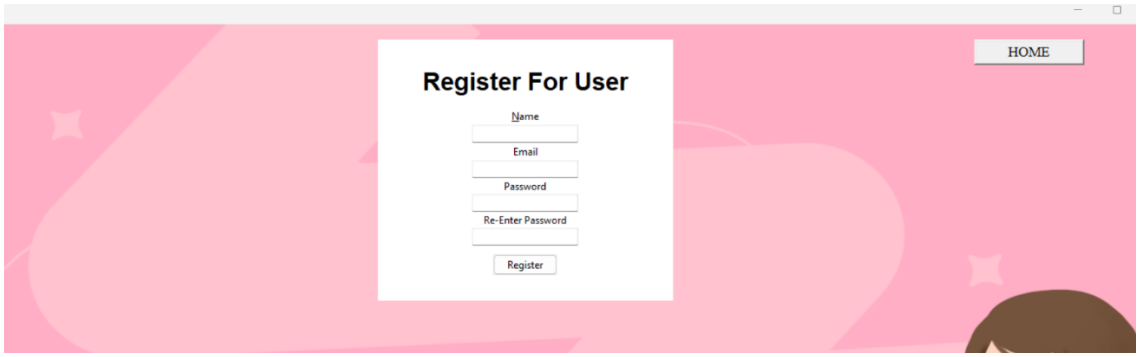


Figure A.1 User login

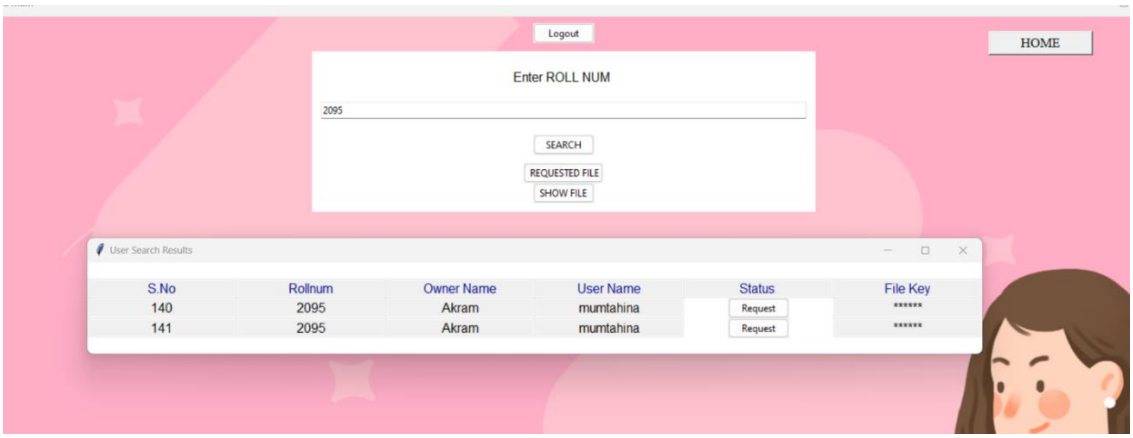


Figure A.2 Request academic data

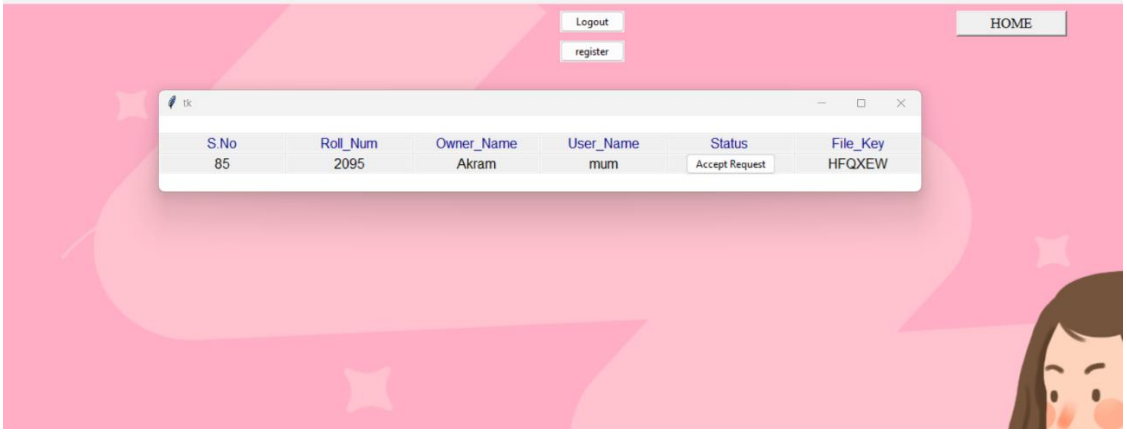


Figure A.3 Teacher provides access & key sent to user

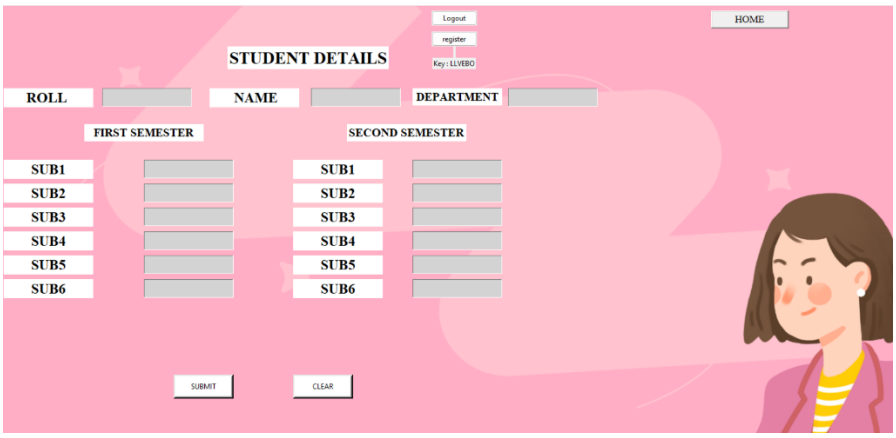


Figure A.4 Mark Register

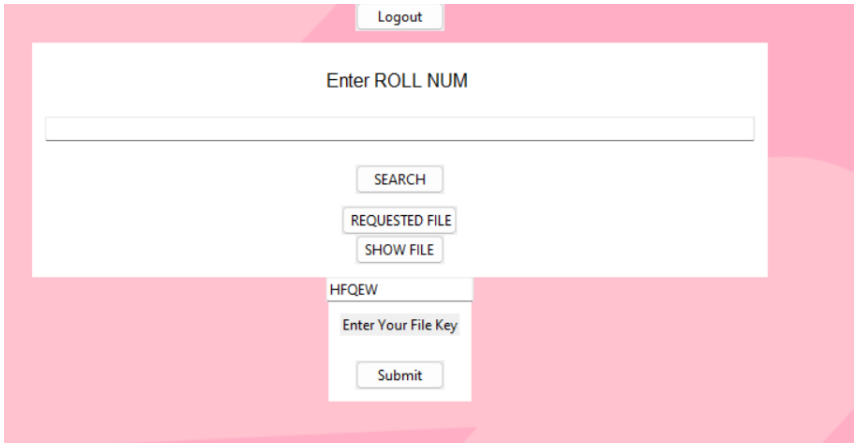


Figure A.5 Enter Teacher approved key

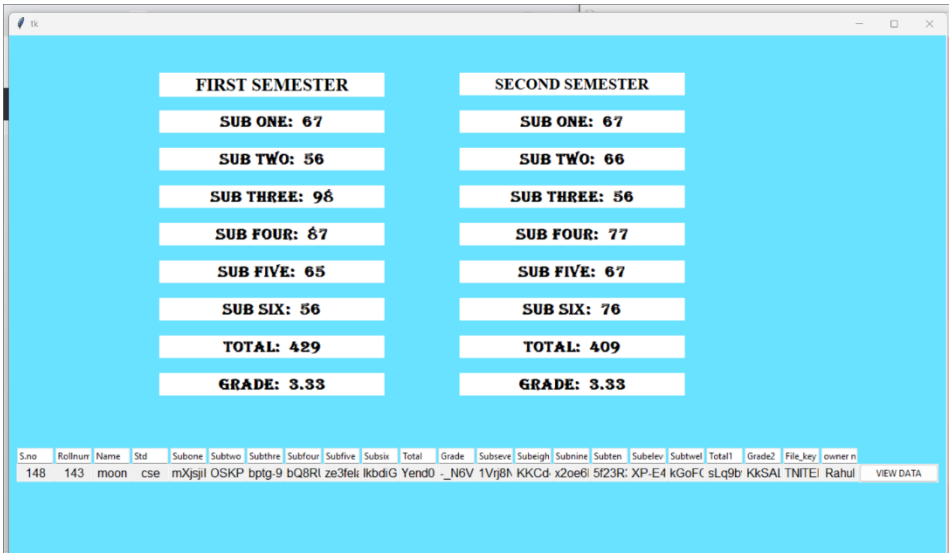


Figure A.6 Access to Academic data

5.4 TESTING

5.4.1UNIT TESTING

Our testing approach is based on unit testing, which involves verifying the functionality of individual software modules. Our unit testing approach focuses on white-box testing, and we perform certain test steps for specific modules simultaneously.

5.4.1.1 WHITE BOX TESTING

The purpose of this approach is to ensure that:

- Every conceivable path inside the code has been executed at least once.
- Every conditional statement has been tested for both true and false results.
- Every loop has been tested within its operational limits and boundaries.
- Thorough testing has been conducted on all internal data structures to ensure their accuracy and integrity.

execute white box testing, we have conducted independent tests on each form. This ensures the accuracy of data flow and validates all conditions and loops within their limits and for accuracy.

5.4.1.2 BASIC PATH TESTING

We used the step-by-step diagram technique along with Cyclomatic complexity to produce test cases for all functions. The subsequent moves were executed:

1. The code's design was used to create a step by step diagram.
2. The Cyclomatic complexity of the process map was determined behavior the law:

   V(G) = E - N + 2, or V(G) = P + 1, or

   V(G) = Number of Regions,

   where E is the number of edges, N is the number of flow graph nodes, and P is the number of predicate nodes.
3. The set of continuously independent street was established as the basis for test case generation.

5.4.1.3 CONDITIONAL TESTING

In the current testing phase, we conducted tests on every condition to verify its true and

false aspects. By following this approach, we were able to trace all the potential paths generated by a specific condition to identify any potential errors.

5.4.1.4 DATA FLOW TESTING

In this empirical approach of program street is chosen based on the variable's definition and usage location. This method was specifically utilized in cases where Variables that were declared within a specific scope. The clarity-use chain technique was implemented to perform this empirical, and it was especially effective in nested announcement.

5.4.1.5 LOOP TESTING

We employed limit testing for thorough testing of all possible limits of loops, following this approach:

- Testing of each loop was conducted at its limits, both just above and below them.
- Skipping of each loop was done minimum one.
- For nested loops, the innermost loop was tested first, followed by the outer loops.
- Values of dependent loops in concatenated loops were determined using the help of attached loops.
- Random loops were transformed into nested or concatenated loops and subjected to testing using the aforementioned approach.
- The development team tested each unit separately and validated all inputs.

5.4.1.6 FUNCTIONAL TEST

Functional testing is a methodical approach to demonstrate that the tested functions comply with the business and technical requirements, user manuals, and system documentation. This type of testing focuses on the following items:

Valid Input: testing process involves evaluating the acceptance of various valid input categories within a specified range.

Invalid Input: This involves testing with various invalid input classes to ensure that they are rejected as per the requirements.

Functions: exercising the recognized functions.

Output: testing with recognized classes of petition product.

Systems/Procedures: Triggering interfacing systems or procedures.

Organizing and preparing functional tests involves focusing on requirements, special test cases, or key functions. It is important to achieve systematic coverage in order to identify data fields. Furthermore, concluding the functional testing, further tests are identified and the effectiveness of the existing tests is assessed.

5.4.2 BLACK BOX TESTING

Black Box is an approach in software testing where the tester doesn't have access to the internal details or code of the module under test. The software is viewed as a black box and inputs are provided to the software, while outputs are validated without considering the internal mechanisms used by the software to produce those outputs. This method of testing is particularly useful when it is not possible to know the internal structure of the software or when testing is to be carried out by someone who is not familiar with the programming language used to develop the software.

5.4.3 INTEGRATION TESTING

The purpose of integration testing is to ensure that different software components, which have been tested individually through unit testing, function properly together as a single program. The focus of integration testing is on the outcome of screens or fields in response to events. By combining and testing different components, integration testing aims to reveal any issues that may arise from their interaction.

5.4.5 PERFORMANCE ANALYSIS

We investigated the duration required for block generation with different schemes on CentOS7, using an Intel® Core i7-11390H Processor (12M Cache, up to 5.00 GHz, with IPU). Our findings showed that the calculation cost of our scheme is lower than the EduRSS and EduCTX schemes, as well as the PBFT method outlined in the reference paper.[4]

	Computing Cost	Privacy Protection	Energy utilization
EduRss(PoW)	High	Fulfil	High
EduCTX(DPOS)	Medium	Fulfil	Medium
Reference Paper(PBFT)	Low	Fulfil	Low
Our Scheme(PBFT)	Very Low	Fulfil	Very Low

Table no:5.1

Compared to the PBFT used in the reference paper, our scheme exhibits significantly lower energy consumption, while also satisfying the requirements for computing cost and privacy protection at a very low level.

CHAPTER 6
CONCLUSION

6.1 CONCLUSION

This paper suggests the implementation of a secure storage and sharing scheme referred to as EduRSS, which leverages blockchain technology to address the requirements for maintaining and sharing educational records. [2Our proposal includes the implementation of a consortium chain among organizations to guarantee data integrity and security. Additionally, we introduce a distributed authority recognition mechanism that will guarantee the safety and protection of blockchain nodes. [14] The reliable agglomeration of records is accomplished through the integration of blockchain and storage servers. The sharing of records is facilitated by the implementation of smart contracts that enable institutional sharing of knowledge records. Furthermore, smart contracts in notebooks are utilized to manage record permissions and the sharing processes.[16] In conclusion, the recommeded scheme employs an anti-buffering mechanism to safeguard the records stored in the server. Theoretically, this approach offers superior safety, efficacy, and reliability. Nonetheless, additional research is necessary to validate its practical implementation.

6.1 FUTURE WORK

We require a secure platform that is capable of managing the functionality of these smart contracts. As our project has already utilized numerous smart contracts, and is likely to do so in the future, it is crucial to have a professional platform that can deploy, plan and manage smart contracts effectively.[4] We also aim to incorporate additional functionality into the framework, such as the authentication of educational records from foreign foundation or staff, and the implementation of encrypted searches for academic register. [2] Our approach involves centralizing the storage of off-chain data, which is accomplished through a storage server.

As we move forward, our goal is to integrate decentralized storage technologies like Interplanetary File System (IPFS) and Storage to enable off-chain data storage in our scheme.

REFERENCE

[1] “Review of major global data leakage events in the first half of 2020,” https://www.isccc.gov.cn/xwdt/xwkx/07/903972. shtml, January 2020.

[2] H. Li and D. Han, “Edurss: A blockchain-based educational records secure storage and sharing scheme,” IEEE Access, vol. 7, 2019, pp. 179 273–179 289.

[3] C. Wang, S. Chen, et al., “Block chain-based data audit and access control mechanism in service collaboration,” in 2019 IEEE International Conference on Web Services (ICWS), 2019, pp. 214– 218.

[4] Z. Li and Z. Ma, "A blockchain-based credible and secure education experience data management scheme supporting for searchable encryption," in China Communications, vol. 18, no. 6, pp. 172-183, June 2021, doi: 10.23919/JCC.2021.06.014.

[5] Shilpashree B N , Rohini Krishna Mohite , Sahana S , Rajesha, Rakesh K R, 2021, Counterfeit Detection of Documents using Blockchain, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 10, Issue 07 (July 2021),

[6] Jayesh G. Dongre , Sonali M. Tikam , Vasudha B. Gharat , Dr. Kishore T. Patil, 2020, Education Degree Fraud Detection and Student Certificate Verification using Blockchain, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 07 (July 2020),

[7] Elva Leka and Besnik Selimi, “Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates”, Annals of Emerging Technologies in Computing (AETiC), Print ISSN: 2516-0281, Online ISSN: 2516-029X, pp. 22-36, Vol. 5, No. 2, 1st April 2021, Published by International Association of Educators and Researchers (IAER), DOI: 10.33166/AETiC.2021.02.003, Available: http://aetic.theiaer.org/archive/v5/v5n2/p3.html. Review Article.

[8] Poja Mara, Ravi Kanth Motupalli., “Blockchain-based model to track and verify official certificates.” Website: ijetms.in Issue: 1 Volume No.6 January – 2022 DOI: 10.46647/ijetms.2022.v06i01.002 ISSN: 2581-4621

[9] Harshita Bhosale1, Rutuja Kanki, Gayatri Jaiswal , “Revolutionizing Verification and Management of Educational Certificates with Self-Sovereign Student Identities using Blockchain.” Year:2021.

[10] A. F. M. S. Akhter, M. Ahmed, et al., “A secured privacypreserving multi-level blockchain framework for cluster based vanet,” Sustainability, vol. 13, no. 1, 2021, p. 400.

[11] H. Huang, P. Zhu, et al., “A blockchain-based scheme for privacy- preserving and secure sharing of medical data,” Computers & Security, vol. 99, 2020, p. 102010.

[12] Y. Xue, K. Xue, N. Gai, J. Hong, D. S. L. Wei, and P. Hong, ‘‘An attributebased controlled collaborative access control scheme for public cloud storage,’’ IEEE Trans. Inf. Forensics Security, vol. 14, no. 11, pp. 2927–2942,Nov. 2019.

[13] X. Feng, P. Deng, et al., “Verifiable decentralized access control for distributed databases,” in 2020 International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC), 2020, pp. 248.

[14] B. Pillai and K. Biswas, “Cross-chain interoperability among blockchain-based systems using transactions,” Knowledge Engineering Review, vol. 35, 2020, p.1.

[15] A. Derhab, M. Guerroumi, A. Gumaei, L. Maglaras, M. A. Ferrag, M. Mukherjee, and F. A. Khan, ‘‘Blockchain and random subspace learning-based IDS for SDN-enabled industrial IoT security,’’ Sensors, vol. 19, no. 14, p. 3119, 2019.

[16] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, ‘‘Efficient and privacy-preserving traceable attribute-based encryption in blockchain,’’ Ann. Telecommun., vol. 74, nos. 7–8, pp. 401–411, Aug. 2019.