Department of Computer Science and Engineering
Jahangirnagar University

A Study on Blockchain Base for Students Marks Data Management Using PBFT Algorithm

Presented by

MD. Nazmul Alam Khan
Reg.No : 47936
Session:2017-2018

Mumtahina Mim
Reg.No :48090
Session :2017-2018

Supervised by

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

Sunday, 28 May, 2022

Presentation Outline

- Introduction
- Objectives
- Literature Survey
- Existing storage management System
- Blockchain Algorithm
- PBFT Algorithm
- Blockchain System model for Students Marks Management
- Module Description
- Result Analysis
- Conclusion & Future Scope

Introduction

- Some academic centers allow a quick and simple online query to verify the **authenticity** of student's academic information without even asking who requires that information.
- This leads to **academic frauds** and information stealing from the students and misusing it.
- Hence **Blockchain** come in handy to store students **information encrypted** in the database.
- Blockchain acts as a ledger system where data stored in a transparent and immutable format.
- The **PBFT algorithm** is the key method to make the blockchain consistent.

Objectives of the Project

- The main objective of the project the **keyword dictionary** sent by the **data owner**

- The smart contract can perform the search algorithm according to the user’s **query keywords**, and return the abstract and encrypted keywords of the corresponding **data file** found.

- After the query is completed, the **transaction** between the data owner and the user, that is, the **query record** can be published in the block chain.

Literature Survey

Sl No	Year	Title Of The Paper	Author	Description
1.	2023	Improved PBFT Consensus Algorithm Based on Node Role Division	Ren, X., Tong, X. and Zhang, W.	This paper discusses the core of the PBFT consensus algorithm that is composed of consistency protocol, checkpointing protocol, and view change protocol.
2.	2023	Improved PBFT Algorithm Based on Comprehensive Evaluation Model	Jiang, Wangxi, Xiaoxiong Wu, Mingyang Song, Jiwei Qin, and Zhenhong Jia	This paper discusses the difference between blockchain systems and traditional distributed systems is that the environment is complex, and Byzantine nodes will be introduced even in strict consortium blockchains, so research on the

Literature Survey

Sl No	Year	Title Of The Paper	Author	Description
3.	2022	Blockchain-based model to track and verify official certificates	Pooja Mara, Ravi kanth Motupalli	In this paper ,the Authors have developed a web-based application that is using Blockchain technology to store academic certificates to avoid certificate counterfeit as lots of fake certificates are being stolen and used to get jobs
4.	2021	Revolutionizing Verification and Management of Educational Certificates with Self-Sovereign Student Identities using Blockchain	Harshita Bhosale, Rutuja Kanki, Gayatri Jaiswal	In this paper, a framework which is a decentralized system is discussed.It performs a mechanism for the system to enable us to validate and track the operations performed by these institutions.

Existing storage management System

- **Centralized storage** and management mode is usually adopted, which makes systems that use this **mode vulnerable** to various attacks.

- The records of different educational stages are stored in **separate storage servers** of education institutions and these storage servers are usually designed to allow access only by internal staff

- In this system , a **server failure** could easily cause a **data loss** or leakage

Blockchain Algorithm

Some Blockchain Algorithm Name-

- Proof of Work (PoW)
- Direct Acyclic Graph (DAG)
- Practical Byzantine Fault Tolerance (PBFT)
- Proof of Capacity (PoC)
- Delegated Proof of Stake (DPoS)
- Advanced Encryption Standard (AES)

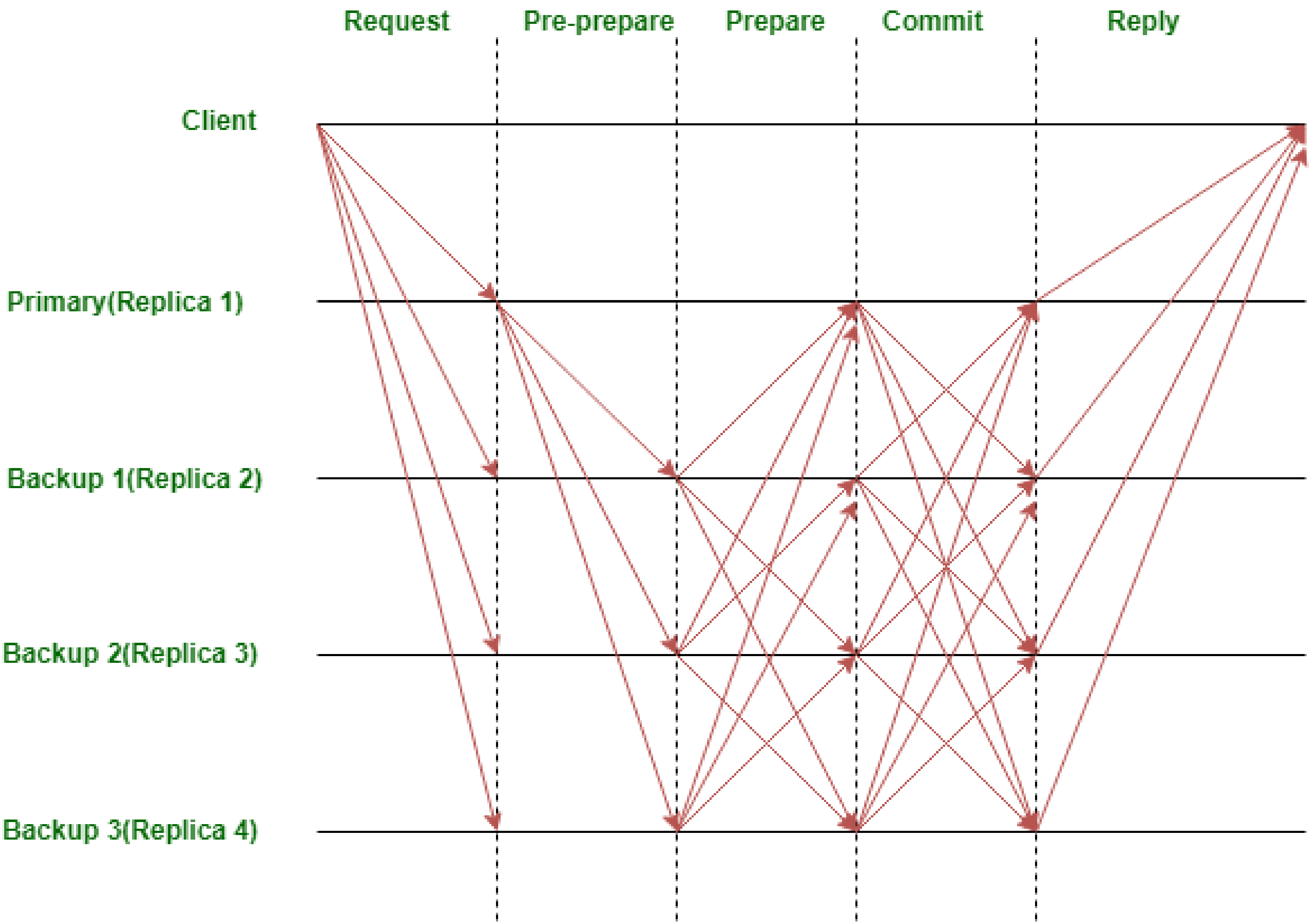
PBFT Algorithm

PBFT consensus rounds are broken into 4 phases(refer with the image in next slide):

- The **client** sends a request to the primary(**leader**) node.
- The primary(leader) node **broadcasts the request** to the all the secondary(backup) nodes.
- The nodes(primary and secondaries) perform the service requested and then **send back a reply** to the client.
- The **request** is served successfully when the client receives ‘m+1’ replies from different nodes in the network with the same result, where m is the maximum number of faulty nodes allowed.

- The Communication complexity of the PBFT algorithm: **$C1= 2n^{2} - n+1$**

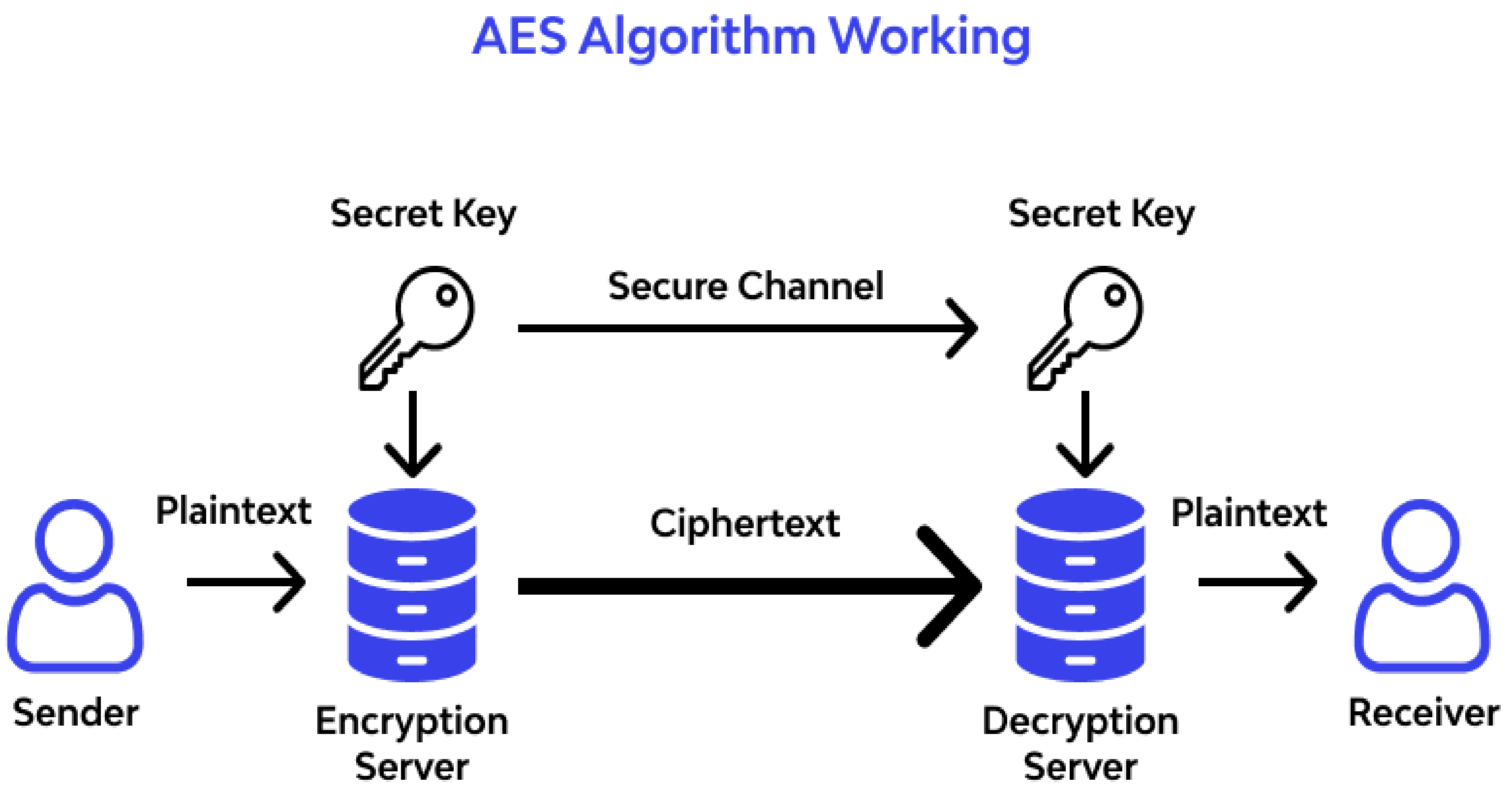
PBFT Algorithm



AES Algorithm

- The **AES algorithm** is a symmetrical block cipher algorithm that takes plain text in blocks of 256 bits and converts them to ciphertext using keys of 128, 192, and 256 bits
- **SHA-256** in cryptographic hash function.
- Uses **256 bit key** to **encrypt data** into unrecognizable text.
- **Plain text**(32 bits words)-**Block size**(256 bits)
- No of **rounds**-10 –**cipher text**(256 bits)

AES Algorithm



BlockChain System Model For Students Marks Management

- The **blockchain** is responsible for ensuring the **security** and auditability of the data, the smart contract is used to define the **permissions of the records** and to regulate the behaviours of the member nodes

- We remark that **public blockchain is not suited** in this case, because educational records are related to personal privacy and contain **sensitive information**, such as family address, age, contact details, etc.

BlockChain System Model For Students Marks Management (1)

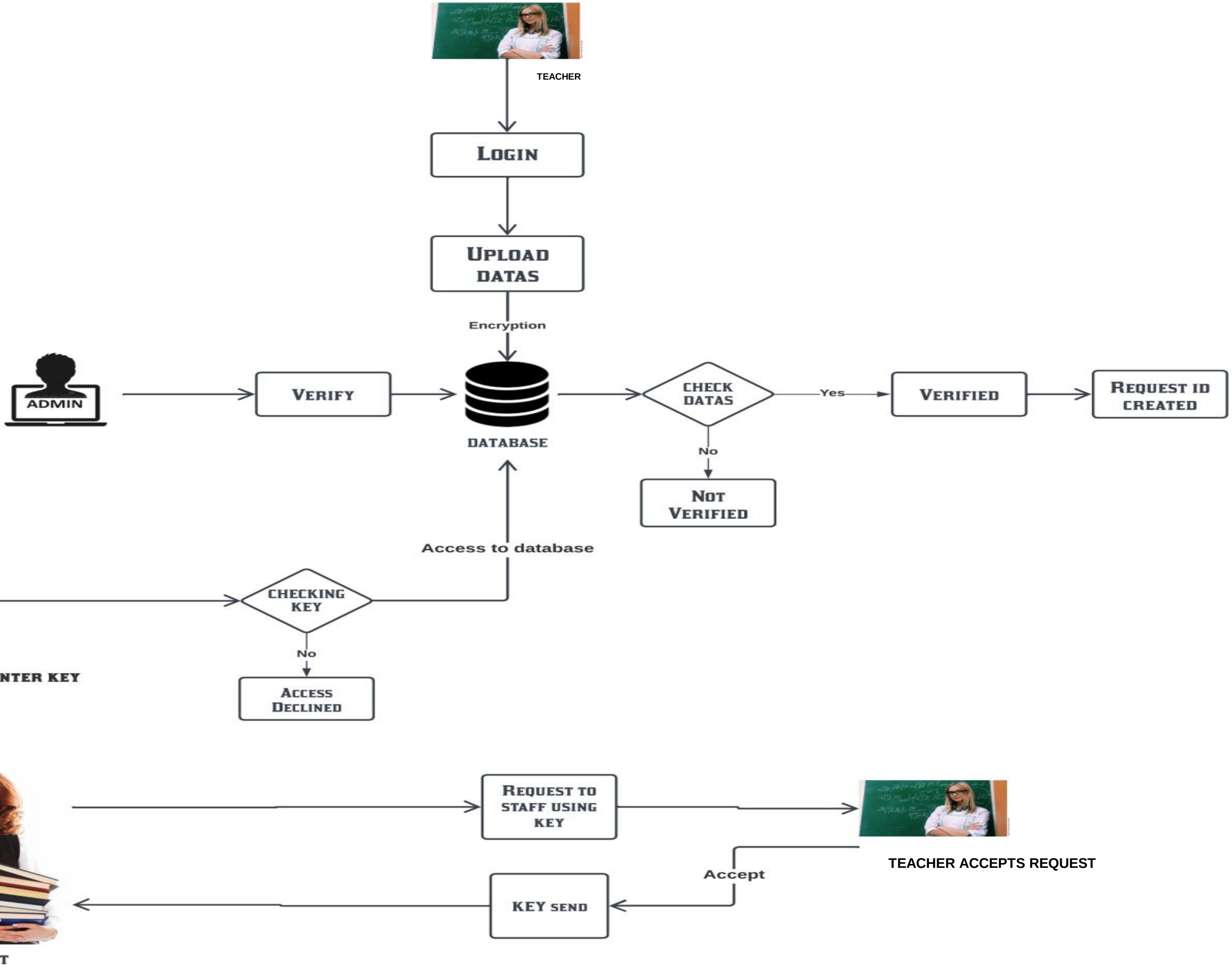
- Moreover, even if the institutions put encrypted data on the **public blockchain**, it still will expose their operation situations and statistical data.
- We firstly use **data masking** for the part of the student’s private data and then encrypt it and store it on the server.
- The user must have the **authorization** of the data owner to query the data, and the verification of the user’s authority is realized using a smart contract. Students can take their documents using **key** from the server.

Blockchain System Algorithm For Students Marks Management

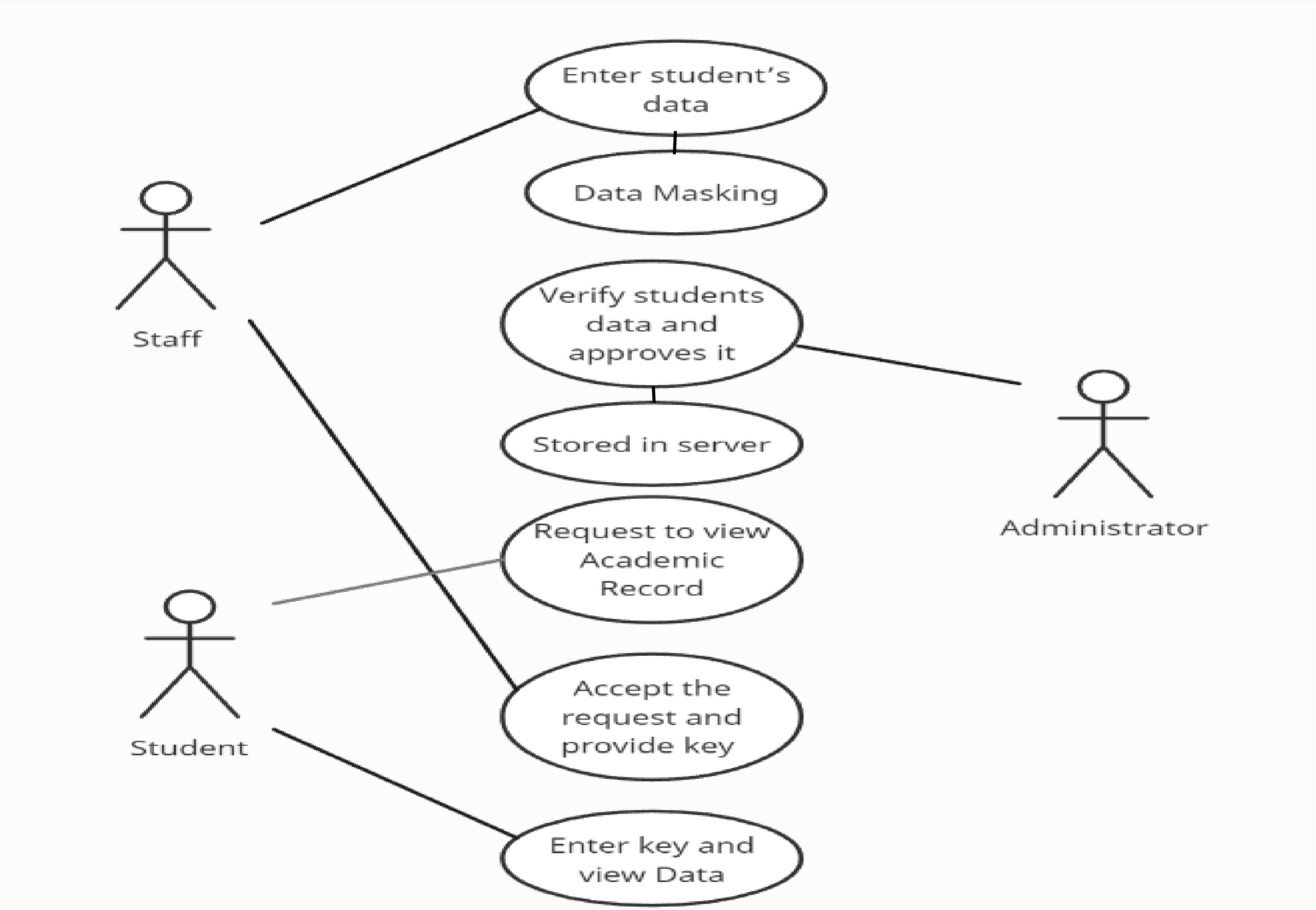
```
1.      studLoginId=XYZ
2.      if(StudEnteredID== studLoginId)
                Login to DB;
                Gives request to view data;
                 if(request accepted && key sent to student)
                      Enters key;
                      View Academic Data;
                 else if(request 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 proposed system.

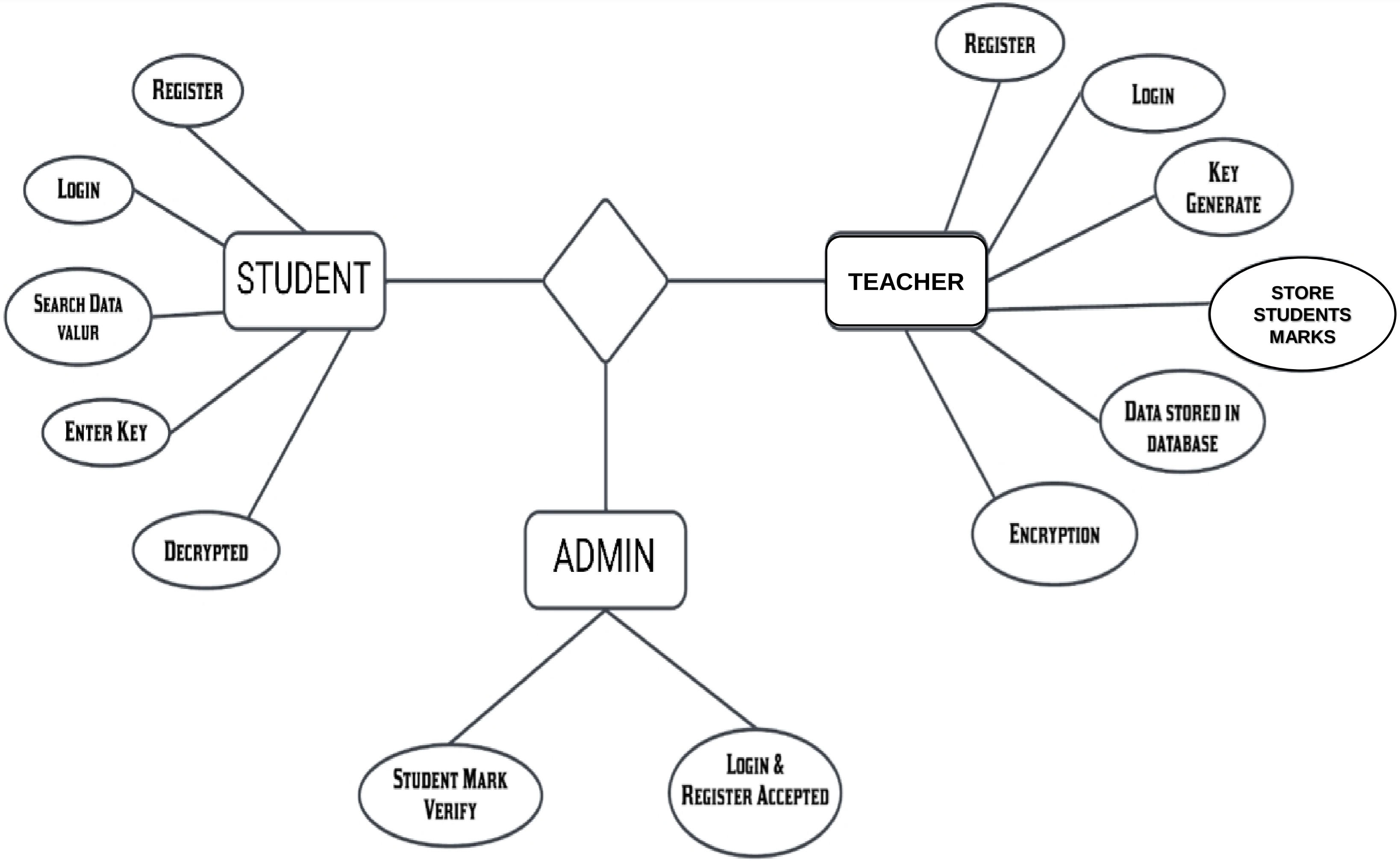
System Architecture



System Design – Use Case Diagram


Enter student's data
Data Masking
Staff
Verify students data and approves it
Stored in server
Administrator
Request to view Academic Record
Student
Accept the request and provide key
Enter key and view Data

System Design – ER Diagram



Module Description

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 **teacher approval**.
- When the staff gives approval, the **respective secret key** for that students data is sent to the student.

Module Description

Encrypted Data Storing:

- The encrypted data is stored in the storage server and their **hash** is put on the blockchain and **keyword** also **generated** for the each student for the security. The amount of data on student education records is huge.
- For the transmission of big data used **Encryption algorithm**. The original records and files are **encrypted and stored** in the storage server. The blockchain database is chosen as the storage server to efficiently store and retrieve data and support encrypted storage of files.

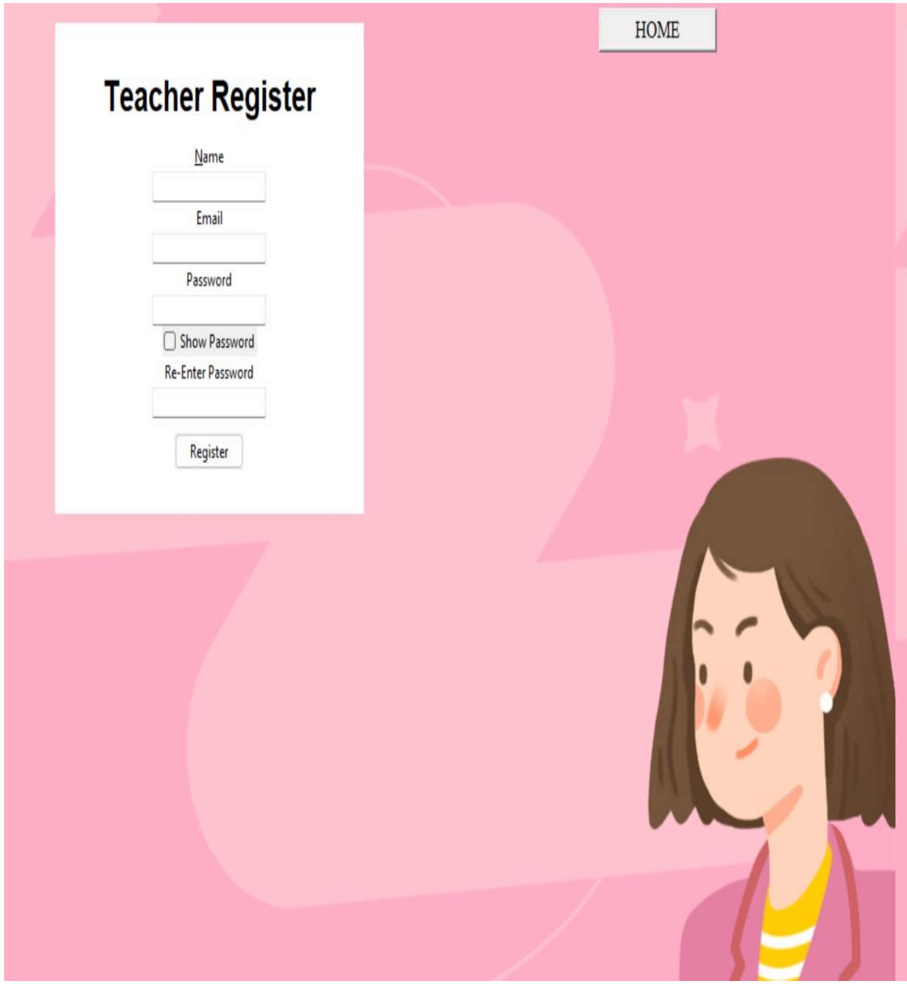
Module Description

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.
- The blockchain is applied in several domains and acts as a **trusted data storage** technology. This technology is often used for information **secure storage** and information traceability, because of its decentralized and **anti-tampering** characteristics.

Result Analysis

- Teacher & User Create Account



HOME

Teacher Register

Name

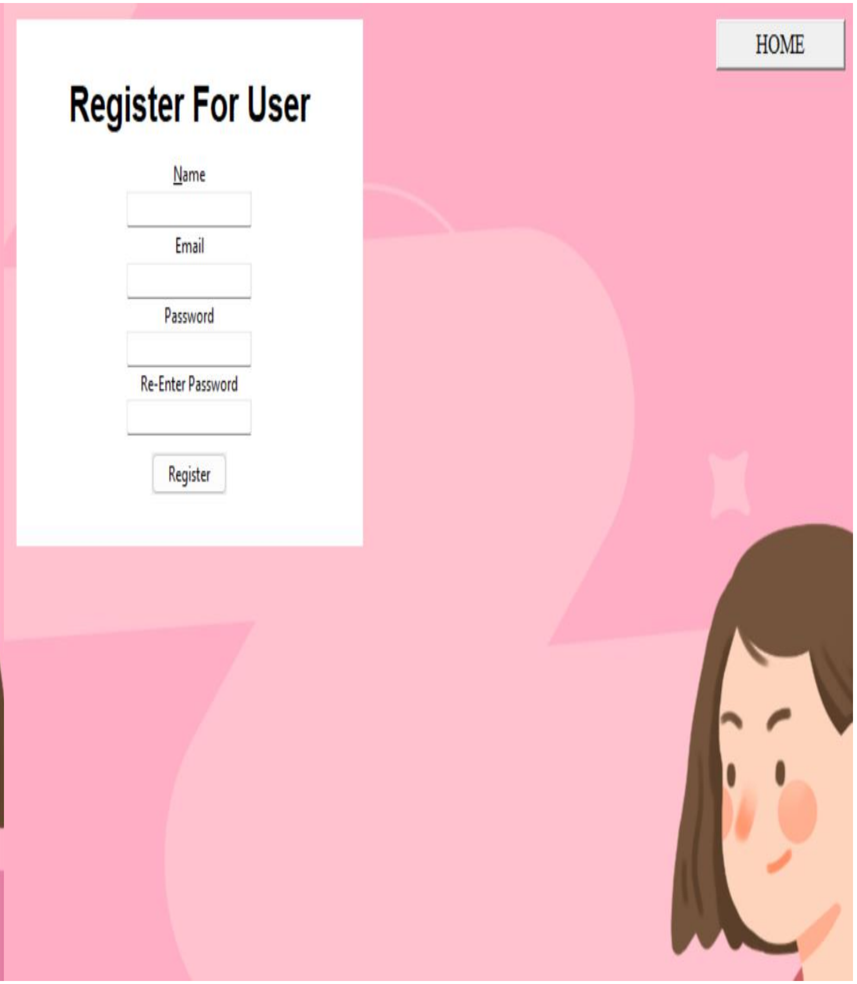
Email

Password

□ Show Password

Re-Enter Password

Register



HOME

Register For User

Name

Email

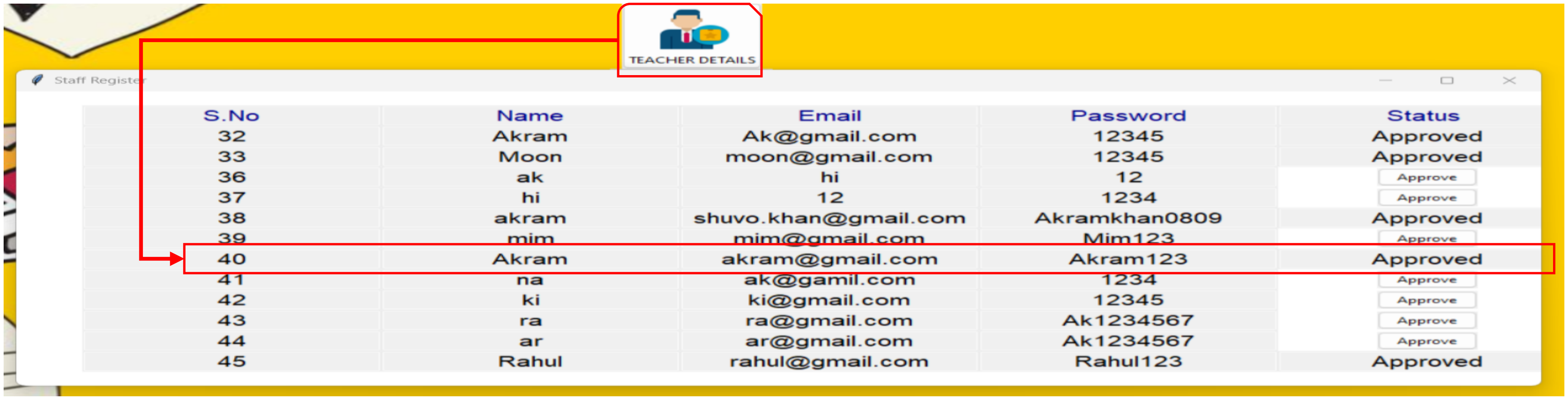
Password

Re-Enter Password

Register

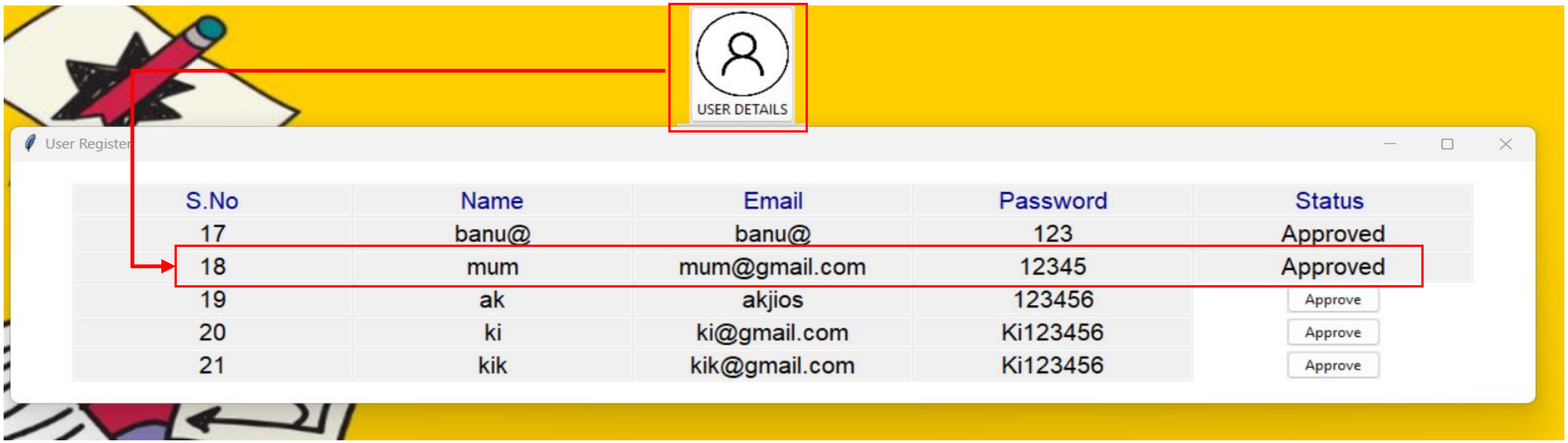
Result Analysis

- Teacher Account Approved by admin



S.No	Name	Email	Password	Status
32	Akram	Ak@gmail.com	12345	Approved
33	Moon	moon@gmail.com	12345	Approved
36	ak	hi	12	Approve
37	hi	12	1234	Approve
38	akram	shuvo.khan@gmail.com	Akramkhan0809	Approved
39	mim	mim@gmail.com	Mim123	Approve
40	Akram	akram@gmail.com	Akram123	Approved
41	na	ak@gamil.com	1234	Approve
42	ki	ki@gmail.com	12345	Approve
43	ra	ra@gmail.com	Ak1234567	Approve
44	ar	ar@gmail.com	Ak1234567	Approve
45	Rahul	rahul@gmail.com	Rahul123	Approved

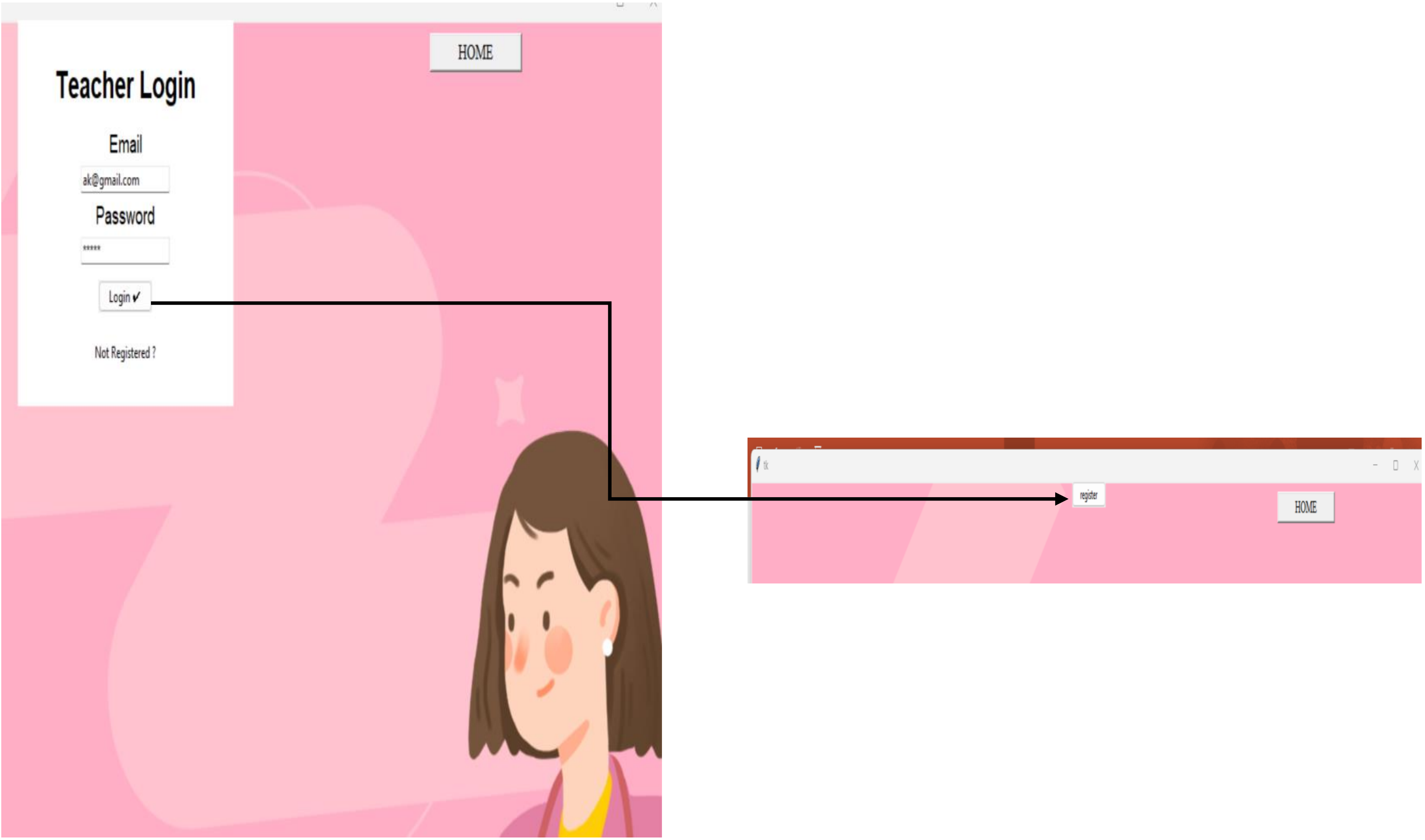
- User Account Approved by admin



S.No	Name	Email	Password	Status
17	banu@	banu@	123	Approved
18	mum	mum@gmail.com	12345	Approved
19	ak	akjios	123456	Approve
20	ki	ki@gmail.com	Ki123456	Approve
21	kik	kik@gmail.com	Ki123456	Approve

Result Analysis

- Teacher login



Teacher Login

Email

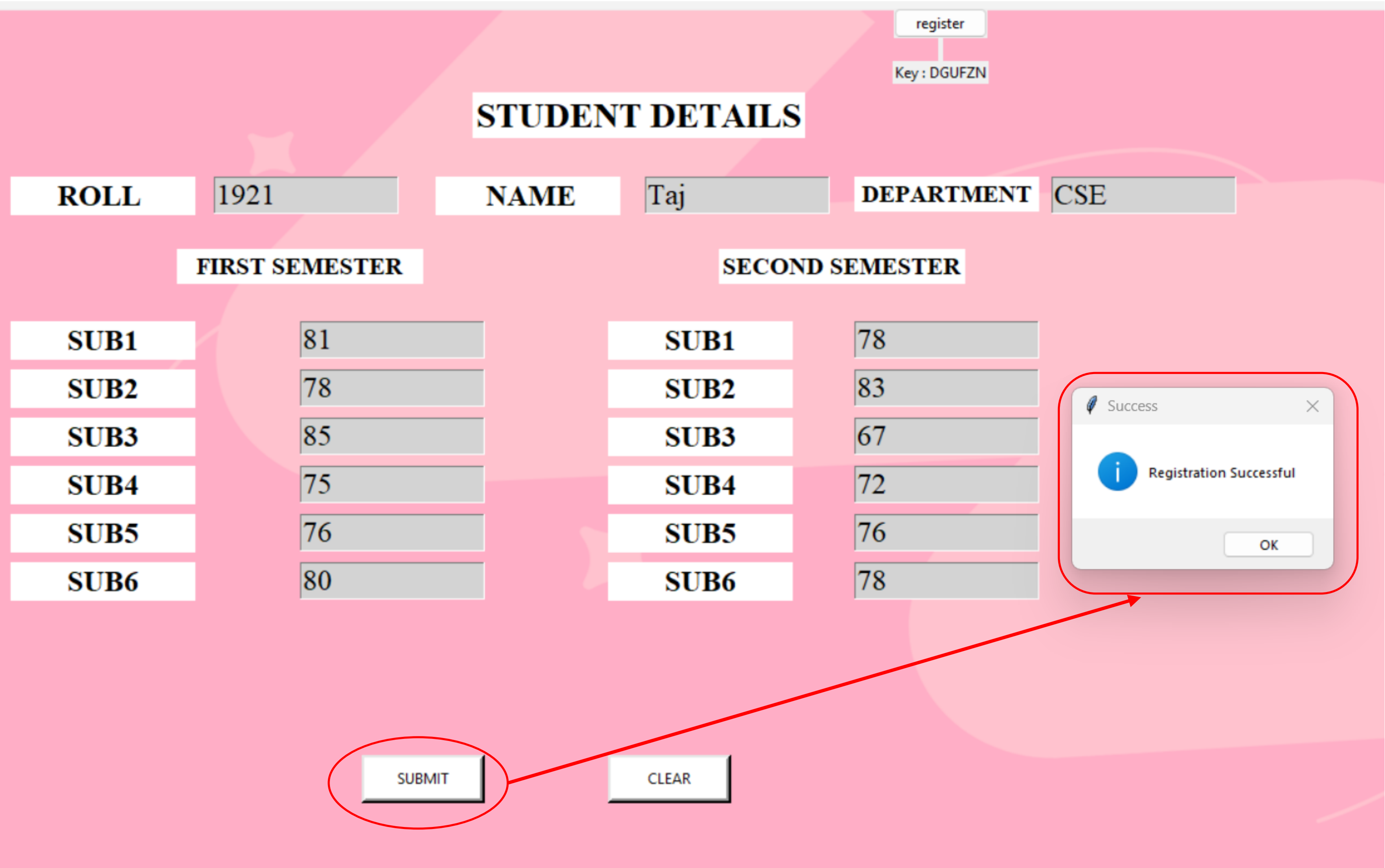
ak@gmail.com

Password

*****

Result Analysis

- Teacher Register student info & Submit Mark



Key : DGUFZN

STUDENT DETAILS

ROLL 1921 NAME Taj DEPARTMENT CSE

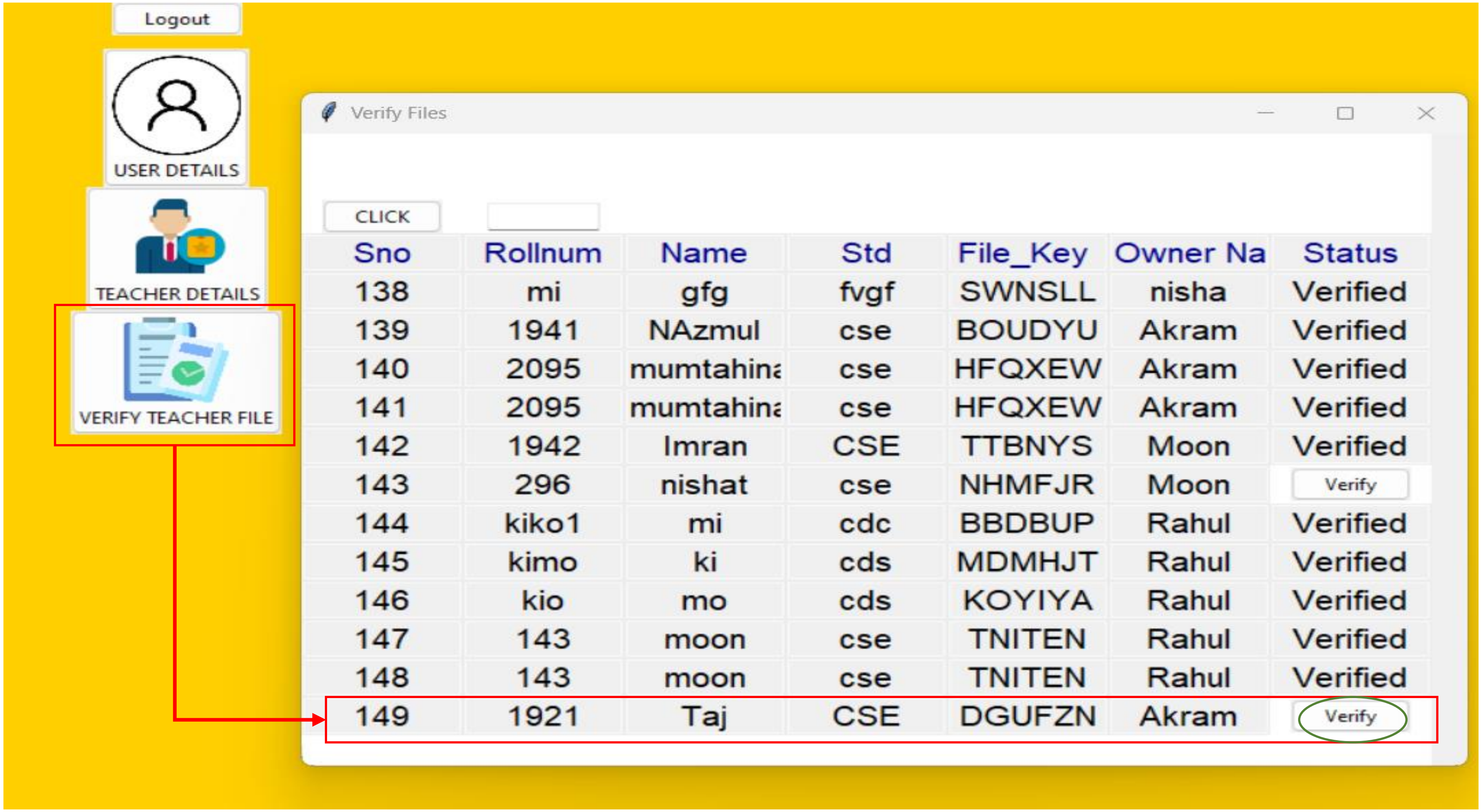
FIRST SEMESTER		SECOND SEMESTER	
SUB1	81	SUB1	78
SUB2	78	SUB2	83
SUB3	85	SUB3	67
SUB4	75	SUB4	72
SUB5	76	SUB5	76
SUB6	80	SUB6	78

Success

Registration Successful

Result Analysis

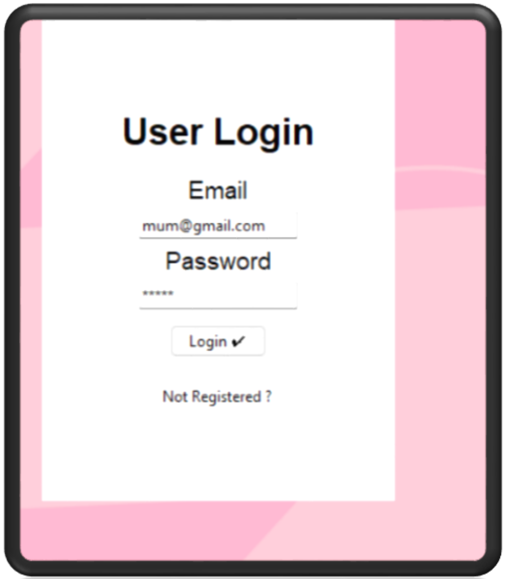
- Admin panel Approve Submitted mark file:



Sno	Rollnum	Name	Std	File_Key	Owner Na	Status
138	mi	gfg	fvgf	SWNSLL	nisha	Verified
139	1941	NAzmul	cse	BOUDYU	Akram	Verified
140	2095	mumtahina	cse	HFQXEW	Akram	Verified
141	2095	mumtahina	cse	HFQXEW	Akram	Verified
142	1942	Imran	CSE	TTBNYS	Moon	Verified
143	296	nishat	cse	NHMFJR	Moon	Verify
144	kiko1	mi	cdc	BBDBUP	Rahul	Verified
145	kimo	ki	cds	MDMHJT	Rahul	Verified
146	kio	mo	cds	KOYIYA	Rahul	Verified
147	143	moon	cse	TNITEN	Rahul	Verified
148	143	moon	cse	TNITEN	Rahul	Verified
149	1921	Taj	CSE	DGUFZN	Akram	Verify

Result Analysis

- User login



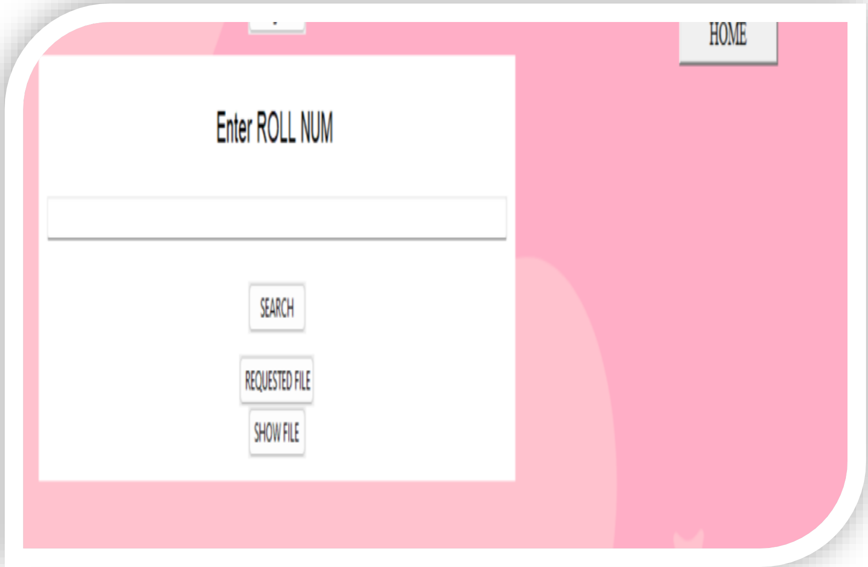
User Login

Email

mum@gmail.com

Password

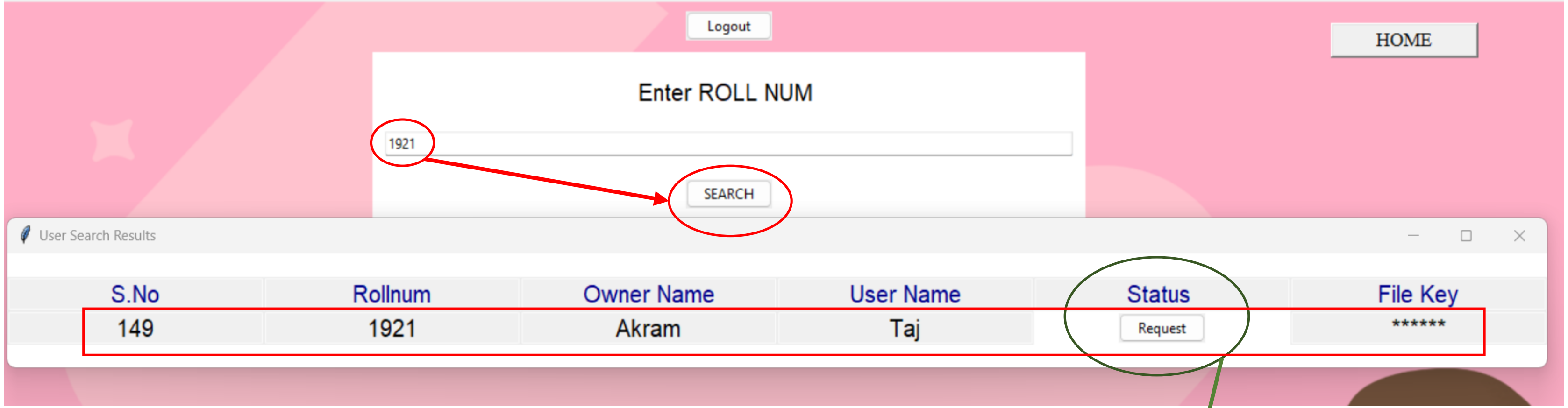
*****



Enter ROLL NUM

Result Analysis

- Search academic data

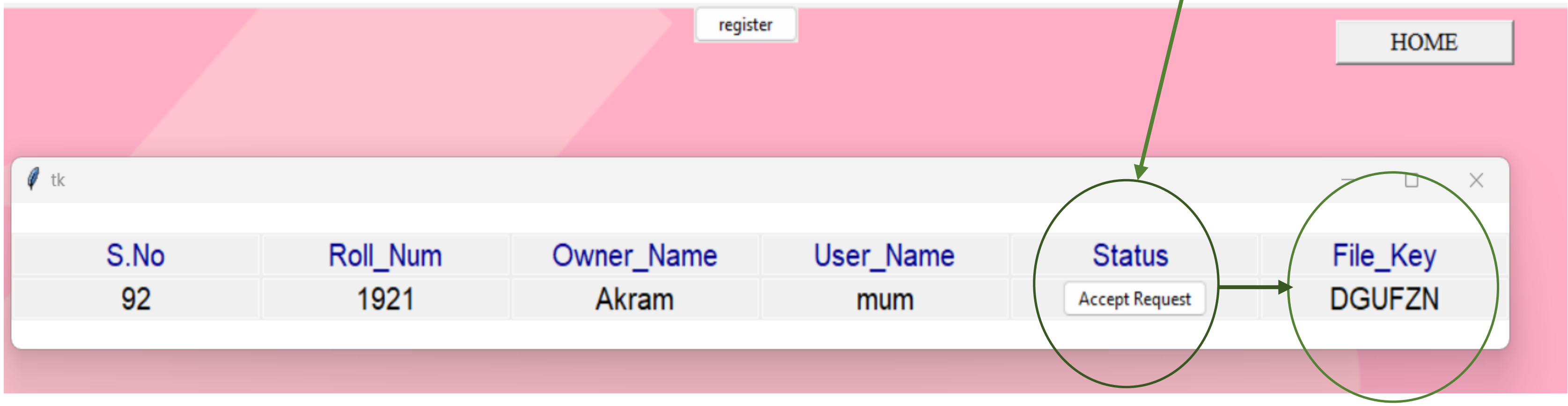


Enter ROLL NUM

1921

S.No	Rollnum	Owner Name	User Name	Status	File Key
149	1921	Akram	Taj	Request	******

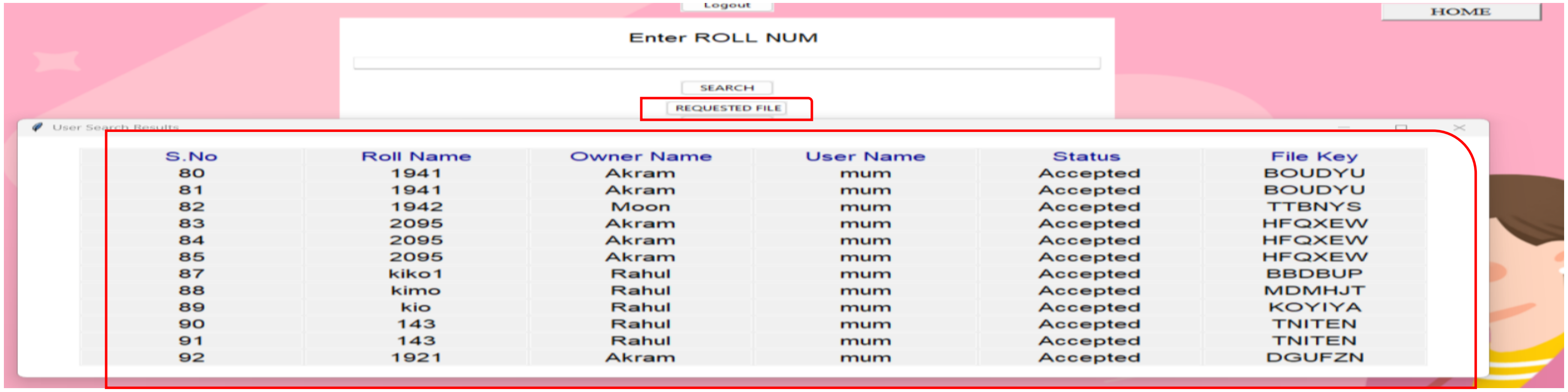
- Teacher provides access & key sent to user



S.No	Roll_Num	Owner_Name	User_Name	Status	File_Key
92	1921	Akram	mum	Accept Request	DGUFZN

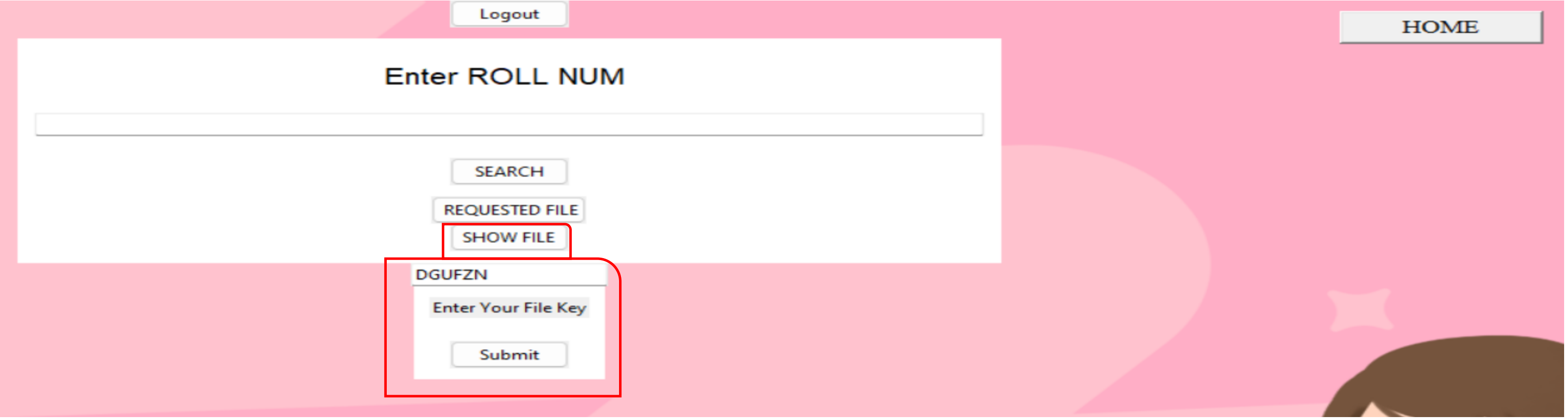
Result Analysis

- User Requested File



S.No	Roll Name	Owner Name	User Name	Status	File Key
80	1941	Akram	mum	Accepted	BOUDYU
81	1941	Akram	mum	Accepted	BOUDYU
82	1942	Moon	mum	Accepted	TTBNYS
83	2095	Akram	mum	Accepted	HFQXEW
84	2095	Akram	mum	Accepted	HFQXEW
85	2095	Akram	mum	Accepted	HFQXEW
87	kiko1	Rahul	mum	Accepted	BBDBUP
88	kimo	Rahul	mum	Accepted	MDMHJT
89	kio	Rahul	mum	Accepted	KOYIYA
90	143	Rahul	mum	Accepted	TNITEN
91	143	Rahul	mum	Accepted	TNITEN
92	1921	Akram	mum	Accepted	DGUFZN

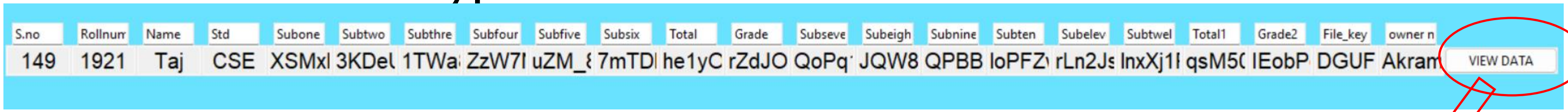
- Enters teacher approved uniqe key



Enter Your File Key: DGUFZN

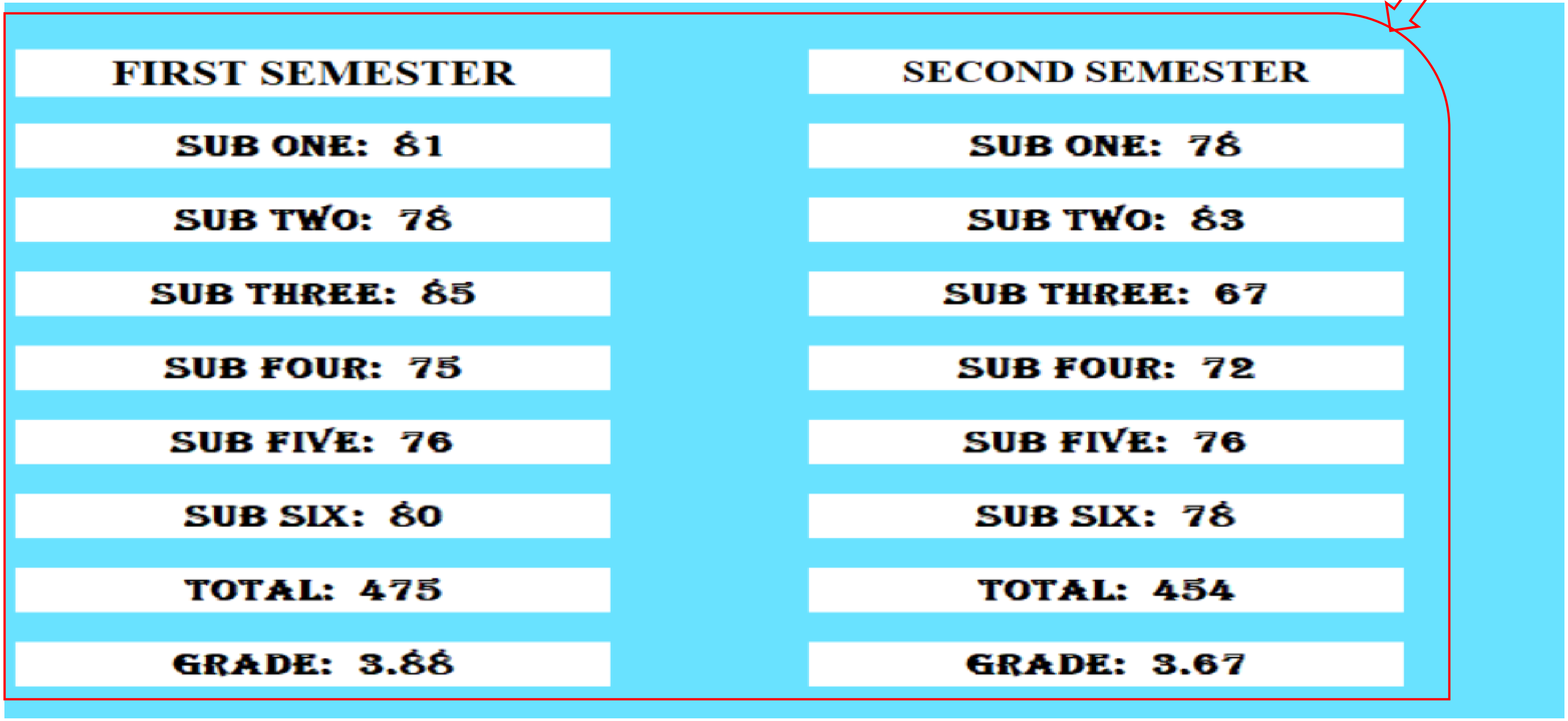
Result Analysis

- Access to Encrypted data



S.no	Rollnum	Name	Std	Subone	Subtwo	Subthre	Subfour	Subfive	Subsix	Total	Grade	Subseve	Subeigh	Subnine	Subten	Subelev	Subtwel	Total1	Grade2	File_key	owner n
149	1921	Taj	CSE	XSMxl	3KDel	1TWa	ZzW7l	uZM_	7mTDI	he1yC	rZdJO	QoPq	JQW8	QPBB	loPFZ	rLn2Js	lnxXj1	qsM5(	IEobP	DGUF	Akram

- Enter Show Button & Seen Academic data



FIRST SEMESTER	SECOND SEMESTER
SUB ONE: 81	SUB ONE: 78
SUB TWO: 78	SUB TWO: 83
SUB THREE: 85	SUB THREE: 67
SUB FOUR: 75	SUB FOUR: 72
SUB FIVE: 76	SUB FIVE: 76
SUB SIX: 80	SUB SIX: 78
TOTAL: 475	TOTAL: 454
GRADE: 3.88	GRADE: 3.67

Result Analysis

Stored Database

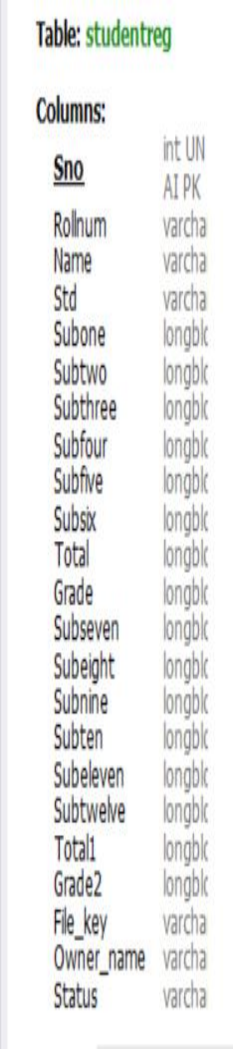
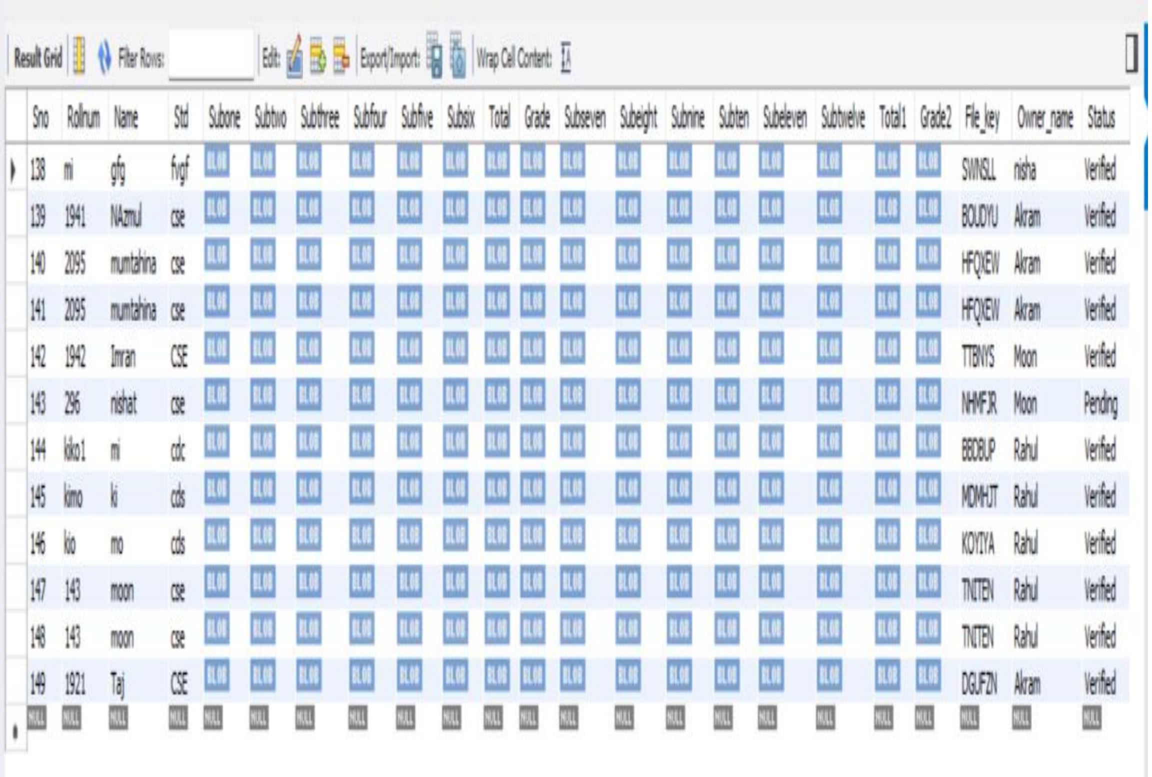


Table: studentreg

Columns:

Sno	int UN AI PK
Rollnum	varcha
Name	varcha
Std	varcha
Subone	longbl
Subtwo	longbl
Subthree	longbl
Subfour	longbl
Subfive	longbl
Subsix	longbl
Total	longbl
Grade	longbl
Subseven	longbl
Subeight	longbl
Subnine	longbl
Subten	longbl
Subeleven	longbl
Subtwelve	longbl
Total1	longbl
Grade2	longbl
File_key	varcha
Owner_name	varcha
Status	varcha



Sno	Rollnum	Name	Std	Subone	Subtwo	Subthree	Subfour	Subfive	Subsix	Total	Grade	Subseven	Subeight	Subnine	Subten	Subeleven	Subtwelve	Total1	Grade2	File_key	Owner_name	Status
138	mi	gfg	fvgf	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	SWNSLL	nisha	Verified
139	1941	NAzmul	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BOUDYU	Akram	Verified
140	2095	mumtahina	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	HFQXEW	Akram	Verified
141	2095	mumtahina	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	HFQXEW	Akram	Verified
142	1942	Imran	CSE	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	TTBNYS	Moon	Verified
143	296	nishat	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	NHMFJR	Moon	Pending
144	kiko1	mi	cdc	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BBDBUP	Rahul	Verified
145	kimo	ki	cds	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	MDMHJT	Rahul	Verified
146	kio	mo	cds	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	KOYIYA	Rahul	Verified
147	143	moon	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	TNITEN	Rahul	Verified
148	143	moon	cse	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	TNITEN	Rahul	Verified
149	1921	Taj	CSE	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	BLOB	DGUFZN	Akram	Verified
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Result Analysis

Stored Database

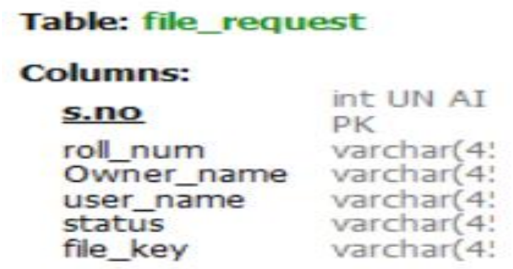
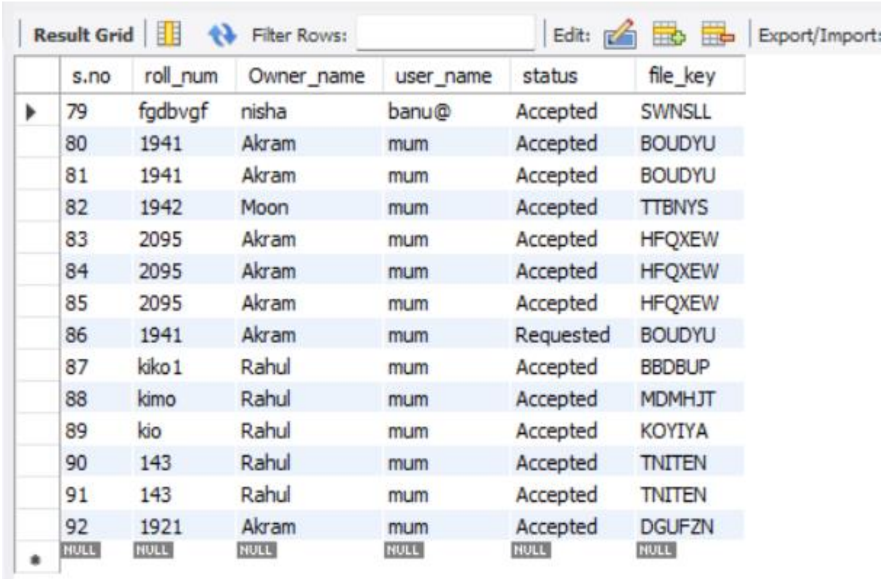


Table: file_request

Columns:

s.no	int UN AI PK
roll_num	varchar(4!
Owner_name	varchar(4!
user_name	varchar(4!
status	varchar(4!
file_key	varchar(4!



s.no	roll_num	Owner_name	user_name	status	file_key
79	fgdbvgf	nisha	banu@	Accepted	SWNSLL
80	1941	Akram	mum	Accepted	BOUDYU
81	1941	Akram	mum	Accepted	BOUDYU
82	1942	Moon	mum	Accepted	TTBNYS
83	2095	Akram	mum	Accepted	HFQXEW
84	2095	Akram	mum	Accepted	HFQXEW
85	2095	Akram	mum	Accepted	HFQXEW
86	1941	Akram	mum	Requested	BOUDYU
87	kiko1	Rahul	mum	Accepted	BBDBUP
88	kimo	Rahul	mum	Accepted	MDMHJT
89	kio	Rahul	mum	Accepted	KOYIYA
90	143	Rahul	mum	Accepted	TNITEN
91	143	Rahul	mum	Accepted	TNITEN
92	1921	Akram	mum	Accepted	DGUFZN
NULL	NULL	NULL	NULL	NULL	NULL

Conclusion and Future Scope

Conclusion

- The EduRSS scheme proposes a secure storage and sharing solution for educational records using blockchain technology, ensuring data integrity and security through a consortium chain and distributed institution authentication. The scheme combines blockchain and storage server for secure storage, and employs an anti-tampering inspection mechanism for record protection.

Future Scope

- Further research can focus on optimizing performance and scalability, enhancing privacy with advanced encryption techniques, incorporating smart contracts or digital signatures, real-world implementation, and evaluating effectiveness in different educational settings to validate the practicality and identify potential challenges.

References

- [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.

ThANk you