



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 12, December 2025

A Blockchain-Based Validation Protocol for Education Data Management System

Vani K T, Musheer Ahmed

P.G. Student, Department of Master of Computer Application, PES Institute of Technology and Management,
Shivamogga, Karnataka, India

Assistant Professor, Department of Master of Computer Application, PES Institute of Technology and Management,
Shivamogga, Karnataka, India

ABSTRACT: To prevent student records from being tampered with or misused A Blockchain-Based Validation Protocol For Education Data Management System is suggested. To guarantee transparency and integrity it incorporates hashing AES-generated secret keys and PBFT validation. Administrators verify staff uploads and student grades are kept in blockchain-like sequences that are only accessible with staff-approved keys. This multi-level controlled workflow guarantees reliable confidential and accurate handling of academic data.

KEYWORDS: PBFT consensus, hashed student marks, AES secret key, blockchain-based educational system, encryption and validation.

I. INTRODUCTION

Digital record-keeping has replaced manual record-keeping in educational institutions increasing efficiency but also raising risks such as data manipulation unauthorized access and system failures because of centralized databases. A Blockchain Based Validation Protocol For Student Data Management System is suggested to safeguard private academic data. It guarantees decentralized tamper-proof and verified records by using blockchain AES-generated secret keys and PBFT consensus. The system consists of three modules: User Staff and Admin. Users request access staff upload marks and create keys and administrators check all entries to ensure safe data flow. This method guarantees long-term data reliability improves transparency and builds stakeholder trust. For each update it also offers full traceability. In general the system establishes a secure and responsible environment for academic data.

II. LITERATURE SURVEY

When researchers started looking into blockchain to address problems with data manipulation and unauthorized access in educational systems the idea of secure academic record management using decentralized technologies first surfaced. Early research concentrated on employing distributed ledgers and cryptographic hashing to guarantee the accuracy transparency and verifiability of student records. [1] suggests using blockchain and IPFS to make verification easier and stop document fraud. [2] focuses on using digital signatures and blockchain timestamps to validate degrees for trustworthy hiring. [3] presents an AES-encrypted Ethereum-based smart contract system for safe certificate storage and verification. [4] combats widespread certificate fraud by swiftly and precisely authenticating credentials using a distributed ledger. In order to do away with unnecessary verification [5] places a strong emphasis on autonomous student identities and decentralized validation methods. When taken as a whole these pieces show how blockchains immutability decentralization and cryptographic security can address problems with forgery illegal access and administrative delays in the processing of educational documents while maintaining confidence among employers institutions and students.

III. PROPOSED METHODOLOGY

To create a safe and impenetrable academic data management system the suggested methodology combines blockchain AES-generated secret keys and PBFT consensus. In order to ensure immutability student marks are first gathered and processed into a blockchain-like sequence where each subject marks is hashed. Instead of encrypting the marks themselves the system uses AES to create a distinct secret key that serves as a secure credential. In order to guarantee that only authorized users can request access staff members upload academic records along with the generated secret key. PBFT consensus verifies each upload preventing manipulation even when malicious or malfunctioning nodes are present. Academic data is fully transparent and traceable thanks to this decentralized method which also removes the drawbacks of conventional centralized databases.

To ensure secure data flow the workflow is split into three modules: User Staff and Admin. Each module has distinct roles. When users request access to their academic records the staff-approved secret key must be issued before they can obtain the readable version. Employees enter grades create a unique key verify user requests and start formatting student data on the blockchain. As the last layer of verification administrators ensure system-wide data integrity and authenticate staff uploads. To prevent unwanted changes every transaction whether uploading approving or verifying is documented on the blockchain. All parties involved are more confident because this multi-level validation framework ensures accurate confidential and reliable handling of academic records.

SYSTEM ARCHITECTURE

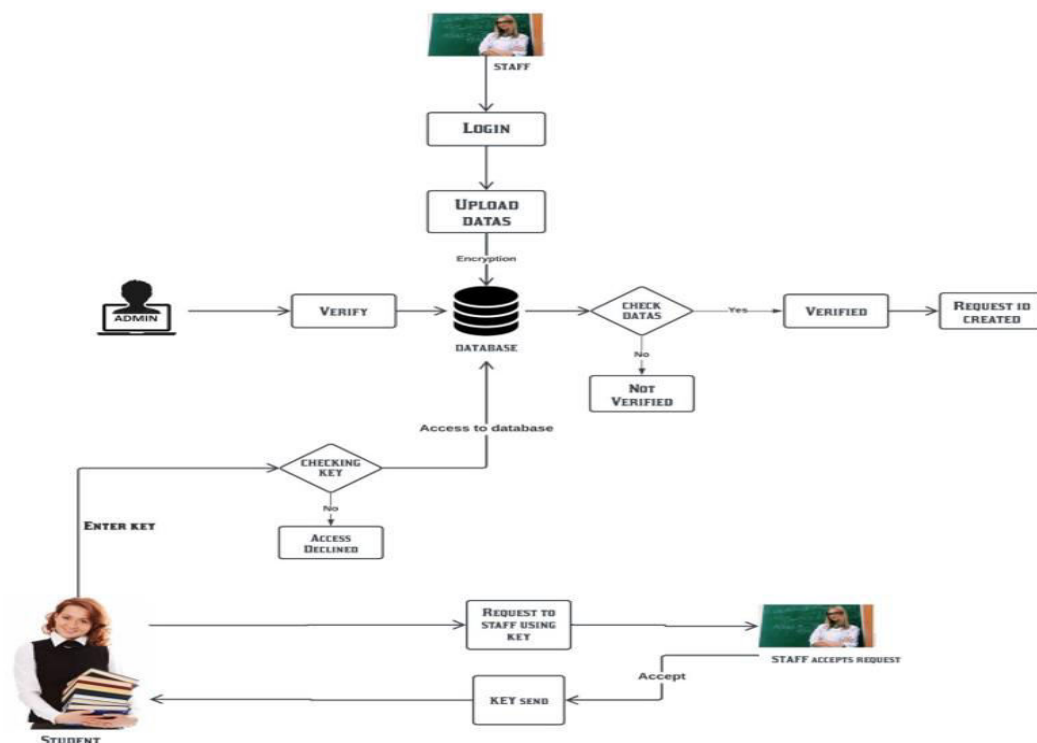


Fig 1. System Architecture

The first step in the system architecture is for staff members to log in and upload student academic data which is subsequently encrypted and saved in the database. After that admin verify these uploaded details and marks them as either verified or not verified. Only authorized users have access to verified records which are safely stored. The staff will provide a secret key that the student must enter in order to view their academic data. Strong security is ensured by the system which verifies the validity of this key and only permits access if it is correct. If the student does not have the secret key they can submit a request to the staff who will review it and if approved send the appropriate key. The student can access their verified academic information with the valid key. A safe regulated and transparent data flow between staff, administrators and students is guaranteed by this architecture.

ALGORITHM USED: The Advanced Encryption Standard algorithm is called AES. A popular symmetric block cipher for safe key generation and data security is AES. It uses a secret key to convert plaintext blocks into ciphertext using fixed-size blocks (128 bits). Longer keys are more resistant to brute-force attacks AES supports key lengths of 128 192 or 256 bits.

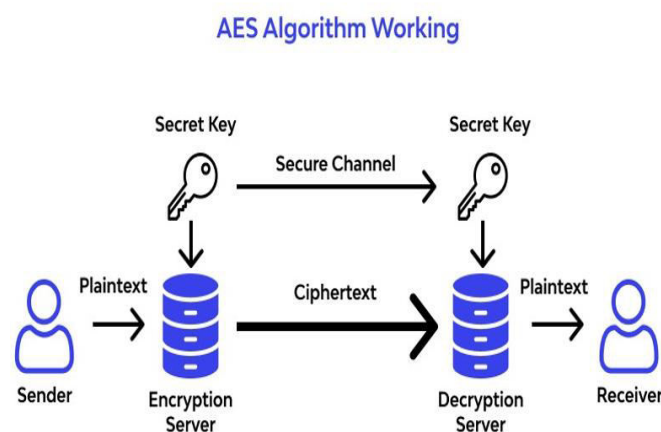


Fig 2. The basic encryption-decryption process

Sender → Ciphertext → Encryption → Decryption → Receiver.

- Plaintext is given by the sender. Normal readable data is entered into the encryption system by the sender. A secret key is used.
- The sender and recipient share a secret key in a secure manner. Because AES is symmetric both encryption and decryption require the same key.
- Ciphertext is created by an encryption server from plaintext. Using the secret key AES transforms the plaintext mathematically in several ways. Ciphertext which appears random and is unintelligible is the result of encryption.
- The ciphertext is sent. The communication channel is used to transmit the encrypted data. It cannot be read without the key even if it is intercepted.

- The recipient employs the same secret key. The decryption server receives the same key from the recipient. Plaintext is restored after decryption. AES restores the origin all readable data by undoing the encryption changes.

SYSTEM TESTING: A Blockchain-Based Validation Protocol For Education Data Management overall and integrated functionality is assessed through system testing. It confirms that all three modules User, Staff and Admin work together seamlessly and that functions like data upload handling secret keys blockchain hashing and record retrieval function as intended. Before the system is deployed this testing makes sure it satisfies functional and security requirements.

Unit testing: Unit testing examines the smallest parts of the system including database operations hashing AES key generation and login validation. To guarantee accuracy and early bug detection every function is tested separately.

Functional testing: Functional testing validates key distribution decryption staff uploads admin verification and user registration. It guarantees that every feature functions as required by the project.

Security testing: Hashes secret keys and student data are protected from unwanted access thanks to security testing. It looks for flaws like SQL injection and brute-force attacks as well as tampering and risky key handling.

Testing of performance: System behaviour under load such as numerous uploads or user requests is measured by performance testing. To guarantee stability and quick performance it measures response time database speed and encryption/decryption effectiveness.

TEST CASES:

Test Case ID	Description	Input	Expected Output	Result
TC-01	Validate user login with valid credentials	Email: student@gmail.com , Password: 12345	User logged in successfully, user dashboard displayed	Pass
TC-02	Handle invalid user login credentials	Email: wrong@gmail.com , Password: invalid	Error message: "Invalid username or password"	Pass
TC-03	Staff uploading student marks	Roll No: 101, Marks entered for all subjects	Marks stored, secret key generated, blockchain hashes created	Pass
TC-04	Admin verifying uploaded student data	Click "Verify" on pending record	Record status updated to "Verified" in system & database	Pass
TC-05	User requesting file using roll number	Roll No: 101 → Click "Request File"	Request sent to corresponding staff, request ID created	Pass
TC-06	Staff accepting user's request	Click "Accept Request"	Secret key sent/made available to the student	Pass
TC-07	User entering correct secret key	Key: Valid AES-generated key	Blockchain data decrypted and actual marks displayed	Pass
TC-08	User entering incorrect secret key	Key: Wrong key	Error: "Invalid key – Access denied"	Pass
TC-09	Display blockchain format data before decryption	Click "Show File"	Encrypted blockchain-styled data shown on screen	Pass

TC-10	Registration form validation	Missing fields (Name/Email/Password)	Display error: "All fields are required"	Pass
TC-11	Logout process for any module	Click Logout button	Session cleared, returned to login page	Pass

IV. EXPERIMENTAL RESULTS

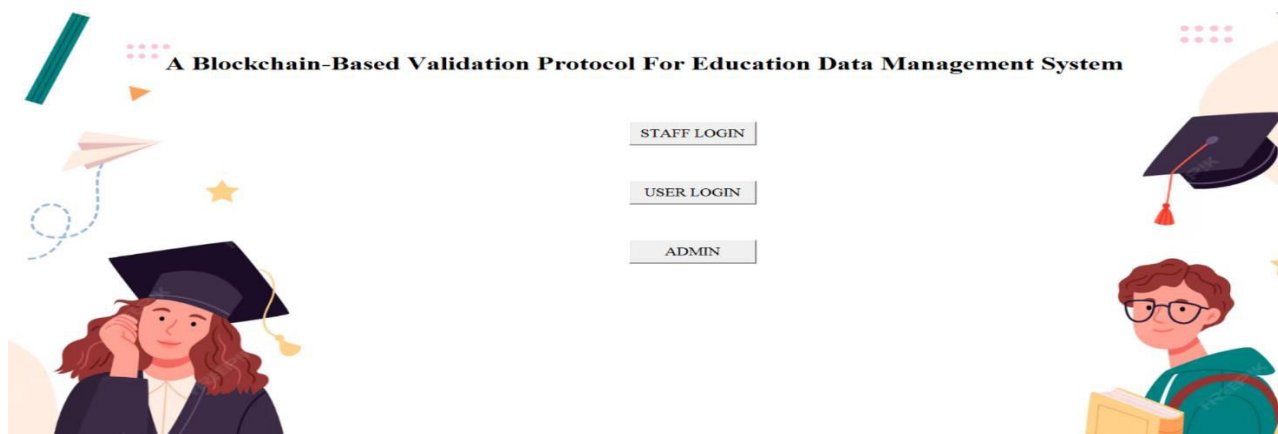


Fig.1 Home Page

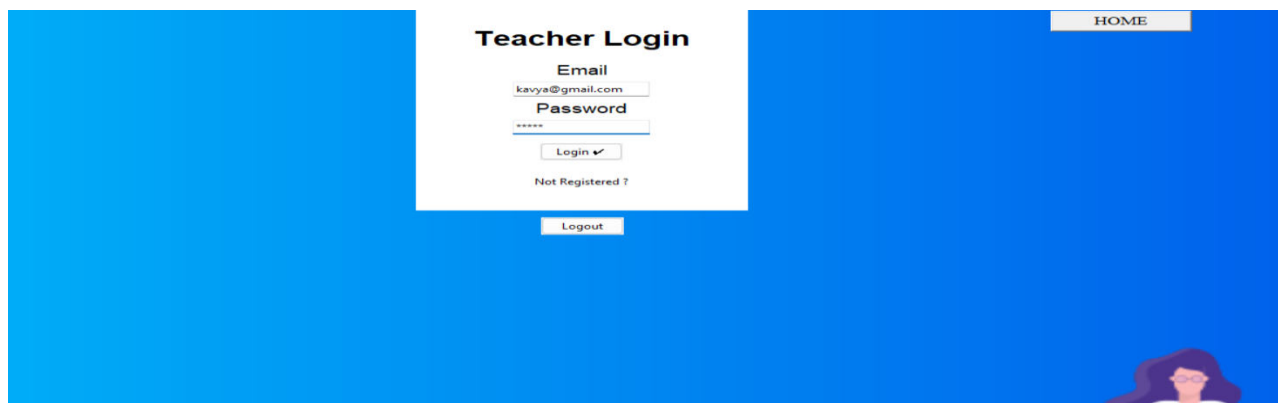
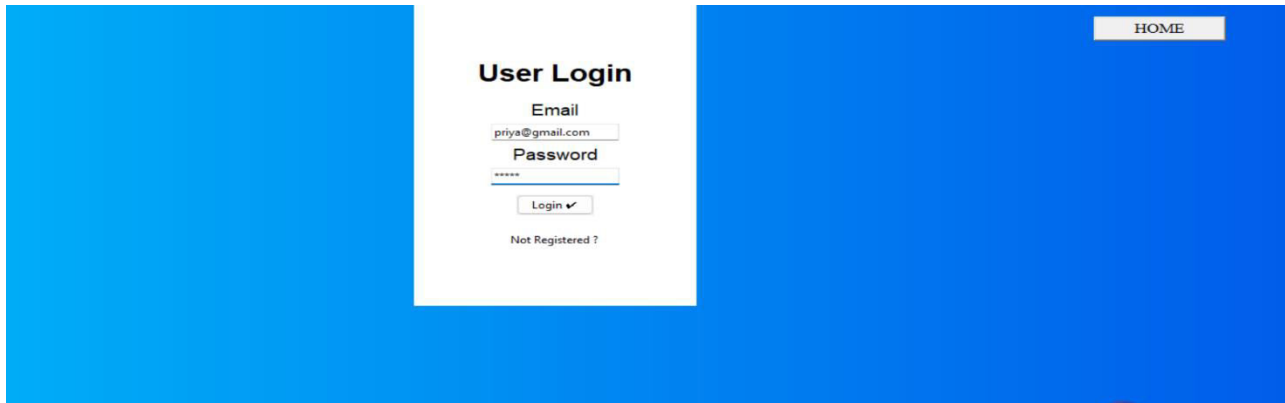


Fig. 2 Staff Login Page



Fig. 3 Staff Uploading The academic data of Respective Student



HOME

User Login

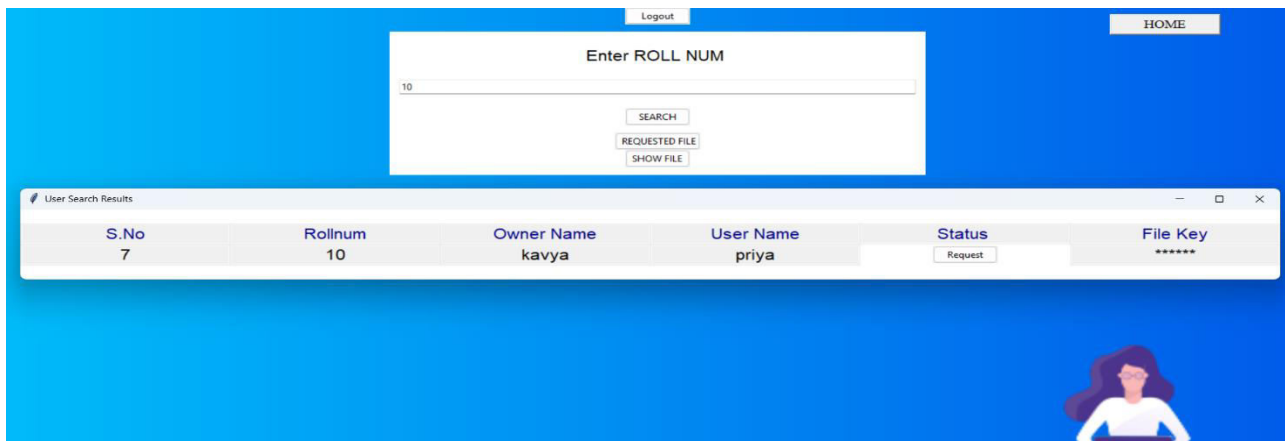
Email
priya@gmail.com

Password

Login ✓

Not Registered ?

Fig. 4 User Login Page



Logout HOME

Enter ROLL NUM

10

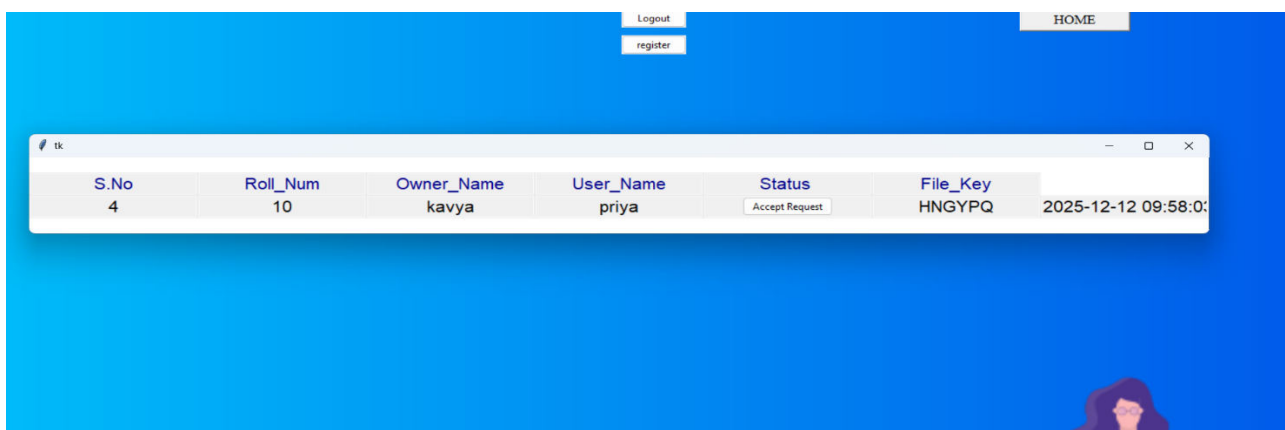
SEARCH

REQUESTED FILE

SHOW FILE

S.No	Rollnum	Owner Name	User Name	Status	File Key
7	10	kavya	priya	Request	*****

Fig. 5 Student Sent a Request for Secret Key



Logout register HOME

S.No	Roll_Num	Owner_Name	User_Name	Status	File_Key	
4	10	kavya	priya	Accept Request	HNGYPQ	2025-12-12 09:58:00

Fig.6 Staff Accept Request From Student and Provide a Secret Key

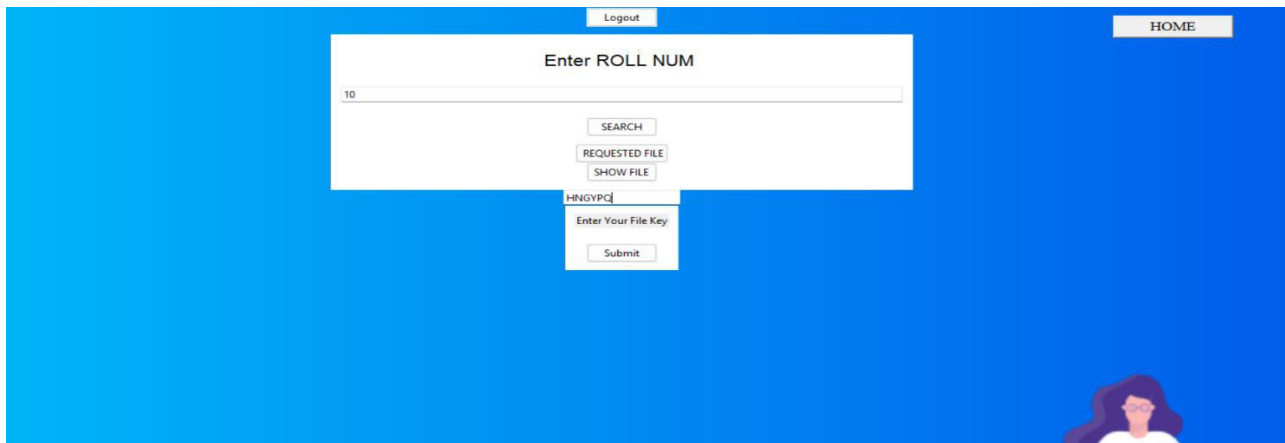


Fig. 7 Student Entering Secret Key for View Academic Data

S.no	Rollnum	Name	Std	Subone	Subtwo	Subthree	Subfour	Subfive	Subsix	Total	Grade	Subseven	Subeight	Subnine	Subten	Subeleven	Subtwelve	Total1	Grade2	File_key	owner nam
7	10	priya	mca	Djk8iA	NBerki	uDWI1	0JvJw	pt4mzi	0h4ec	W4Jy)	r_PgH	fXVu2i	fXVu2i	fXVu2i	fXVu2i	fXVu2i	fXVu2i	fXVu2i	fXVu2i	HNGY	kavya

Fig. 8 Data Shown Like a Blockchain-encryption Form

SEMESTER				
STUDENT DETAILS				
ROLL NUM :		10	NAME :	priya
		STD :	mca	
SUBJECT	INTERNAL (50)	EXTERNAL (50)	TOTAL	RESULT
JAVA	47	34	81	PASS
DBMS	45	32	77	PASS
WEB	48	35	83	PASS
PYTHON	45	30	75	PASS
OS	42	39	81	PASS
Grand Total:				
397				
Overall Result:				
PASS				

Fig. 9 Final Result

V. CONCLUSION

A Blockchain Based Validation Protocol For Education Data Management Systems is an ideal example of how the use of cutting-edge technologies can offer academic record security and transparency. With the use of blockchain-like hashing AES key generation and PBFT-inspired validation the system ensures that student data is reliable and unchangeable. A controlled and accountable workflow has been established through the layering of permissions involving the User Staff and Admin modules. Unauthorized viewing is prevented since students can only access their grades securely with staff approval and confirmation of the correct secret key. An efficient uploading process that encrypts the documents and automatically arranges them into connected blocks benefits the employees. By using verification methods that stop errors before records are made available the administrators maintain complete control. By identifying an attempt to tamper by breaking the hash link the system eliminates the threat of centralized storage. The database only sees data that has been hashed or encrypted meaning that sensitive information is kept safe. While maintaining confidentiality the process permits open communication between students staff and administrators. The automated process of key generation and decryption reduce human error and boosts process dependability. Additionally the approach aligns with the demands of the contemporary education sector where digital data security is becoming increasingly important. The use of cryptography boosts the institutions credibility as well as user trust. Since the design permits future growth it wont be difficult to integrate with more students. Academic information can only be accessed by those with permission thanks to the well-organized request-and-approval system.

REFERENCES

- [1] 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.
- [2] A. F. M. S. Akhter, M. Ahmed, et al., "A secured privacy-preserving multi-level blockchain framework for cluster based vanet," Sustainability, vol. 13, no. 1, 2021, p. 400.
- [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] 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.
- [5] 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. 24
- [6] 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.
- [7] B. Pillai and K. Biswas, "Cross-chain interoperability among blockchain-based systems using transactions," Knowledge Engineering Review, vol. 35, 2020, p.1.
- [8] A. Derhab, M. Guerroumi, A. Gumaï, 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.
- [9] 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.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details