IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

Block chain Based Secure Student Data Management System

Mrs. M. Anitha[1], M. Maha Lakshmi[2], SK. Rifath[3], T. Bindu Naidu[4]

M. Tech, CSE, BWEC, Bapatla, India[1]

B. Tech, CSE, BWEC, Bapatla, India[2]

B. Tech, CSE, BWEC, Bapatla, India[3]

B. Tech, CSE, BWEC, Bapatla, India[4]

Abstract: The secured data management systems in the education sector cannot be over emphasized. The storage and sharing model of student education records data still faces many challenges in terms of privacy protection and efficient transmission. The use of block chain technology has been proposed as solution to address the challenges faced in the current centralized education sector. The Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to ensure credible and secure data management. The need for precise privacy data is achieved by constructing a dictionary. Cryptographic techniques such as AES is used for encrypted storage of data and keywords. The random secret key is generated for each record through hashing technique for data security storage in block chain . The storage server store database management system with block size 256 bits using SHA-256. Smart contract provides protection for data keywords, the storage server stores data after data masking. Security analysis, privacy protection and computational cost shows that high efficiency and low cost can be achieved. Meanwhile, this scheme has better robustness compared to other educational records data sharing models

I. INTRODUCTION

Educational records describe their education-specific processes. These records are of great importance for the further study and career of an individual. The essential attribute of records is primitive, which enables records to restore the actual historical situation, so these records are essential to the students themselves, education institutions and potential employers. With the development of information technology, educational records have been digitized. Compared with the traditional paper physical records, digital records are stored on the storage medium which has a high degree of variability, hence such records could be easily modified during the processes of storage, transmission, and sharing. Centralized storage and management mode is usually adopted, which makes systems that use this mode vulnerable to various attacks. Besides 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, without any form of interoperability. Moreover, a server failure could easily cause a data loss or leakage. Therefore, in order to protect personal information, institutions usually adopt security policies to restrict the access and sharing of records. However, there is a lack of secure and effective record sharing mechanisms among institutions. Students may experience difficulties when they transfer from one institution to another, while still preserving their completeness of courses from the previous institution. In cases when students apply for postgraduate programs in another education institution, this process requires the provision of past educational records, such as, courses grades, award certificates and so on, by which time they have completed the previous stage of education, left the previous education institution, etc., but usually, such students have no access to the online educational records system. In this case, they have to visit the previous institution to request a paper copy of their educational records. The data owner encrypts the education records data and stores them with cloud storage, and stores the index and record summary of the education records data into the block chain. For the remote server, we determine that it is malicious, so we firstly use data masking for the part of the student's private data and then encrypt it and store it on the cloud 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. the keyword dictionary sent by the data owner, the smart contract can perform the query record, can be published in the block chain.

II. LITERATURE SURVEY

A. Counterfeit Detection of Documents using Blockchain

Document verification is a domain that involves various challenges and monotonous processes to authenticate the documents. The verification for each type of document is to be processed in distinct ways. The issuing of documents is not transparent and hence fake documents can be created. Documents or certificates generated by organizations play a

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

vital role for students. With the increase of forged documents, credibility of both the students and the organization is imperilled. Verifying a document takes some time and also requires more human resources to request for the confirmation of the data provided. Managing documents or records often comes at the cost loss of data or document counterfeits. In this paper, we aim to enhance the document verification process using block chain. We propose a system which uses the Interplanetary File System [IPFS] protocol and also a peer- to-peer-network for storing and sharing data in a distributed file system. By using this block chain technology, we can provide a more secure and efficient digital certificate validation.

B. Education Degree Fraud Detection and Student Certificate Verification using Blockchain

To verify the authenticity of an academic degree and certificates we propose a system which employs a digital signature scheme and timestamps using blockchain technology. As the number of universities and tertiary education students, the number of graduates is constantly increasing. Due to this verification process of these degree certificates generates a lot of new job opportunities. The sudden changes in the technology and development of new technologies like blockchain is booming, the implementation of blockchain using block certs software provides us a solution of plausible business models. In this paper we showcase two financial models balancing where the service rates is been balanced between graduates and employer as to main stakeholders of that service. A proof check of certificates for students is done at low cost and an easy check of the authenticity of the certificate is done from and trustable source while recruiting by the employer.

C. Development and Evaluation of Blockchain based Secure Application for Verification and Validate Academic Certificates

Academic degrees are subject to corruptions, system flaws, forgeries, and imitations. In this paper we propose to develop a blockchain smart contract-based application using Ethereum Platform, to store, distribute and verify academic certificates. It constitutes a trusted, decentralized certificate's management system that can offer a unified viewpoint for students, academic institutions, as well as for other potential stakeholders such as employers. The article describes the implementation of three main parts of our proposed solution that includes: verification application, university interface and accreditor interface. This application avoids administrative barriers, makes the process of deployment, verification, and validation of certificates faster, efficient, and more secure. Additionally, it offers confidentiality of the data by using AES encryption algorithm before creating transactions and allows bulk submission of multiple academic certificates.

D. Revolutionizing Verification and Management of Educational Certificates with Self-Sovereign Student Identities using Blockchain

Educational Institutions have come a long way in transforming education systems, but they still require a better and fraud-proctored system to address the issues that exist even today. The need of a single secure platform for all educational stakeholders such as, e-learning platforms, academic institutes, universities and students to avoid re-verification and maintaining immutable record of a student's digital assets are a driving fuel to significantly transform current system. The main objective of the work is to highlight the existing issues of fraudulent degrees, redundancy in verification process of documents, lack of validation for authenticity of certificates in the current education sector, lack of single authorised identity for students and resolve them using decentralization, immutability, traceability, consensus mechanism and other features of blockchain. The existence of third parties between Universities, institutions and students gets eliminated by the distributed nature that blockchain offers. The consensus mechanism employed will make sure that only authenticated data is put on chain, quelling the fraud certificates that often end up getting amassed at the employer's desk. The intent is to design a prototype to test the applicability of blockchain in solving above stated issues.

III. PROPOSED SYSTEM

A novel scheme is proposed, which integrates educational records storage and sharing among education institutions enabled by blockchain, storage servers and smart contracts. 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. 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 cloud 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 cloud.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

IV. SYSTEM IMPLEMENTATION

A. User Search Process

Generate user information Info, use private key Sk(U) to encrypt information CT(U) = Encrypt(Sk(U), Info). Write multiple search keywords into Q,run CQ = Encrypt (Sk(U), Q) obtain the encrypted keywords CQ and send the request Req = Send(Q, CT(U), P k(U)) to the data owner.The user obtains the key of the educational institution through Sk = Decrypt(Key, Sk(U)), decrypts the file D = DENC(CD, Sk), and finally obtains the student's education records.

B. 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.

C. Encrypted Data Strong

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 cloud database is chosen as the storage server to efficiently store and retrieve data and support encrypted storage of files.

D. Data Accessing by Entering Data

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.

E. Consensus Phase

After user obtains the student data, the smart contract submits the query record to the verification node, which requires the digital signature of user and educational institution. If the transaction is passed by the verification node through the PBFT consensus algorithm, it will be published and recorded on the blockchain. The record can also be used to prove the authenticity and credibility of the data source when external institutions do related research based on students educational records.

V. RESULTS

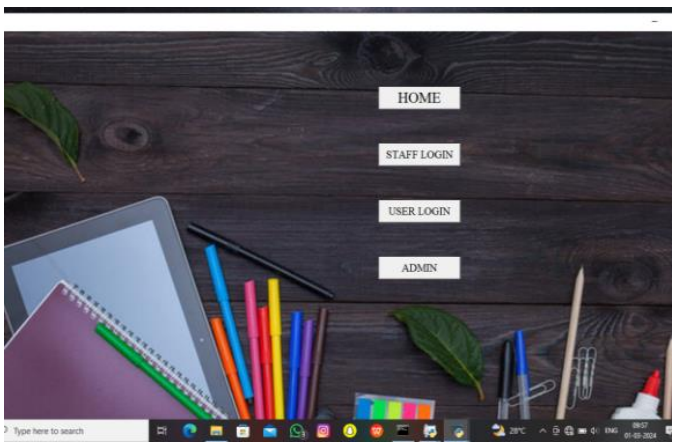

Fig. 1 Home Page

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

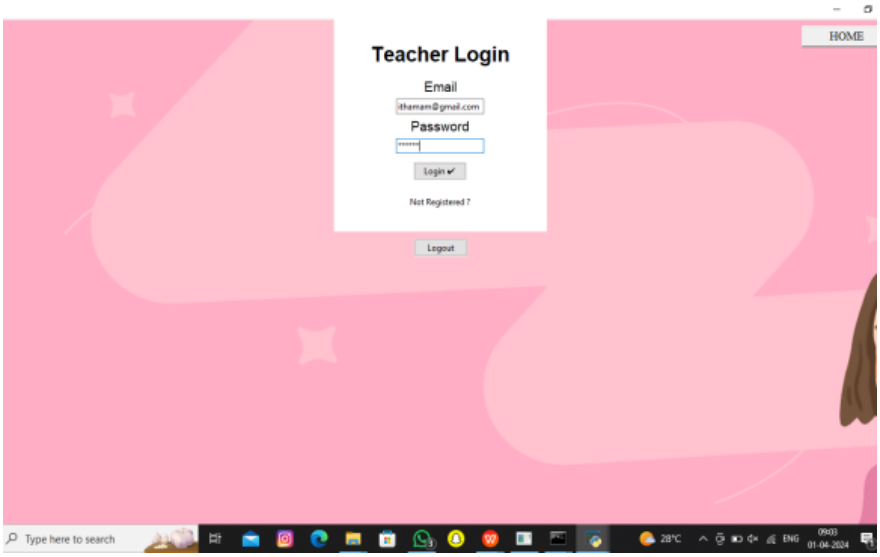

Fig. 2 Teacher Login Page

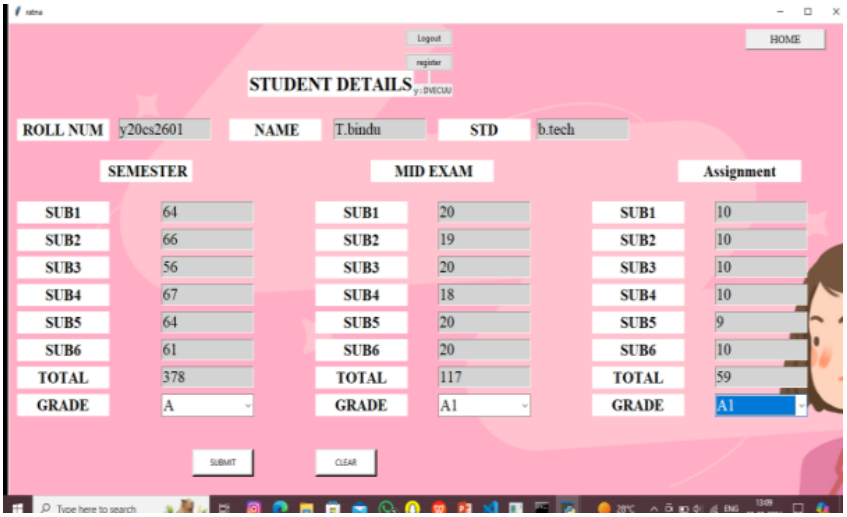

Fig. 3 Academic Data Page

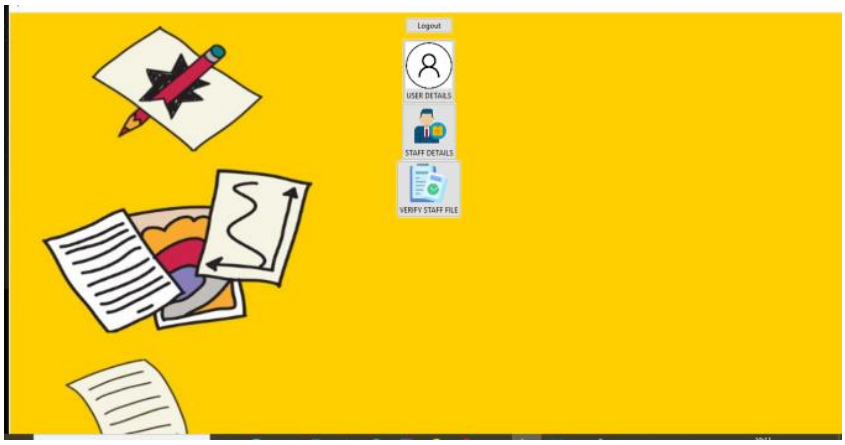

Fig. 4 Admin Page

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

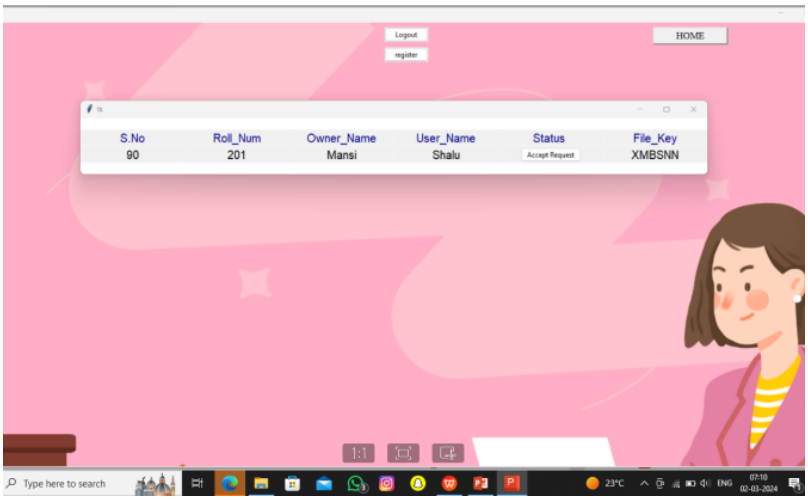

Fig. 5 Staff Provides access&Key Page

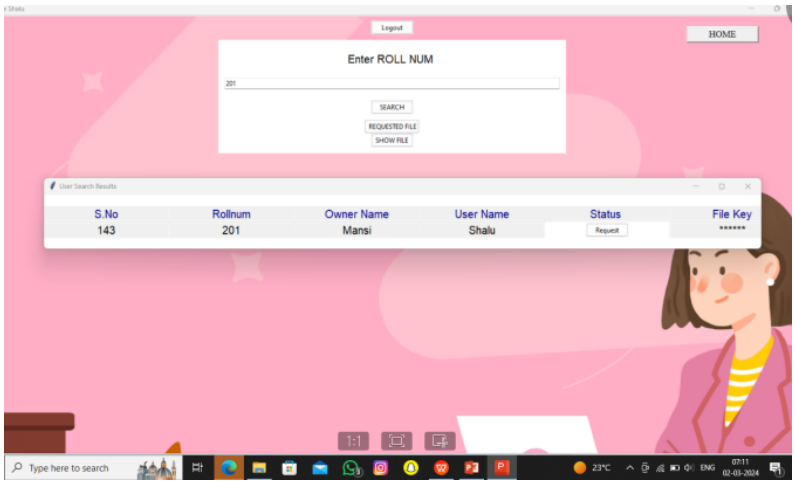

Fig. 6 Request Academic Data

VI. CONCLUSION

this project,Aiming at the need for protection and sharing of educational records, a secure storage and sharing scheme based on the blockchain, referred to as EduRSS is proposed in this paper. In our proposal, the integrity and security of the data can be ensured by the consortium chain between institutions. A distributed institution authentication mechanism is proposed to ensure the security of blockchain nodes. Secure Storage is achieved by combining Blockchain and Storage Server. For records sharing, to achieve cross-institutional sharing of educational records, smart contracts are introduced, the permissions of record and the records of the sharing process are managed by smart contracts on the blockchain. Finally,an anti- tampering inspection mechanism is employed to protect records in the storage server. In theory, the proposed scheme with higher security, efficiency, and credibility, but further research works are still needed.

VII. FUTURE SCOPE

We still need a secure platform to manage these smart contracts in use. Since many smart contracts have been applied in our scheme and there may be more in the future, there is a need for a professional platform for deploying, scheduling, and managing smart contracts. In addition, the security of smart contracts is one of our main focus for future research. More functions need to be introduced into the framework, such as support for educational record certification of external institutions or employers, and encrypted retrieval of educational records. The storage of the off-chain data in our scheme depends on the centralized storage serverIn the future, decentralized storage technologies such as the Inter Planetary File System (IPFS) and Storage will be used.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11355

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]. 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.

[4]. 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.

[5]. 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.

[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]. 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.