BLOCKCHAIN-BASED ACCESS CONTROL MODEL FOR STUDENT ACADEMIC RECORD WITH AUTHENTICATION

Submitted in partial fulfillment of the
requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

PRASATH S (Reg.No - 39110794)
RAJESH R (Reg.No - 39110829)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHISALAI,
CHENNAI - 600119

APRIL - 2023

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with —All grade by NAAC Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **Prasath S (Reg.No - 39110794) and Rajesh R (Reg.No - 39110829)** who carried out the Project Phase-1 entitled **"BLOCKCHAIN-BASED ACCESS CONTROL MODEL FOR STUDENT ACADEMIC RECORD WITH AUTHENTICATION"** under my supervision from January 2023 to April 2023.

Internal Guide

Dr. M. MAHESWARI

Head of the Department

Dr. L. LAKSHMANAN, M.E., Ph.D.

Submitted for Viva voce Examination held on 24.04.2023

Internal Examiner **External Examiner**

DECLARATION

I, **Prasath S (Reg.No- 39110794),** hereby declare that the Project Phase-1 Report entitled **"BLOCKCHAIN BASED ACCESS CONTROL MODEL FOR STUDENT ACADEMIC RECORD WITH AUTHENTICATION"** done by me under the guidance of **Dr. M. Maheswari** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**.

DATE:24.04.2023 Prasath.s

PLACE: Chennai **SIGNATURE OF THE CANDIDATE**

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management** of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph. D**, **Dean**, School of Computing, **Dr.L. Lakshmanan M.E., Ph.D.,** Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. M. Maheswari** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my phase-1 project work.

I wish to express my thanks toall Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

Schools and Institutions maintain student's records and certificates for future needs like verification and credit transfer. These procedures are carried out manually to ensure that documents and the data are valid and non-tampered, which usually needs more energy and time. Converting these procedures into digital form minimizes the time and energy consumption but with the cost of high-security risks. Storing student's data on a centralized system has problems like data breaches due to human error, injection attacks, and buffer overflow attacks, and even if the server gets damaged physically, it'll take more time to repair and recover the damaged data and start running. But in blockchain technology, the data stored in blocks with a cryptographical code of the previous block, gives enhanced security compared to the traditional database. If anyone tries to tamper or hack the data, the decentralized technology can easily recognize the modification and prevent it from happening. Three layers of blockchain are being employed to give the Academic Record System the highest level of security possible. Data Storage Blockchain is the third layer of the model which stores the student's records. The Access Control Model Blockchain is the second layer, which includes additional layer security to the Data Storage Blockchain as it records all the activities around it. And the final layer is the Authentication Blockchain, which is based on Ethereum Blockchain. This model validates transaction using Smart Contracts given to them, creating a new user and validating the login process securely for the Authority, Institution, and the Student for accessing the Data Storage.

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

In recent years, there has been an increasing interest in utilizing blockchain technology for secure and transparent data storage and management. One area where this technology holds significant promise is in the field of education, specifically in the management of student academic records. The current system for managing these records is often complex and vulnerable to security breaches and data loss. In response to these challenges, a blockchain-based access control model for student academic records with authentication has been proposed. This model aims to provide a secure, transparent, and efficient method for storing and sharing academic records while ensuring the privacy and confidentiality of student data.

Five important blockchain benefits: **(i) Enhanced Security:** Your data is sensitive and crucial, and blockchain can significantly change how critical information is viewed. By creating a record that can't be altered and is encrypted end-to-end, blockchain helps prevent access. Information is stored personal data and using permissions to prevent access. Information is stored across a network of computers rather than a single server, making it difficult for hackers to view data.

(ii) Greater Transparency: Without blockchain, each organization has to keep a separate database. Because blockchain uses a distributed ledger, transactions and data are recorded identically in multiple locations. All network participants with permissioned access see the same information at the same time, providing full transparency. All transactions are immutability recorded, and are time-and date-stamped. This enables members to view the entire history of a transaction and virtually eliminates any opportunities for fraud. **(iii) Instant Traceability:** Blockchain creates an audit trail that documents the provenance of an asset at every step on its journey. In industries where consumers are connected about environmental or human rights issues surrounding a product – or an industry troubled by counterfeiting and fraud – this helps provide the proof. With blockchain, it is possible to share data about provenance directly with customers. Traceability data can also expose weakness in any supply chain – where goods might sit on a loading dock awaiting transit.

(iv)Increased Efficiency and Speed: Traditional paper-heavy processes are time-consuming, prone to human error, and often requires third meditation. By streamlining these processes with blockchain, transaction can be completed faster and more efficiently. Documentation can be stored on the blockchain along with transaction details, eliminating the need to exchange paper. There's no need to reconcile multiple ledgers, so clearing and settlement can be much faster. **(v) Automation:** Transactions can even be automated with "Smart Contracts", which increases your efficiency and speed the process even further. Once pre-specified conditions are met, the nest step in transaction or process is automatically triggered. Smart contracts reduce human interventions as well as reliance on third parties to verify that terms of a contract have been met. In insurance, for documentation to file a claim, the claim can automatically be settled and paid.

By handling a decentralized storage system, data storage and authentication can equate parallelly, which makes the data stored more secure, contrary to the traditional database. Three layers of blockchain are employed to make this approach more secure. To authenticate the users who need to access the data, Authentication Blockchain is used. Here, the Authentication Blockchain was made using open source Ethereum based model. Smart Contracts are used for creating and verifying the users and their credentials. All transactions should satisfy the Smart Contract in order to complete the job. The Data Storage Blockchain stores the student data on the blockchain in blocks. These blocks are interlinked using hash values between the blocks. If the data ever got tampered, this model identifies the change by comparing the hash values of the blocks. And the Access Model stores all the changes made to the data storage blockchain. The user can see what was changed and when using this access model. The main objective is to store the student's credit information using blockchain technology as secure as possible.

CHAPTER 2

LITERATURE SURVEY

This problem statement has been extensively studied over the past 5 years by researchers and to create a solution, and all their solutions vary from analyzing various patterns.

The work of Ali, S.I.M., Farouk, H. and Sharaf, H. [1] Their proposed models emphasize on the data availability; represented in student's ability to access all of their data at any time. This paper proposes three models for using blockchains to implement fully functional SIS that maintains transactions such as students and faculty member's records, course registration records and student marks. Using the proposed models pushes towards a genuine certificate can be easily issued and published to the interested parties without the need for involving a centralized administration. The three models avoid the need for miners because there is no incentive for miners. Instead, the consensus protocols allow one full node to verify and add a transaction, then broadcasts it to other full nodes.

Dwivedi, S.K., Amin, R., Das, A.K. [2] Their proposed models emphasize the benefits associated with EHR systems examples like public healthcare management, online patient access, and patients' medical data sharing. Depending on the actual deployment, data in the ledger can be stored in the encrypted form using different cryptographic techniques. Hence, preserving data privacy. Users can also protect their real identities in the sense of pseudo-anonymity. In this paper we perform a symmetric literature review of blockchain approaches designed for EHR systems, focusing only on the security and privacy aspects. It has some complex key management and the risk of ID/PWD (password of users) and data leakage. It also high-cost PKE computation. Data leakage on purpose or accidentally by customers who have decrypted the requested data. High-cost on MPC computation replicas of data to requestors may cause the tamper or leakage of data without the owner's permission.

Saito, K. and Watanabe, S [3] This project is about selective disclosure is an important mechanism to protect the privacy of users by hiding unnecessary parts of certificates or other documents, and providing just partial disclosure for proof. We propose an XML format for documents that can hide arbitrary elements using a cryptographic hash function and salts, which allows to be partially digitally signed and efficiently verified, as well as a JSON format that can be converted to such XML. The documents can be efficiently proven to exist by representing multiple such structures as a Merkle tree and storing its root in blockchain. Their proposal will bring computationally simple compared to the known practice and other related work. Another advantage is that it is easy to handle structured documents, and allows digital signatures on parts of the documents.

Gurreiroa., Ferreira., F [4] In this paper, we describe a case study that integrates a university management system with a blockchain-based application that enables certificates to be deployed on the Ethereum blockchain so that it can be easily integrated with a blockchain solution for verifiable certificates. Its main aims at the creation, piloting, and evaluation of a decentralized platform for the storage, sharing, and verification of education and employment verification of education and employment qualifications. They used the blockchain solution for verifiable qualifications certificates. This solution uses blockchain technology and smart contracts, to support decentralized verification of higher education certificates.

Zheng, K., Zheng, L.J., Gauthier, J., [5] The combination of blockchain and privacy protection can reduce the risk of lax third-party supervision, ensure data security and effectiveness at a certain extent, and have broader application value. With distributed storage, anonymity, and the advantages of data consistency, it is widely used in supply chain finance.

Satoki Watanabe and Kenji Saito [6] uses the Merkle tree method for storing information and also uses it to retrieve a specific set of requested data to be validated. It authorizes partial signature to assure the authenticity of the data or the information received.

Norah Alilwit [7] uses a unique digital id to retrieve information for the user since it is more secure than the traditional authentication method. All types of legal documents can be stored and verified using a digital database.

Joberto S. B. Martins and Emanuel E. Bessa [8] stores the transcripts and certificates of the students on the blockchain. So, the transfer and verification of the documents can be a pushover compared to traditional hard copy verification, which takes more time and resources.

Patrick C. K. Hung, Qusay H. Mahmoud, Ahmed Badr, and Laura Rafferty [9] makes the application open to students as they can access their certificates and send them for verification and scholarships. The coordinator verifies the provided data before being added to the blockchain.

Omar Musa, Shu Yun Lim, Abdullah Almasri, and Pascal Tankam Fotsing [10] uses distributed ledger technology, by which authentication was more secure and data modification.

Xin Liu and Wentong Wang, Ning Hu [11], shared their services between domains through authentication. A Certificate Authority will verify the authenticity of the user.

Hui Lin, Xiaoding Wang, Fu Xiao, Quanwen He [12], made the consortium blockchain stores all transactions between the private blockchains for future reference.

Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, and Ahmed Serhrouchni [13], the Certificate Authority verifies and revokes unwanted certificates by analyzing the validity of the certificates.

Hrithik Gaikwad, Navil D' Souza, Rajkumar Gupta, and Amiya Kumar Tripathy [14] uses the OCR module to extract details from the requested certificates. The extracted data is converted to a hash value and then verified by the server.

Shenyi Huang [15] uses asymmetric cryptography techniques for verification. It uses a private key to access data and a public key to verify data.

Xiangwu Ding and Jianming Yang [16] used an access model, which gives access to the data according to their role. The role varies based on the attributes assigned.

Aastha Chowdhary, Shubham Agarwal and Dr. Bhawana Rudra [17] converts the certificate to complex hash values and then compares the hash value to an existing certificate in the server.

Jintao Zhu, Yinzhen Wei, and Xiaoxiao Shang [18] used a decentralized blockchain to store the data securely. The data verification is done by using the public key and comparing the nonce of the data.

Oiza Salau, and Steve A. Adeshina [19] use the Interplanetary file system hash method for accessing and verifying data.

Untung Raharja, Qurotul Aini, Ninda Lutfiani, Fitra Putri Oganda, and Ahman Ramadan [20] used Distributed Ledger Technology for storing and verifying the data.

The main goal of our approach is the proposal of a new certificate revocation and status verification scheme. Our approach relies on a public blockchain to store and disseminate the revoked certificates information. Some problem of our solution is, widely used in slow speed, high energy consumption increasing the cost of the attack. Indeed, we work to provide an alternative solution that avoids the downloading of all the LRSIs from the server.

2.1 INFERENCES FROM LITREATURE SURVEY

In the above survey the blockchain stores data that is permanently recorded and encrypted using cryptographic technologies into decentralized blocks. Cryptographic procedures used in block generation and connecting blocks improve the security of each blockchain transaction, and the data recorded on the blockchain are immutable records whose states cannot be changed once they are generated certificates can be easily issued and published to the genuine certificates can be easily issued and published to the interested parties without the need for involving a centralized administration. Keep sensitive data accountability and integrity cryptographic functions can protect user's data return the control right of private data back to user use the data and it can protect the real identity of the user.

Protect the privacy and integrity of sensitive data using blockchain. It has some complex key management and the risk of ID/PWD (password of users) and data leakage. User data is stored in the private blockchain cloud against confidentiality and integrity attacks it is flexible and easy to integrate user data using simple Indicator-centric schema as storage model. But it is high-cost MPC computation replicas of data to requestors may cause the tamper or leakage of data without the owner's permission.

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

Although it has a number of advantages, regular Access Control technology presupposes that all the information is stored at a server, where all the processed data is centralized. This means providers might gain unauthorized access to the data and control operations might gain unauthorized access to the data and control operations of their clients' devices. Thus, when outsourcing your company's security to a third party, you have to put a lot of trust in them. Then again, in case you want to change your cloud-based Access Control operator, what happens to the data they possess? How can you be sure that it won't be tampered with?

Another downside of a legacy Access Control is that it's vulnerable to various attacks and in some cases can easily be broken. The existing system just gives access to other universities or institutes. And the blockchain contains multiple student data. This makes the student data accessible without the knowledge of the student. This system doesn't have any authentication for the user and also doesn't verify the document of an individual.

The management of student academic records faces various challenges that have yet to be fully addressed. One of the main concerns is security and privacy, as the current system is vulnerable to data breaches and loss, which can compromise the confidentiality of student data. Inefficient data management is also a significant issue, with multiple parties accessing and sharing academic records, resulting in time-consuming and inefficient data management. Another challenge is the lack of transparency, making it difficult for students to track and verify the authenticity of their academic records.

Limited accessibility is also a problem as the current system is often inaccessible to students who have migrated to different regions or countries, making it difficult for them to access their academic records. Moreover, the current system is susceptible to fraudulent activities, such as creating fake academic records or altering existing records. To address these challenges, a blockchain-based access control model for student academic records with authentication has been proposed as a potential solution. It provides a secure and transparent method for storing and sharing academic records while ensuring the privacy and confidentiality of student data.

CHAPTER 3

REQUIREMENT ANALYSIS

3.1 FEASIBILITY STUDIES / RISK AMALYSIS OF THE PROJECT

A feasibility study and risk analysis of a blockchain-based access control model for student academic records with authentication would involve examining the technical, economic, and legal viability of the project, as well as identifying potential risks and developing strategies to mitigate them.

3.1.1 Technical Feasibility

The technical feasibility of the project would involve assessing the capability and reliability of the proposed blockchain-based access control model. This would include evaluating the performance and scalability of the blockchain technology, determining the level of security and privacy that can be achieved with the model, and identifying any technical limitations or obstacles that may arise during implementation.

3.1.2 Economic Feasibility

The economic feasibility of the project would involve examining the financial implications of developing and implementing the blockchain-based access control model. This would include estimating the costs of development, deployment, and maintenance of the model, as well as identifying potential revenue streams or cost savings that may be realized through its implementation.

3.1.3 Legal Feasibility

The legal feasibility of the project would involve evaluating the regulatory and legal framework surrounding the storage and sharing of student academic records. This would include examining relevant laws and regulations regarding data protection, privacy, and security, as well as ensuring compliance with any applicable industry standards and guidelines.

3.1.4 Risk Analysis

The risk analysis would involve identifying potential risks associated with the development and implementation of the blockchain-based access control model, such as security breaches, data loss, and system failures. Strategies would be developed to mitigate these risks, such as implementing robust security protocols, conducting regular audits and reviews, and developing contingency plans in the event of a system failure or data breach.

Overall, a feasibility study and risk analysis of a blockchain-based access control model for student academic records with authentication would involve a comprehensive examination of the technical, economic, and legal feasibility of the project, as well as the identification and mitigation of potential risks.

3.2 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

3.2.1 Blockchain

Blockchain can be better be understood as an immutable database and laid the foundation of the whole project. It provides a trusted environment where actions have done are visible and can't be tampered with.

3.2.2 Ethereum

Ethereum is a decentralized open-source blockchain featuring smart contract functionality. Ethereum is itself the best example of blockchain and it’s a cryptocurrency system which is the most widely used and is the nest expensive cryptocurrency after bitcoin.

3.2.3 Smart Contract

Smart Contract piece of code that runs on a blockchain when a user performs some action. A smart contract is written in many different languages including low-level languages like C++, Java, and high-level languages like Solidity which is closely similar to TypeScript.

3.2.4 Solidity

Solidity is an object-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms, most notably, Ethereum. It is closely similar to TypeScript but with more specific data types.

3.2.5 IPFS

The Inter Planetary File System is a peer-to-peer network for storing and sharing data in a distributed file system. IPFS use content-addressing to uniquely identify each file in a global namespace connecting all computing devices.

3.2.6 Metamask

Metamask is an extension for accessing Ethereum enabled distributed applications or "Dapps" in your browser. The extension injects the Ethereum web3 API into every website's JavaScript context so that Dapps can read from the blockchain.

3.2.7 Ganache

Ganache is used for testing Solidity contracts on a personal Ethereum Blockchain. It by default provides an easy setup for spinning up a network with around ten users with each having 100 eths on their account. These accounts can be used to mimic the transactions between the users.

3.2.8 Truffle

Truffle provides easy compilation, linking, deployment, and binary management of smart contracts written in solidity language.

3.2.9 Rinkeby

Rinkeby provides an Ethereum test network which is used by developers to test their code and perform some actions. It just provides an environment that works on proof of authority, unlike Ethereum which works on proof of work.

3.2.10 NodeJS

NodeJS is used to write backends and is responsible for serving frontend pages, assets and managing user authentication using JWT (Json Web Token). It also has web3 as a dependency which allows us to run solidity code on frontend.

3.2.11 React

React is used to write our frontend and serves a purpose of providing a better user experience in the frontend for the end user as it provides functionality like no page reload on page switch and fast loading of sites. Keeping security in mind we have added Next.js which compiles and saves html pages in the backend and provides fast user experience along with better SEO for react pages and security as it doesn't reveal and backend details on the user end.

TABLE 3.2.1 SOFWTARE REQUIREMENTS

Operating Environment	**Tools**
Local Blockchain	Ganache v2.5.4
Server Environment	NodeJS v18.13.0
Pipeline for Blockchain	Truffle v.5.4.29
ETH Wallet	Metamask v10.22.2

3.3 SYSTEM USE CASE

A blockchain-based access control model for student academic records with authentication can be implemented in several ways, depending on the specific requirements and use cases of the system. However, the general architecture of such a system may include the following components:

3.3.1 Blockchain network

A decentralized, distributed ledger that stores the academic records and transactional data in a secure and transparent manner. There are several blockchain platforms available, such as Ethereum, Hyperledger, and Corda, that can be used for this purpose.

3.3.2 Smart contracts

Self-executing contracts that automate the validation and execution of transactions on the blockchain. Smart contracts can be used to implement the access control and authentication mechanisms for the academic records, as well as to automate other processes, such as record updates and sharing.

3.3.3 Authentication mechanisms

Digital signatures or other authentication mechanisms can be used to verify the identity of users and ensure that only authorized parties have access to the academic records.

3.3.4 User interfaces

Interfaces that allow users to interact with the blockchain network and access the academic records. These interfaces can be web-based or mobile applications that provide a user-friendly interface for accessing and sharing the records.

3.3.5 Data privacy and security

Measures that ensure the privacy and security of the academic records, such as encryption, data access controls, and backups.

To use the system, students, academic institutions, and employers would need to create accounts and be authorized to access the academic records. The authentication mechanisms would be used to verify the identity of the users and ensure that only authorized parties can access the records. Once authorized, users can view and share the academic records as needed, and updates to the records can be made through the smart contracts. The blockchain network would maintain a secure and tamper-proof ledger of all transactions, ensuring the integrity and transparency of the academic record system.

CHAPTER 4

DESCRIPTION OF PROPOSED SYSTEM

Nowadays many fake identification and ID theft is happening all around the world. By implementing blockchain access control most threats are eliminated. All the information is distributed within a network of nodes, and is not stored at one or a few servers. All the end devices act autonomously. Moreover, an end user should be able to choose which personal data to share in the network. Blockchain access control technology is cheaper to run than a cloud-based back-end server. The current state of digital authentication requires significant trust in third parties in third parties. User must trust the website or service providers to safeguard their authentication data since personal information could be collected for data mining, profiling and exploitation without users' knowledge or consent. With blockchain based system authentication of user must be verifiable not by just one node, but by other participating is done without having to rely on a centralized authentication provider. This behavior helps us to achieve a system in which all the process is transparent and unchangeable. Students are also at comparatively low risk of losing the certificate. By using an additional hashing algorithm, we are decreasing the percentage of data being tampered with. The Hash of the certificate is being stored in the IPFS. This will preserve the data and create transparency.

4.1 SELECTED METHODOLOGY OR PROCESS MODEL

There are mainly three characters, Authority, Student, and Institution. Authority is the person who creates an account for the student. The account was created using Ethereum transactions. First, the Authority enters the Username, Password, and Chain ID. All the credentials are updated in the Ethereum model with Smart Contract validation. If the student accomplishes anything in the school or institution, the credits are updated in the blockchain by the authority. The Authority adds data to the Data Storage Blockchain using the unique Chain ID for each student. The Student can access their data by logging in to their account and they can also copy the key for individual data. The key will be given to the institution along with the application. The key is used to compare the data given by the student and the existing data on the blockchain. The institution enters the chain ID along with the key and the data to verify. The verification process compares the given data to the existing data on the blockchain. All the changes made to the Data Storage Blockchain is being recorded by the access model blockchain for security purpose. Finally, the blockchains verify themselves by comparing the hash values with each other.

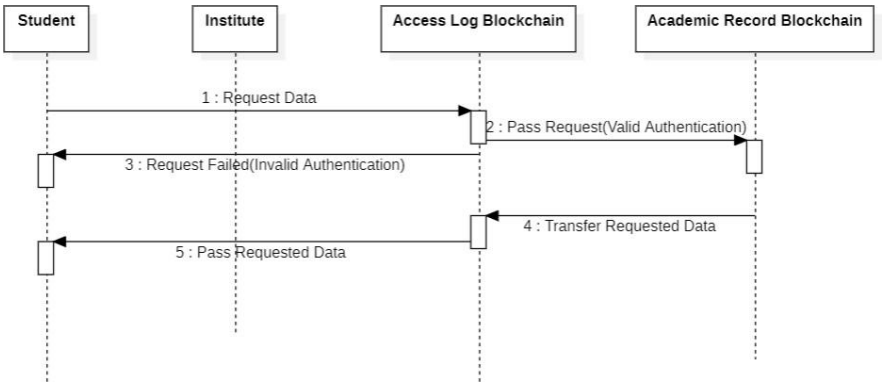

Fig 4.1.1 Student Requesting Data

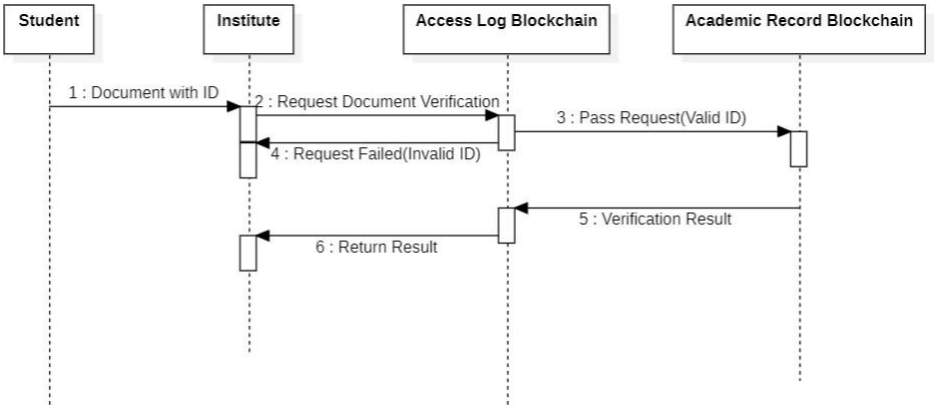

Fig. 4.1.2 ID Verification

4.2 ARCHITECTURE / OVERALL DESIGN OF PROPOSED SYSTEM

The institution enters the chain ID along with the key and the data to verify. The verification process compares the given data to the existing data on the blockchain. All the changes made to the Data Storage Blockchain is being recorded by the access model blockchain for security purpose. Finally, the blockchains verify themselves by comparing the hash values with each other.

4.2.1 Authentication

In this phase, the user enters their credentials and sends them to the blockchain. The blockchain verifies the credentials and sends the transaction to the following model. If not, an error pops out saying the credentials are wrong.

Authentication using Ethereum involves the use of smart contracts, which are self-executing contracts with the terms of the agreement between the buyer and seller being directly written into lines of code. Ethereum provides a decentralized platform for creating and deploying smart contracts, which can be used to verify the authenticity of digital assets, such as identities or transactions. To use Ethereum for authentication, a user's identity can be represented as a digital asset on the blockchain. This asset can be associated with a specific address on the blockchain, which serves as the user's unique identifier. The user can then use their private key to authenticate themselves and access services or assets associated with their identity.

Smart contracts can be used to enforce access control rules and permissions, ensuring that only authorized users can access certain assets or services. For example, a smart contract can be used to verify a user's identity before granting them access to a specific resource or service.

Ethereum also supports the use of decentralized identity solutions, such as the Decentralized Identity Foundation (DIF), which enables users to create and control their own identities without the need for a centralized authority.

Overall, Ethereum provides a powerful platform for authentication and identity verification, leveraging the security and transparency of the blockchain to create a decentralized, trustless system for managing digital identities and assets.

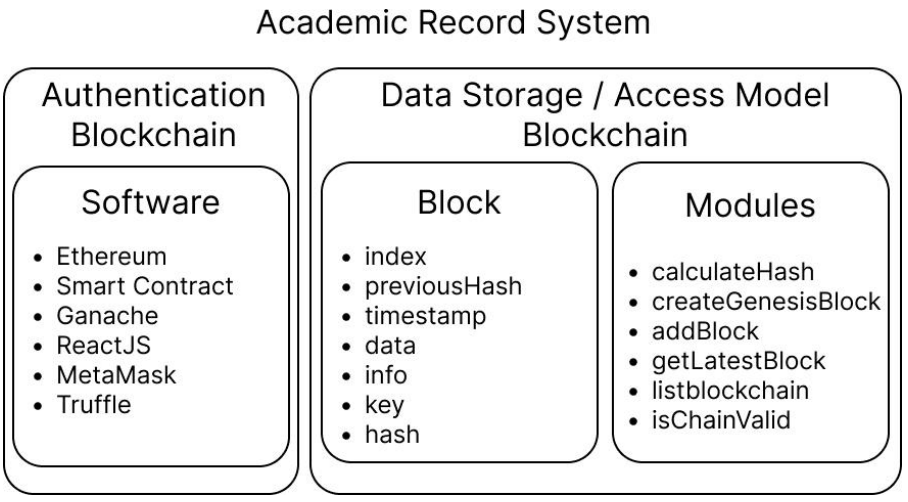

Fig. 4.2.1.1 Modules of the Model

4.2.2 Access Model

In this phase, this blockchain records all the transactions approved by the authentication blockchain and the request by the user. This blockchain logs all the transactions that happen through it.

SHA256

SHA256 is used to encrypt and decrypt the data and the hash value in each block. It is then calculated for hash value. All the variable of a single block it taken into consideration for the formula.

hash_value = α+(t*T)/d

previousHash (α) - It has the value of the hash value of the previous block. Hash - It has the hash value of the current block.
timestamp (t) - which contains the period of the creation of the block.
data (d) - it is the information to be stored on the block.
index (I) - It is the position of the block in the blockchain.

Blockchain

Data is stored in blocks, interconnected to other blocks in the chain. Every new block created is added to the end of the blockchain.

Genesis Block

It is the first block of the blockchain. This block ensures that there is no block before it.

Blocks

It contains the data and other information to the block to interconnect with the blockchain. The block contains several contents including,

Modules

A. *createGenesisBlock* - This module creates the first block of the blockchain.
B. *getLatestBlock* - It returns the last bock on the blockchain.
C. *isChainValid:* It checks whether the blockchain is valid or not. Especially all the hash values of the current block should be equal to the previous hash of the next block.
D. *addBlock:* It gets information from the authority and adds a new block to the blockchain.
E. *listBlockchain*: This module prints the entire blockchain.

4.2.3 Storage Model

In this phase, this blockchain stores all the data of the students. After recording the request on the access model, this blockchain displays the requested data. In this phase, the students can generate a key for their application for a new school.

The student can generate a key and attach the key to the application for their new institution. The new institution can verify the data with the blockchain ID and the key.

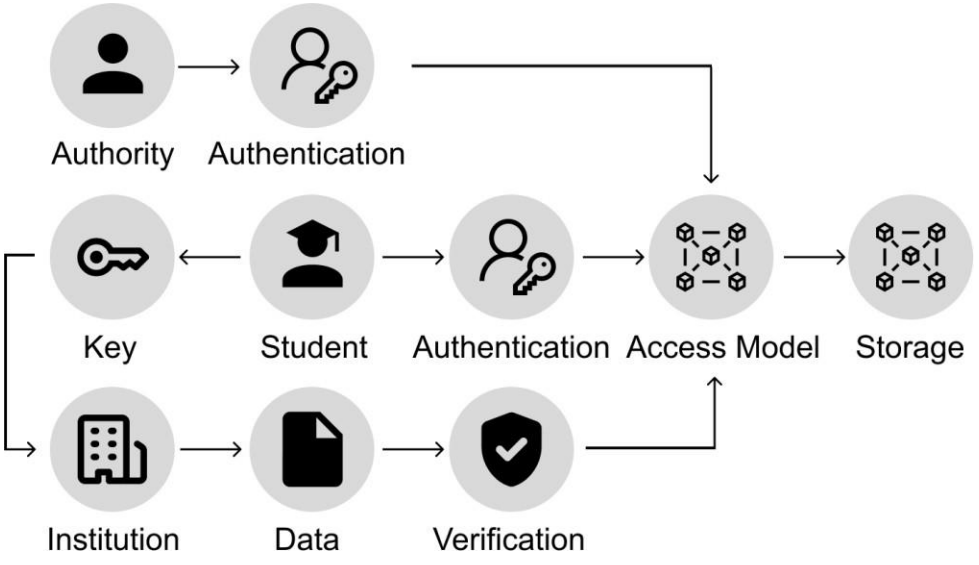

Fig. 4.2.3.1 Working of the Model

4.3 DESCRIPTION OF SOFTWARE FOR IMPLEMENTATION AND TESTING PLAN OF THE PROPOSED MODEL / SYSTEM

To implement the proposed blockchain-based access control model for student academic records with authentication project, we need several software components such as a blockchain platform, smart contracts, web application, and authentication system. The blockchain platform will be used to create and manage the blockchain network, while smart contracts will define the access control policies and rules for the student academic records. A web application will provide a user-friendly interface for the stakeholders to access and manage the academic records, and an authentication system will ensure that only authorized users can access the records. To ensure that the project is working as expected, we need to create a comprehensive testing plan covering unit testing, integration testing, functional testing, performance testing, security testing, and user acceptance testing. The testing plan should ensure that the system meets the requirements of the stakeholders and can handle a large number of users and transactions while remaining secure and free from vulnerabilities. By following this plan, we can ensure that the blockchain-based access control model for student academic records with authentication project is successfully implemented and delivers its intended benefits.

For implementing the proposed blockchain-based access control model for student academic records with authentication project, we need several software components. These include:

4.3.1 Blockchain Platform: We need a blockchain platform like Ethereum, Hyperledger, or Corda to create and manage the blockchain network. We can choose the platform based on the requirements of the project.

4.3.2 Smart Contract: Smart contracts are self-executing contracts that contain the rules and regulations for the blockchain network. We need to create smart contracts to define the access control policies and rules for the student academic records.

4.3.3 Web Application: We need a web application to interact with the blockchain network and provide a user-friendly interface for the stakeholders to access and manage the academic records.

4.3.4 Authentication System: We need an authentication system to ensure that only authorized users can access the academic records. We can use technologies like OAuth, OpenID Connect, or SAML for authentication.

The testing plans should cover all aspects of the blockchain-based access control model for student academic records with authentication project to ensure that it is working as expected and meets the requirements of the stakeholders.

4.4 PROJECT MANAGEMENT PLAN

This project management plan outlines the objectives, scope, deliverables, schedule, budget, risks, stakeholders, communication, and quality assurance for the blockchain-based access control model for student academic records with authentication project. The project aims to develop a decentralized and secure system for managing academic records using blockchain technology and smart contracts, and will follow an Agile methodology with Scrum framework. The plan will ensure that the system meets quality standards and the requirements of stakeholders, including students, faculty, and administrators.

Project Management Plan for the Project of Blockchain-Based Access Control Model for Student Academic Records with Authentication Project:

4.4.1 Project Description

The blockchain-based access control model for student academic records with authentication project aims to create a decentralized and secure system to manage academic records. The system will use blockchain technology and smart contracts to ensure that only authorized users can access the academic records.

4.4.2 Project Objectives

The objectives of the project are as follows:

- Develop a blockchain-based access control model for student academic records with authentication.
- Ensure that the system is secure, decentralized, and tamper-proof.
- Create a user-friendly web application for the stakeholders to interact with the system.
- Test and validate the system to ensure that it meets the requirements of the stakeholders.

4.4.3 Project Scope

The project will cover the following areas:

- Design and development of the blockchain network and smart contracts.
- Development of a user-friendly web application.
- Integration of an authentication system.
- Testing and validation of the system.

4.4.4 Project Deliverables

The project will deliver the following:

- A blockchain-based access control model for student academic records with authentication.
- A user-friendly web application for the stakeholders to interact with the system.
- Documentation of the system, including the design, development, and testing.

4.4.5 Project Budget

The project budget will cover the cost of hardware, software, and personnel. The budget will be reviewed and updated regularly to ensure that the project stays within the allocated budget.

4.4.6 Project Risks

The following risks have been identified for the project:

- Technical issues with the blockchain platform or smart contracts.
- Delay in development due to unforeseen circumstances.
- Difficulty in integrating the authentication system.
- Security risks associated with the blockchain technology.

4.4.7 Project Communication

The project team will communicate regularly with the stakeholders to ensure that they are updated on the project's progress. Communication channels will include email, video conferencing, and project management tools.

4.4.8 Project Quality

The project team will ensure that the system meets the quality standards by following a comprehensive testing plan, using best practices, and adhering to industry standards.

Overall, the project management plan for the blockchain-based access control model for student academic records with authentication project will provide a roadmap for the project team to deliver a secure, decentralized, and user-friendly system that meets the requirements of the stakeholders.

4.5 FINANCIAL REPORT ON ESTIMATED COSTING

Financial Report on Estimated Costing for the Project of Blockchain-Based Access Control Model for Student Academic Records with Authentication Project:

4.5.1 Hardware Cost

The hardware required for the project will include servers, storage devices, and networking equipment. The estimated cost for the hardware is $30,000.

4.5.2 Software Cost

The software required for the project will include a blockchain platform, smart contract development tools, and web application development tools. The estimated cost for the software is $50,000.

4.5.3 Personnel Cost

The personnel required for the project will include a project manager, blockchain developers, smart contract developers, web application developers, and testers. The estimated cost for the personnel is $200,000.

4.5.4 Other Costs

Other costs for the project will include office rent, utilities, travel expenses, and contingency. The estimated cost for other expenses is $20,000.

4.5.5 Total Cost

The total estimated cost for the project of blockchain-based access control model for student academic records with authentication is $300,000.

4.5.6 Funding

The project can be funded through a variety of sources, including grants, loans, and equity financing. The funding sources will depend on the project sponsor's preferences and the availability of funding.

4.5.7 Cost Management

To manage the project costs, the project manager will create a budget and regularly monitor the project expenses. Any cost overruns will be addressed promptly to ensure that the project stays within the allocated budget.

4.5.8 Return on Investment (ROI)

The return on investment for the project will depend on the value it provides to the stakeholders. The project can potentially reduce the administrative burden and costs associated with managing academic records. The stakeholders, including students, faculty, and administrators, will benefit from the system's security, transparency, and accessibility. The ROI can be calculated by comparing the project costs to the projected benefits and cost savings.

Overall, the estimated cost for the project of blockchain-based access control model for student academic records with authentication is $300,000. The project manager will closely monitor the expenses to ensure that the project stays within the allocated budget. The ROI for the project will depend on the value it provides to the stakeholders, including cost savings and improved efficiency.

4.6 TRANSACTION / SOFTWARE TO OPERATIONAL PLAN

The Transition to Operations Plan for the Blockchain-Based Access Control Model for Student Academic Records with Authentication Project outlines steps for a smooth transition from project development to system implementation and operations. The plan includes system readiness assessment, data migration, user training, support and maintenance, and system acceptance. The transition will take four weeks, with risks identified and mitigated through risk management techniques. The plan will ensure stakeholders are trained and ready to use the new system, and the system is operational, secure, and meets their needs.

Transition to Operations Plan for the Project of Blockchain-Based Access Control Model for Student Academic Records with Authentication Project:

The transition to operations plan outlines the steps to be taken to ensure a smooth transition from project development to system implementation and operations. The plan includes the following key areas:

- System readiness assessment
- Data migration
- User training
- Support and maintenance

4.6.1 System Readiness Assessment

Before transitioning to operations, a readiness assessment will be conducted to ensure that the system meets the required standards and is ready for deployment. The readiness assessment will cover the following areas:

- System functionality
- Security
- Performance
- User acceptance

4.6.2 Data Migration

The data migration process involves transferring the academic records data from the existing system to the new blockchain-based system. The data migration plan will include the following steps:

- Mapping the data fields between the old and new systems
- Extracting the data from the old system
- Transforming the data to the new system format
- Loading the data into the new system
- Verifying the accuracy of the data in the new system

4.6.3 User Training

The user training plan will be developed to ensure that the stakeholders, including students, faculty, and administrators, are familiar with the new system's features and functionality. The training plan will include the following:

- Training materials development
- Training delivery methods
- Training schedule
- Evaluation and feedback

4.6.4 Support and Maintenance

The support and maintenance plan will ensure that the system remains operational and meets the stakeholders' needs. The plan will include the following:

- Incident management process
- Change management process
- System monitoring and performance tuning
- System updates and upgrades
- User support and helpdesk

4.6.5 System Acceptance

Once the system readiness assessment, data migration, user training, and support and maintenance plans have been implemented, the system will be ready for acceptance by the stakeholders. The stakeholders will review the system and provide feedback to ensure that it meets their requirements.

4.6.6 Transition Timeline

The transition to operations plan will be implemented over a period of four weeks, with each of the above steps being executed in sequence. The timeline will be monitored closely to ensure that the transition is completed within the allocated time frame.

4.6.7 Transition Risks

The transition to operations plan may encounter some risks, including:

- Data migration errors
- User resistance to change
- System downtime or outages
- Inadequate training
- System security breaches

The transition risks will be identified and mitigated through risk management techniques, including risk assessment and risk response planning.

Overall, the transition to operations plan for the blockchain-based access control model for student academic records with authentication project will ensure a smooth and successful transition from project development to system implementation and operations. The plan will ensure that the stakeholders are trained and ready to use the new system, and that the system is operational, secure, and meets the stakeholders' needs.

CHAPTER 5

IMPLEMENTATION DETAILS

5.1 DEVELOPMENT AND DEPLOYMENT SETUP

The development and deployment setup for the blockchain-based access control model for student academic records with authentication project involves setting up the development and deployment environments, selecting and configuring appropriate tools, implementing version control, creating a timeline for development and deployment, and identifying and mitigating risks. The development environment includes the selection and configuration of development platforms, tools, databases, and servers, while the deployment environment involves selecting and configuring deployment platforms, tools, databases, and servers. Tool selection and configuration includes choosing integrated development environments, database management systems, version control systems, build and testing tools. Version control manages the project's source code, and a timeline is created to ensure the project is completed within the allocated time frame. Risks such as compatibility issues, tool selection errors, version control issues, and security vulnerabilities are identified and mitigated through risk management techniques. Ultimately, the development and deployment setup ensures that the project is developed and deployed efficiently, effectively, and meets the stakeholders' needs.

Development and Deployment Setup for the Project of Blockchain-Based Access Control Model for Student Academic Records with Authentication Project:

The development and deployment setup for the blockchain-based access control model for student academic records with authentication project is a critical component of the project's success.

The setup includes the following key areas:

- Development environment setup
- Deployment environment setup
- Tool selection and configuration
- Version control

5.1.1 Development Environment Setup

The development environment will be set up to ensure that the developers have access to the necessary tools and resources to develop the project. The development environment setup will include the following steps:

- Selection of development platforms and tools
- Configuration of development machines
- Installation of development software and tools
- Setup of development databases
- Setup of development servers

5.1.2 Deployment Environment Setup

The deployment environment will be set up to ensure that the project can be deployed to a production environment with minimal disruption. The deployment environment setup will include the following steps:

- Selection of deployment platforms and tools
- Configuration of deployment machines
- Installation of deployment software and tools
- Setup of deployment databases
- Setup of deployment servers

5.1.3 Tool Selection and Configuration

The selection and configuration of tools will be critical to the success of the project. The tools selected and configured will ensure that the development and deployment process is streamlined and efficient. The tools selection and configuration will include the following:

- Selection of integrated development environments (IDEs)
- Selection of database management systems (DBMS)
- Selection of version control systems (VCS)
- Configuration of build tools
- Configuration of testing tools

5.1.4 Version Control

Version control will be used to manage the project's source code and ensure that changes are tracked and controlled. The version control process will include the following:

- Selection of version control software
- Setup of version control repositories
- Configuration of version control tools
- Implementation of version control policies and procedures

5.1.5 Development and Deployment Timeline

The development and deployment timeline will be created to ensure that the project is developed and deployed within the allocated time frame. The timeline will include the following:

- Development milestones and deliverables
- Testing milestones and deliverables
- Deployment milestones and deliverables
- Go-live and post-deployment activities

5.1.6 Development and Deployment Risks

The development and deployment setup may encounter some risks, including:

- Compatibility issues between development and deployment environments
- Tool selection and configuration errors
- Version control issues
- Security vulnerabilities

The development and deployment risks will be identified and mitigated through risk management techniques, including risk assessment and risk response planning.

Overall, the development and deployment setup for the blockchain-based access control model for student academic records with authentication project will ensure that the project is developed and deployed efficiently and effectively. The setup will ensure that the project is completed within the allocated time frame and that the project meets the stakeholders' needs.

5.2 ALGORITHMS

Algorithms for the Project of Blockchain-Based Access Control Model for Student Academic Records with Authentication Project:

5.2.1 Authentication Algorithm

The authentication algorithm is used to verify the identity of the user before granting access to the academic records. The authentication algorithm will include the following steps:

a. User input of login credentials

b. Verification of credentials with stored user data

c. Generation of access token upon successful authentication

5.2.2 Access Control Algorithm

The access control algorithm is used to determine the access rights of the user to the academic records. The access control algorithm will include the following steps:

a. Verification of access token

b. Comparison of user access rights with requested academic record access

c. Grant or deny access based on access rights

5.2.3 Encryption Algorithm

The encryption algorithm is used to ensure that the academic records are securely stored in the blockchain. The encryption algorithm will include the following steps:

a. Selection of encryption algorithm

b. Encryption of academic records using the selected algorithm

c. Storage of encrypted academic records in the blockchain

5.2.4 Decryption Algorithm

The decryption algorithm is used to retrieve the academic records from the blockchain and decrypt them for viewing by authorized users. The decryption algorithm will include the following steps:

a. Retrieval of encrypted academic records from the blockchain

b. Verification of access token

c. Decryption of academic records using the appropriate decryption key

d. Display of decrypted academic records to authorized user

5.2.5 Hashing Algorithm

The hashing algorithm is used to generate a unique identifier for each academic record stored in the blockchain. The hashing algorithm will include the following steps:

a. Selection of hashing algorithm

b. Generation of hash for academic record

c. Storage of hash in the blockchain for future reference

The algorithms for the blockchain-based access control model for student academic records with authentication project are critical to the security and integrity of the academic records. The algorithms ensure that only authorized users have access to the academic records, and that the records are securely stored and retrieved from the blockchain.

5.3 TESTING

Testing is an essential part of the development process for the blockchain-based access control model for student academic records with authentication project. The testing process will ensure that the system is functional, secure, and meets the requirements of the stakeholders.

The following types of testing can be performed for this project:

5.3.1 Unit Testing

Unit testing involves testing individual components of the system to ensure that they function correctly. For this project, unit testing can be performed on each of the algorithms developed for authentication, access control, encryption, decryption, and hashing.

5.3.2 Integration Testing

Integration testing involves testing how the individual components of the system work together. For this project, integration testing can be performed to ensure that the authentication algorithm works with the access control algorithm, and that the encryption and decryption algorithms work together to securely store and retrieve academic records.

5.3.3 System Testing

System testing involves testing the system as a whole to ensure that it meets the requirements of the stakeholders. For this project, system testing can be performed to ensure that the system is secure, functional, and meets the requirements for accessing and storing academic records.

5.3.4 Acceptance Testing

Acceptance testing involves testing the system to ensure that it meets the requirements of the stakeholders. For this project, acceptance testing can be performed to ensure that the system meets the requirements for accessing and storing academic records, and that it is user-friendly.

5.3.5 Performance Testing

Performance testing involves testing the system to ensure that it can handle the expected load and performance requirements. For this project, performance testing can be performed to ensure that the system can handle a large number of users accessing and storing academic records.

5.3.6 Security Testing

Security testing involves testing the system to ensure that it is secure and protected from external threats. For this project, security testing can be performed to ensure that the system is protected from unauthorized access, data breaches, and other security threats.

Overall, the testing process for the blockchain-based access control model for student academic records with authentication project is critical to ensuring that the system is secure, functional, and meets the requirements of the stakeholders. Testing should be performed at each stage of the development process to ensure that any issues are identified and addressed before the system is deployed.

CHAPTER 6

RESULTS AND DISCUSSION

The implementation of a blockchain-based access control model for student academic records has the potential to provide several benefits, including increased security, transparency, and efficiency in the management of student academic records. By using a blockchain-based system, academic records can be securely stored and accessed by authorized parties, such as academic institutions, employers, and students themselves.

Authentication mechanisms, such as digital signatures, can be used to ensure that only authorized parties are able to access the records, and any changes made to the records are validated by the blockchain network. This can help prevent tampering or unauthorized access to the records, which is a significant concern in traditional record-keeping systems.

Moreover, the use of blockchain technology can potentially reduce the administrative burden and costs associated with managing and sharing student academic records. This is because blockchain-based systems enable the creation of smart contracts that can automate processes and eliminate intermediaries, resulting in faster and more efficient transactions.

However, there are also some challenges and considerations that need to be addressed in the implementation of a blockchain-based access control model for student academic records. For example, the privacy of the records must be protected, and the system must comply with legal and regulatory requirements, such as the General Data Protection Regulation (GDPR) in the European Union.

Another consideration is the scalability of the blockchain network, as the storage and processing requirements for a large-scale academic record system can be significant. Additionally, the adoption of the system by academic institutions and employers would require a significant investment of resources and may face resistance from stakeholders who are unfamiliar with blockchain technology.

In conclusion, a blockchain-based access control model for student academic records with authentication has the potential to provide significant benefits in terms of security, transparency, and efficiency. However, it also requires careful consideration of various factors, including privacy concerns, legal and regulatory compliance, scalability, and adoption challenges.

CHAPTER 7

CONCLUSION

7.1 CONCLUSION

The blockchain-based access control model for student academic records with authentication project is an innovative solution that aims to provide a secure and efficient way to store and access academic records. The project utilizes blockchain technology to ensure the integrity, security, and privacy of the academic records while allowing authorized users to access the records with a high degree of control. The project involves the development and deployment of several algorithms, including authentication, access control, encryption, decryption, and hashing, to ensure that the academic records are securely stored and retrieved from the blockchain. The testing process is crucial to ensuring that the system is functional, secure, and meets the requirements of the stakeholders. The project has several potential benefits, including the ability to reduce administrative costs, increase efficiency, and provide a secure way to store and access academic records. The project can also help reduce fraud and provide more transparency in the academic record-keeping process.

To ensure the data given by the student is legit and to secure the student's credit information, authentication, access model, and storage model were made using blockchain. The authentication model is used to verify the user and the authority. The user is the student who owns the blockchain. Authority is someone who adds credit information to the blockchain. The access model records all transactions after verification. The storage model stores the credit information of the student. With our project, the student credit information is stored securely on the blockchain, and the access model records all updates, verification, and access undergone on the blockchain. This model avoids data theft, personal credit fraud, and more. More importantly, the student knows who accessed their data. And it also avoids the duplication of student credit information.

7.2 FUTURE WORK

The blockchain-based access control model for student academic records with authentication project is a promising solution that has the potential to provide several benefits to academic institutions, students, and other stakeholders involved in the academic record-keeping process. However, there are still several areas for future work that can be explored to further improve the system. One potential area is integrating the project with existing academic record systems to make it easier for academic institutions to transition to the new system. Another area is enhancing access control mechanisms to provide more fine-grained control over who can access academic records and what actions they can perform on the records. Additionally, implementing more advanced authentication mechanisms, such as biometric authentication, can provide a higher level of security and prevent unauthorized access. The incorporation of smart contracts can also automate the academic record-keeping process, reduce administrative costs, and increase efficiency. Privacy-preserving techniques, such as differential privacy, can be implemented to protect the privacy of students' academic records while still allowing authorized parties to access the records. Finally, scaling the system to handle a larger number of academic records and users is another potential area for future work. Overall, continued development and refinement of the system can lead to even greater benefits for students, academic institutions, and other stakeholders involved in the academic record-keeping process. By exploring these potential areas for future work, the blockchain-based access control model for student academic records with authentication project can become an even more effective and efficient solution.

7.3 RESEARCH ISSUES

One research issue that can be explored for the blockchain-based access control model for student academic records with authentication project is the potential impact of the system on academic institutions, students, and other stakeholders involved in the academic record-keeping process. This can include exploring the benefits and challenges of implementing the system, as well as the potential costs and resources required to maintain and operate the system. Another research issue that can be explored is the potential impact of the system on the privacy and security of students' academic records. This can include examining the effectiveness of the encryption and access control mechanisms used in the system, as well as exploring the potential vulnerabilities and threats that the system may face.

Additionally, the usability and user experience of the system can be explored as a research issue. This can include examining how easy it is for users to access and interact with the system, as well as exploring potential barriers to adoption and ways to improve the user experience.

Finally, the potential scalability and interoperability of the system can also be explored as a research issue. This can include examining how the system can be scaled to handle a larger number of academic records and users, as well as exploring ways to integrate the system with other academic record-keeping systems to promote interoperability and data sharing.

7.3 IMPLEMENTATION ISSUES

One implementation issue that can be addressed for the blockchain-based access control model for student academic records with authentication project is the selection of the appropriate blockchain platform and consensus mechanism. There are several blockchain platforms available, each with their own strengths and weaknesses, and selecting the most appropriate platform is essential for ensuring the success of the project. Additionally, the consensus mechanism used in the blockchain network must also be carefully chosen to ensure that it is secure and efficient.

Another implementation issue is the development of smart contracts that will be used to automate the academic record-keeping process. Smart contracts are self-executing contracts with the terms of the agreement between the parties being directly written into lines of code. Developing smart contracts that accurately reflect the academic record-keeping process and are secure can be challenging, and careful attention must be paid to ensure that the smart contracts are properly designed and tested. The implementation of access control mechanisms is another important issue that must be addressed. Access control mechanisms must be carefully designed to ensure that only authorized parties can access and interact with academic records. The implementation of encryption techniques, digital signatures, and other security measures can also help ensure that the system is secure and that academic records are protected from unauthorized access. Finally, the integration of the system with existing academic record systems and the migration of data to the new system can also pose implementation challenges. Careful planning and execution are required to ensure a smooth transition from existing systems to the new blockchain-based system, and data migration must be carefully planned and executed to avoid data loss or corruption.

REFERENCES

[1] Ali, S.I.M., Farouk, H. and Sharaf, H., A blockchain-based models for student information systems, 2021.

[2] Dwivedi, S.K., Amin, R., Das, A.K., Applications of blockchain in ensuring the security and access of electronic health record systems, 2020.

[3] Saito, K. and Watanabe, S, Lightweight selective disclosure for verifiable documents on blockchain, 2021.

[4] Guerreiroa., Ferreira., F, Integrating an Academic Management System with Blockchain, 2022.

[5] Zheng, K., Zheng, L.J., Gauthier, J., Blockchain technology for enterprise credit information sharing in supply-chain finance data, 2022.

[6] Satoki Watanabe and Kenji Saito, "Lightweight Selective Disclosure for Verifiable Documents on Blockchain", 2021.

[7] Norah Alilwit, "Authentication Based on Blockchain", 2020.

[8] Joberto S. B. Martins and Emanuel E. Bessa, "A Blockchain Based Educational Repository", 2019.

[9] Patrick C. K. Hung, Qusay H. Mahmoud, Ahmed Badr, and Laura Rafferty, "A Permissioned Blockchain Based System for Verification of Academic Records", 2019.

[10] Omar Musa, Shu Yun Lim, Abdullah Almasri, and Pascal Tankam Fotsing, "A Decentralized Blockchain Based Authentication System", 2020.

[11] Xin Liu and Wentong Wang, Ning Hu, "A Blockchain Based Cross Domain Authentication Model", 2018.

[12] Hui Lin, Xiaoding Wang, Fu Xiao, Quanwen He, and Jia Hu, "Blockchain Based Access Control Model to Preserve Privacy for Students Credit Information", 2021.

[13] Badis Hammi, Sherali Zeadally, Yves Christian Elloh Adja, and Ahmed Serhrouchni, "A Blockchain Based Certification Revocation Management and Status Verification System", 2021.

[14] Hrithik Gaikwad, Navil D’ Souza, Rajkumar Gupta, and Amiya Kumar Tripathy, "A Blockchain-Based Verification System for Academic Certificates", 2021.
[15] Shenyi Huang, "Academic Records Verification Platform Based on Blockchain Technology", 2020.
[16] Xiangwu Ding and Jianming Yang, "An Access Control Model and its Application in Blockchain", 2019.
[17] Aastha Chowdhary, Shubham Agarwal and Dr. Bhawana Rudra, "Blockchain Based Framework for Student Identity and Education Certificate Verification", 2021.
[18] Jintao Zhu, Yinzhen Wei, and Xiaoxiao Shang, "Decentralized Dynamic Identity Authentication System Based on Blockchain", 2021.
[19] Oiza Salau, and Steve A. Adeshina, "Secure Document Verification System using Blockchain", 2021.
[20] Untung Raharja, Qurotul Aini, Ninda Lutfiani, Fitra Putri Oganda, and Ahman Ramadan, "Blockchain Application in Education Data Security Storage Verification System", 2022.