Online Blockchain Based Certificate Generation and Validation System

Dr Nagesh R[1], Mr. Rahul S[2], Mr. Chethan A[3], Ms. Yuktha Reddy P M[4], Mr. PrajwalV M[5]

Associate Professor, Department of Information Science and Engineering[1]

U.G. Students, Department of Information Science and Engineering[2,3,4,5]

S J C Institute of Technology, Chikballapur, India

Abstract: *At present a considerable amount of training courses are being held accompanied by the issuance of certificates. Unfortunately there is no proper means of verifying these digital certificates. To overcome this issue a new system must be implemented wherein customized digital certificates can be produced. In this system users can securely store their certificates in a digital locker while other organizations can validate them. This can be achieved through the use of open-source software and blockchain technology. The prevalence of counterfeit certificates in our society has become a significant and troublesome issue. It has now become a lucrative business driven by the demand for employment opportunities. As a result legitimate graduates with authentic credentials are often overlooked for job opportunities. To combat this problem various researchers have proposed a certificate authentication system that ensures tamper-proof and reliable management of digital certificates. Ultimately this will benefit both the issuers and recipients of these certificates.*

Keywords: Agriculture, weed detection, crop disease detection

I. INTRODUCTION

A cutting-edge system for generating and validating certificates based on the revolutionary technology of blockchain has transformed the traditional methods of certificate issuance dissemination and validation. By leveraging the potency of blockchain this innovative system guarantees the unalterable and safekeeping of digital certificates. Educational institutions and organizations can conveniently generate various types of certificates whether educational accomplishments professional accreditations or course completions and each certification is securely recorded on the blockchain ledger. Recipients and outside parties can effortlessly verify the credibility and incorruptibility of these certificates eliminating the need for dependency on centralized agencies. This heightened transparency reliability and efficiency in the certification process reduces tedious administrative tasks and ensures a prompt verification process. In summary an online certificate system utilizing blockchain technology surpasses the vulnerabilities and ineffectiveness of conventional methods in handling such a monumental undertaking.

II. LITERATURE REVIEW

S.NO	TITLE	METHODOLOGY USED
1	A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification Author: Avni Rustemi; Fisnik Dalipi; Vladimir Atanasovski; Aleksandar Risteski Year: 2023	blockchain-based systems

2	Iotverif: Automatic Verification of SSL/TLS Certificate for IoT Applications Author: Anyi Liu; Ali Alqazzaz; Hua Ming; Balakrishnan Dharmalingam Year: 2019	TLS/SSL Data t protocol.		
3	Issuing and Verifying Digital Certificates with Blockchain Author: Trong Thua Huynh; Trung Tru Huynh; Dang Khoa Pham; Anh Khoa Ngo Year: 2018	we propose and implement an issuing and verifying model called UniCert based on UniCoin which is a digital currency built on the blockchain technology.	•It address many other issues such as anti-counterfeiting, copyright protection of music products, patents, etc.	•It consumes more time to verify. •It is not suitable for government certificate verification.
4	Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain Author: Richard Nuetey Nortey; Li Yue; Promise Ricardo Agdedanu; Michael Adjeisah Year: 2019	blockchain technology for privacy preservation	The aim of this paper is to ensure the total privacy, integrity and access control of distributed electronic health records to the data owners during its distribution on the blockchain.	•It is providing security for EHR. •There is no access control list.
5	Towards a blockchain-based certificate authentication system in Vietnam Author: Binh Minh Nguyen, Thanh-Chung Dao, Ba-Lam Do Year: 2020	This s some based develo princip build VECe		
6	EVchain: An Anonymous Blockchain-Based System for Charging-Connected Electric Vehicles Author: Shiyuan Xu; Xue Chen; Yunhua He Year: 2021	smart		

Problem Identification

In modern society the fabrication of certificates has become a lucrative industry fueled by the demand for employment. Despite possessing authentic qualifications graduates often face rejection from employers who favor individuals with falsified credentials. While the current systems attempt to address issues such as storing student records through a central database they remain vulnerable to cyber attacks and tampering due to their reliance on centralized servers. This leaves room for exploitation and deceit undermining the integrity of the education system.

Problem Definition

Published credentials are specifically crafted to maintain their validity during authentication process. Nevertheless there have been numerous instances of fraudulent certificates in most institutions and establishments over the years. Additionally distinguishing between falsified and legitimate credentials requires a great deal of focus and results in significant time wastage. This highlights the urgent need for swift and simpler methods of verifying certificates in order to decrease the occurrence of certificate forgery.As a response to this issue various verification systems were developed to combat this problem. However these systems primarily rely on Relational Database Management System (RDMS) which can now be easily breached due to technological advancements. Furthermore the security measures mainly

revolve around a single mode utilizing only login IDs and passwords. As a result these application systems are vulnerable tosecurity breaches
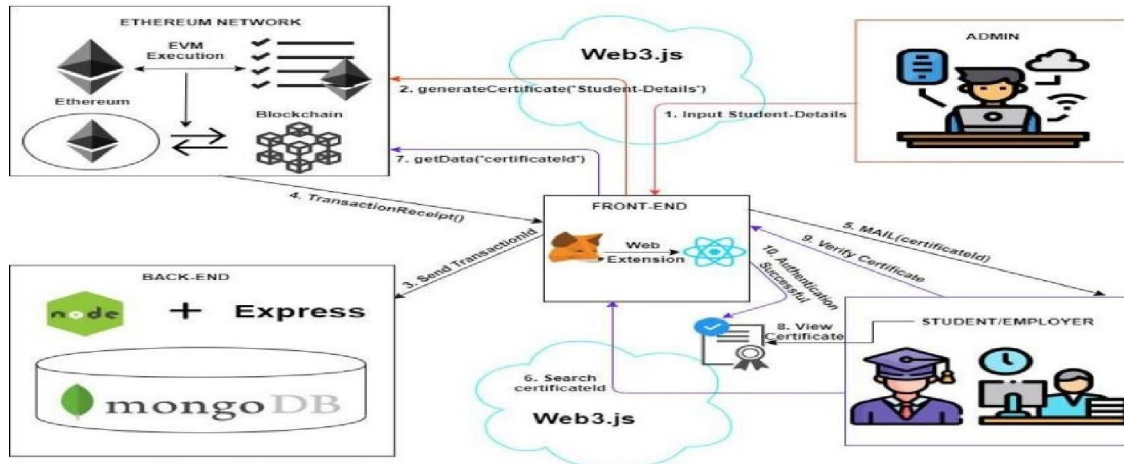
III. METHODOLOGY

SYSTEM ARCHITECTURE

Fig1.SystemArchitecture

SYSTEM ARCHITECTURE

A model may be a complete, basic, and simplified description of software system design that consists of multiple views from a selected perspective or viewpoint as shown in figure1.

A read maybe an illustration of a complete system from the attitude of a connected set of issues.it's accustomed to describe the system from the point of view of various stakeholders like end-users, developers, project managers, and testers
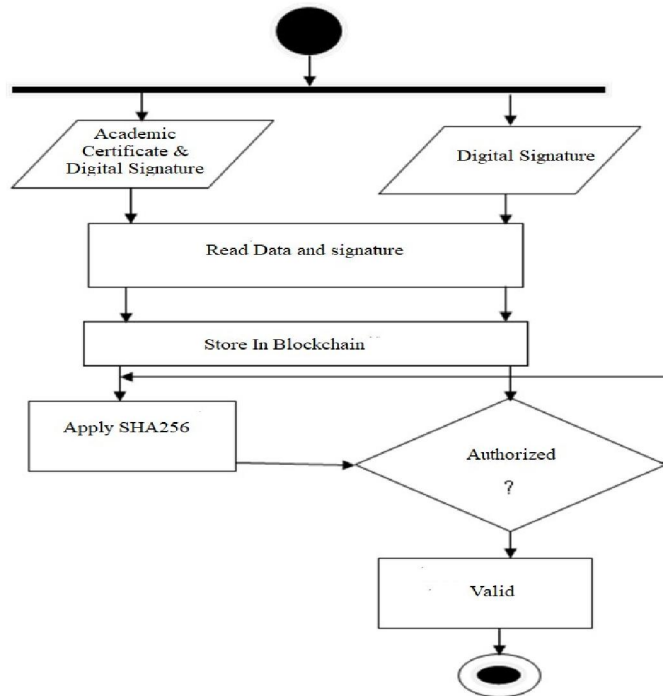
SYSTEM DESIGN- Data Flow Diagram
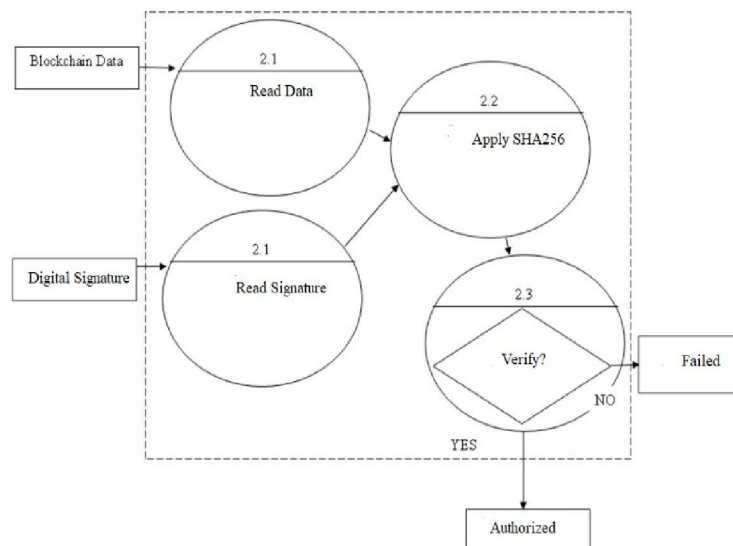
SYSTEM DESIGN- Sequence Diagram
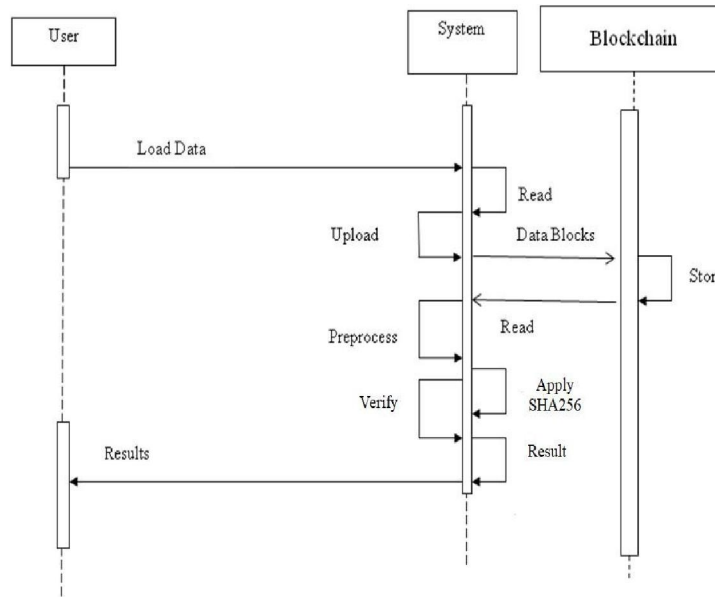
SYSTEM DESIGN- Activity Diagram

System Requirements

Hardware Requirements:

- **Processor:** intel i3 processor and above.
- **Processor Speed:** 2.44gHz or above.
- **RAM:** 8 GB or above.

- **Storage Space:** 50 GB or above.
- **Internet Connectivity:** 20kbs or above required

Functional Requirements:
- This section describes the functional requirements of the system for those requirements which are expressed in the natural language style.
- Create a web application which contains Admin and user.
- Admin should upload the certificate to Etherium.
- System will encrypt and store in Etherium.
- Blockchain will generate the hash key to the user and provide access control
- User can verify the uploaded certificate is original or fake using QR code
- System will securely provide efficient access control and certificate verification.

Non-Functional Requirements:
These are requirements that are not functional in nature, that is, these are constraints within which the system must work.
- The program must be self-contained so that it can easily be moved from one Computer to another. It is assumed that network connection will be available on the computer on which the program resides.

Capacity, scalability and availability.
- The system shall achieve 100 per cent availability at all times.
- The system shall be scalable to support additional clients and volunteers.

Maintainability.
- The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction.

Randomness, verifiability and load balancing.
- The system should be optimized for supportability, or ease of maintenance as far as possible. This may be achieved through the use documentation of coding standards, naming conventions, class libraries and abstraction. It should have randomness to check the nodes and should be load balanced.
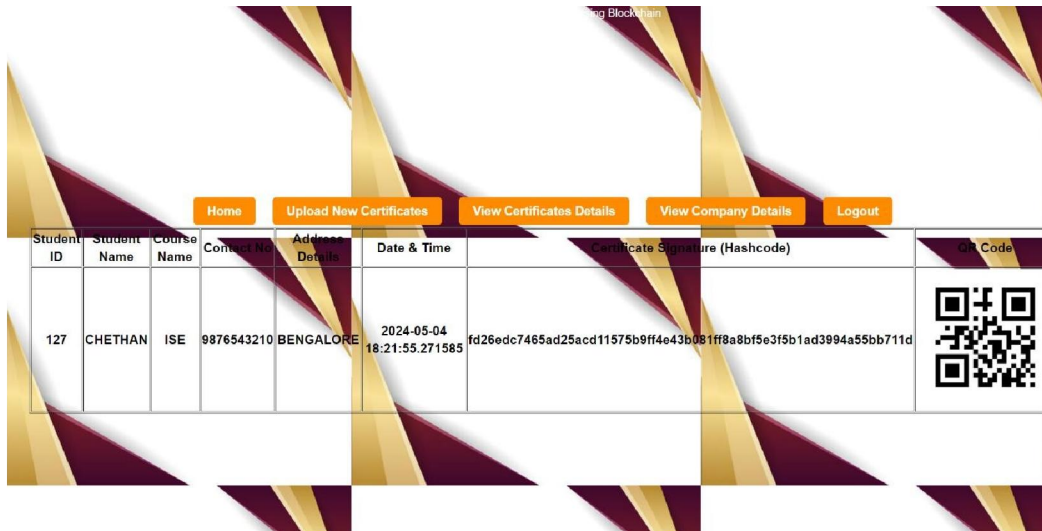
IV. RESULT

The System is designed in such a way that it removes the effect of fake certificates by introducing Digital Academic Certificates and providing a Highly secure Blockchain-Based storage architecture to store these certificates since data in a blockchain is immutable, the Authenticity of the Academic certificates is maintained and Web interface is developed to provide quick access to the Certificates and Authentication of the same.
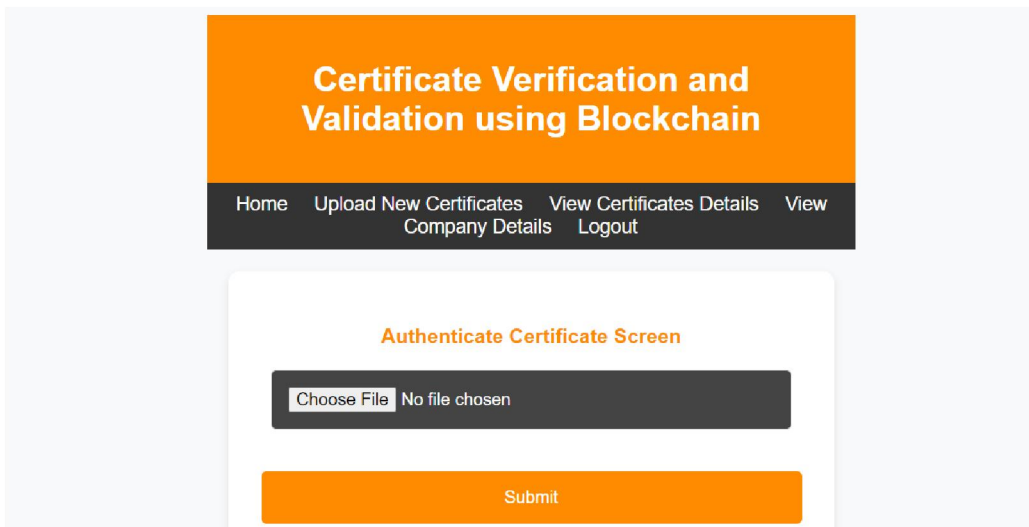
Digital signature:

Certificate details:

Certificate authentication:

Outcome:
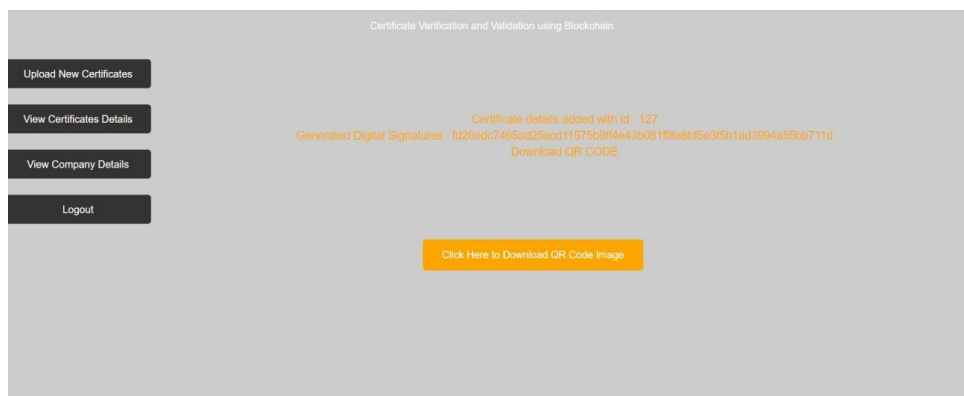
Student ID	Student Name	Course Name	Contact No	Address Details	Date & Time	Certificate Signature (Hash Code)	Status
127	CHETHAN	ISE	9876543210	BENGALORE	2024-05-04 16:09:44.560978	fd26edc7465ad25acd11575b9ff4e43b081ff8a8bf5e3f5b1ad3994a55bb711d	Authentication Successfull

V. CONCLUSION

To conclude the emergence of web-based certificate generation and authentication systems utilizing blockchain technology represents a significant breakthrough in the field of digital credentialing. These platforms utilize the power of blockchain to provide a reliable clear and effective solution for creating distributing and verifying digital certificates. The unchangeable nature of blockchain guarantees that certificates remain untampered with and genuine establishing faith in the certification process. In addition the decentralized design of blockchain lessens dependence on central authorities simplifying the verification procedure and lessening administrative burden. With these advanced systems in place educational institutions corporations and individuals can confidently manage their electronic credentials heralding a new era of credibility and effectiveness in credentialing.

REFERENCES

[1]. Avni Rustemi; Fisnik Dalipi; Vladimir Atanasovski; Aleksandar Risteski," A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification ", Published in: IEEE Access2023 (Volume: 11) [2]. Anyi Liu; Ali Alqazzaz; Hua Ming; Balakrishnan Dharmalingam, "Iotverif: Automatic Verification of SSL/TLS Certificate for IoT Application", on 2020 Published in: IEEE Access2019 (Volume: 8) Topic: Distributed Computing Infrastructure for Cyber-Physical System.

[3]. Trong Thua Huynh; Trung Tru Huynh; Dang Khoa Pham; Anh Khoa Ngo, " Issuing and Verifying Digital Certificates with Blockchain ," Published in: IEEE Access2019(Volume: 9).

[4]. Richard Nuetey Nortey; Li Yue; Promise Ricardo Agdedanu; Michael Adjeisah, " Privacy Module for Distributed Electronic Health Records(EHRs) Using the Blockchain," 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA).

[5]. Nguyen BM, Dao T, Do B. 2020. Towards a blockchain-based certificate authentication system in Vietnam. PeerJ Computer Science 6:e266 https://doi.org/10.7717/peerj-cs.266

[6]. Shiyuan Xu; Xue Chen; Yunhua He : "EVchain: An Anonymous Blockchain-Based System for Charging-Connected Electric Vehicles" Published in: Tsinghua Science and Technology (Volume: 26, Issue: 6, December 2021)

[7]. Muhammad Umar Javed; Abid Jamal; Eman H. Alkhammash; Myriam Hadjouni : Secure Message Handling in Vehicular Energy Networks Using Blockchain and Artificially Intelligent IPFS", Published in: IEEE Access (Volume: 10)2022 Modern agriculture stands on the threshold of a techno- logical revolution propelled by innovative solutions poisedto

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-18069

ISSN
2581-9429
IJARSCT

415