



IJIRCCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH


IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

 9940 572 462

 6381 907 438

 ijircce@gmail.com

 www.ijircce.com

Document Verification and Validation using blockchain

Prof. Bhagyashree Kadam, Ayushi Kulkarni, Shruti Bhavsar, Sumit Katkar, Purvak Tayade

Department of Information Technology, JSPM'S BSIOTR, Wagholi, Pune, Maharashtra, India

ABSTRACT: "In the latest statistics from India's Ministry of Education, approximately a million students graduate annually. While some pursue further studies abroad or in higher educational institutions within the country, others transition into the workforce. Throughout their academic journey, students amass numerous documents such as grades, awards, and certificates. These become vital references when applying to further academic institutions or jobs. As institutions grant these documents, typically only the names of the institutions and students are documented. The current system lacks a robust mechanism to prevent forgery, leading to instances where these credentials are counterfeited. This paper proposes a digital documentation system based on blockchain technology to address this issue. Leveraging the inherent security and immutability features of blockchain, this system aims to create digital documents that are both tamperproof and verifiable. The process involves converting a physical document, along with associated data, into its digital format and computing its hash value. This value is then stored in a blockchain. A combined QR code and unique identifier are attached to the physical document, allowing verification through mobile scans or online checks. By employing the robust features of blockchain, this system not only bolsters the integrity of traditional paper-based documents but also mitigates the risk associated with their potential loss."

KEY WORDS: Forgery, BlockCertAuth, Hash value, QRcode, Certificates.

I. INTRODUCTION

There's a growing demand for systems that enable manual document creation as part of the document verification process, particularly using data from current students. Although the verification methodologies share similarities across various centralized systems, they remain vulnerable. Network threats, ranging from SQL injections to brute force attacks, highlight the inadequacies of centralized defenses. Enter the decentralized solution: blockchain. This approach promises enhanced security, especially when considering the evolving nature of network topologies due to innovations like fog computing and fog networking, or "fogging". Unlike the conventional paradigms where network switches and LTE integrated gateways dominate, fog networking shifts control, configuration, and operations closer to the edge of the internet infrastructure. The fog computing framework can be visualized as an extensively virtualized platform. It offers multi-tiered computational resources, backed by edge nodes (referred to as "fog nodes" in some contexts). These nodes serve a dual purpose: they not only coordinate a myriad of services but also optimize content storage, bringing it nearer to the end-users. The centerpiece of this research is the introduction of a system adept at crafting dynamic, secure electronic documents. This is achieved through the integration of smart contracts within a blockchain environment. Moreover, our study proudly unveils a custom-built blockchain in an open-source environment, complete with a distinctive mining protocol and a smart contract. Our evaluation culminates in employing a consensus algorithm to gauge the efficacy and performance of the system.

II. LITERATURE SURVEY

In a 2020 study published by IEEE, challenges surrounding the maintenance and validation of physical degree certificates such as SSLC, HSC, and other academic accolades were investigated. Students often grapple with the safekeeping of these vital documents, while educational institutions and potential employers find the process of validating their authenticity cumbersome. Addressing these concerns, the study proposes a novel solution to digitalize and safeguard these certificates leveraging blockchain technology. This innovative system transforms paper certificates into their digital equivalents, subsequently generating a unique hash code value using a chaotic algorithm. Ensuring the security and integrity of these digital certificates, they are stored within a blockchain system. The robust design of this system allows for seamless conversion of physical certificates to a digital medium, efficient hash code creation through a chaotic algorithm, and uncompromised storage within the blockchain. A salient feature highlighted is the capability to validate these certificates through a mobile application, enhancing ease of access and validation. With this blockchain-driven system, the researchers anticipate a marked improvement in the security and efficiency of the certificate validation process [1].

A 2022 publication in IJRASET delved into the pervasive issue of duplication and forgery in educational certificates and organizational documents. The existing verification paradigms, besides being time-intensive, often resort to external services, which unfortunately do not always assure transparency or security. Addressing this lacuna, the study introduces the "Secure Doc Verifier," a model underpinned by blockchain technology aimed at verifying educational and organizational documents. A hallmark of this system is its staunch commitment to security and transparency throughout the verification trajectory. Moving away from the conventional centralized storage doctrines, this model champions the use of the Inter Planetary File System (IPFS), a decentralized storage protocol. Such a decentralized ethos not only bolsters data security but also ensures that users retain control over their information, as opposed to centralized counterparts which often assume control of user data. However, while the system is commendably geared towards security and decentralization, the integration of IPFS does pose some potential hitches. Being an evolving decentralized storage framework, IPFS might encounter hurdles related to data retrieval speed and the overarching efficiency of the system. Thus, ensuring a harmonious blend of IPFS with the blockchain, such that it doesn't impede the model's performance, remains imperative [2].

In a 2023 study published by IEEE titled "Certificate validation using blockchain: A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," the authors delve into pressing challenges within the educational domain. At the heart of these challenges is the pressing need for innovation, underlining the vast potential of blockchain technology not only as a tool for cost-effective learning paradigms but also as an instrument to recalibrate the dynamics between educators and learners. The potentialities of blockchain are vast, with the study positing its application as a solution to numerous existing quandaries, particularly the issuance of immutable digital certificates. Such an application stands to transform the current certificate verification landscape, heralding a new era characterized by speed, reliability, and a notable absence of central governing bodies. Instead of presenting a specific system's architecture, the paper is predominantly research-oriented, spotlighting the burgeoning interest in amalgamating blockchain with educational systems. The study underscores the dire need for a more in-depth exploration of blockchain-centric solutions for academic certificate verification. Notably, the researchers have employed the PRISMA framework to sift through and analyze pertinent studies, resulting in the identification of six overarching themes within the literature. This comprehensive literature review also emphasizes the gaps in current research, indicating fertile grounds for future exploration [3].

In a 2020 publication by IJSRED titled "Education Degree Fraud Detection and Student Certificate Verification Using Blockchain," the authors address the escalating challenge of verifying academic certificates' authenticity. This challenge is exacerbated by the burgeoning number of universities, graduates, and the inherent cumbersome nature of traditional verification processes. Such conventional methods, often marred by trust issues, inadvertently pave the way for fraudulent undertakings. In response, the study propounds the fusion of blockchain technology, digital signature schemes, and timestamps to craft a dependable and verifiable mechanism for academic certificate scrutiny. A notable feature is the system's incorporation of digital signatures and timestamps, which act as cornerstones, ensuring both the authenticity and integrity of the certificates. Moreover, the paper advocates the employment of "Blockers Software," providing a streamlined approach to certificate verification. Intriguingly, the study proposes two financial models that aim to equitably distribute the service's cost among primary stakeholders, namely graduates and their potential employers. The ultimate goal is to furnish students with affordable and readily verifiable proof-of-certification. This system also offers the advantage of rapid and trustable degree verification for employers. However, a quandary emerges when broaching the subject of cost-sharing. The challenge lies in keeping the service cost-effective for fresh graduates while ensuring employers don't shoulder a disproportionate financial burden, thus striving to find a middle ground that resonates with both demographics and ascertains the service's sustainability [4].

In a 2020 study published by IEEE and titled "EduBlock: Securing Educational Documents using Blockchain Technology," the authors draw attention to the alarming prevalence of document forgery, especially concerning student credentials. With a staggering figure of approximately one million students stepping into the professional world each year, the entities responsible for dispensing these pivotal documents grapple with the daunting challenge of preserving the integrity and security of student data. This task is made even more herculean due to a conspicuous absence of potent anti-forgery apparatus, leading to an unsettling scenario where fraudulent documents often slip through the cracks undetected. In response to these glaring vulnerabilities, the study proffers an innovative solution grounded in blockchain technology. The authors carve out a multi-node private blockchain infrastructure using the renowned Ethereum framework. To buttress this, they implement an off-chain storage mechanism, harnessing the private Interplanetary File System (IPFS) to house the documents securely. Capitalizing on the immutable nature of blockchain, this system is engineered to amplify the security and authenticity of educational documents, thereby drastically curtailing the necessity for traditional manual verification and voluminous paper storage [5].

In a study conducted from January to February 2020, published by IJSRED, titled "Education Degree Fraud Detection and Student Certificate Verification Using Blockchain," the authors shed light on the mounting challenges in verifying the authenticity of academic certificates. This becomes especially pressing considering the escalating numbers of universities, students, and consequent graduates. The traditional methodologies, which are not only laborious but also susceptible to mistrust, inadvertently become breeding grounds for potential malfeasance. Tackling this predicament head-on, the study suggests the amalgamation of blockchain technology with digital signature schemes and timestamps. This fusion is poised to forge a dependable pathway for academic certificate verification. Central to this system's efficacy are features such as digital signatures and timestamps, both of which bolster the certificates' authenticity and integrity. An intriguing component is the incorporation of "Blockers Software," streamlined explicitly for effortless certificate verification. Additionally, the paper introduces two fiscal models, meticulously crafted to equitably distribute the verification service's cost between recent graduates and potential employers. Students stand to gain an affordable and straightforward proof-of-certification, while employers are afforded the luxury of prompt and unerring degree verifications. However, a nuanced challenge emerges when broaching cost distribution. The task of ensuring affordability for fresh graduates while not burdening employers excessively necessitates finding a balanced financial model that resonates with both parties, ensuring the longevity and viability of the verification service [6].

In a study published on 6 June 2021 by IJCRT titled "Verification and validation of certificate using blockchain," the Indian Ministry of Education acknowledges the multifaceted challenges associated with document verification. This intricate domain is notably fraught with forgery issues, stemming predominantly from an acute absence of effective anti-forgery frameworks. Such vulnerabilities are markedly evident in educational certificates, which are of paramount significance to both students and educational institutions. The ease with which counterfeit certificates are crafted, due to an inherent opacity and non-verifiability in the issuance procedure, casts a shadow on the trustworthiness of the actual certificate holders and the respective issuing entities. Countering these glaring impediments, the study champions the adoption of a digital certificate paradigm grounded in blockchain technology. Blockchain, renowned for its immutable and lucid attributes, emerges as a potent antidote to the epidemic of certificate forgery. The proposed system envisions the digital transformation of paper certificates and their associated data. Following this, the system calculates hash values for these entities and situates them within the blockchain. Augmenting the verifiability quotient, QR codes and inquiry strings are amalgamated with the paper certificates, facilitating effortless verification either via mobile scans or web-based inquiries. Delving deeper, the authors unearth several dilemmas: the rampant proliferation of forged educational certificates corroding the very foundation of trust in the education realm; a palpable lack of transparency in conventional certificate issuance, facilitating the stealthy circulation of spurious documents; and the jeopardized credibility of stakeholders. Furthermore, the paper spotlights existing security chasms in contemporary blockchain-centric verification methods, insinuating that these systems aren't impervious to breaches. In light of these challenges, the authors advocate for blockchain-anchored digital certificates, hash value validations, and the integration of QR codes and inquiry strings. These measures, when synergized, culminate in a fortified verification landscape, resilient against potential threats [7].

In a 2021 publication by IJCCC titled "Verification of University Student and Graduate Data using Blockchain Technology," the transformative potential of blockchain technology in reshaping the landscape of education and academic achievement tracking is expounded. The traditional paradigm, which hinges on education documents, is identified as having inherent flaws: a conspicuous absence of granular academic performance data specific to periods and a susceptibility to unauthorized alterations. As we navigate deeper into the digital age, the urgency to streamline and fortify document verification mechanisms intensifies. Enter the UniverCert platform, an avant-garde prototype developed atop the Ethereum blockchain. This platform taps into the might of a decentralized, globally dispersed peer-to-peer network, facilitating a synergy between educational entities and the blockchain ecosystem. A salient feature of UniverCert is its capability to meticulously track student data, vet academic achievements, and share documents securely with vested parties. Moreover, the platform champions a consortium blockchain design, amping up data storage and security dimensions. As solutions, the platform brings to the fore a myriad of advantages, including detailed academic tracking, mitigation of unauthorized document alterations, streamlined document verifications, and enhanced data management for educational institutions. All these elements collectively underscore the UniverCert platform's potential as a holistic remedy to the extant challenges plaguing the education sector [8].

III. METHODOLOGY

SYSTEM MODULES

Admin: This includes schools, colleges, and universities. **Student:** Individuals seeking document verification. **Company:** Organizations that might require student document verification.

The system introduces a novel method for dynamic document generation leveraging a bespoke blockchain:

- Initially, a student requests a document through a web portal, uploading all necessary educational records.
- This web portal acts as an authenticated intermediary, ensuring the validity of documents with respective educational institutions like universities, colleges, or other relevant entities.
- Upon successful verification, the data is recorded onto the blockchain. Simultaneously, a unique identifier or QR code is generated and provided to the student.
- Students can then share this QR code or unique ID with organizations, eliminating the need to present physical copies of their documents.
- For verification, the organization can input the provided QR code or ID into the portal, accessing the student's document for confirmation.
- Our proprietary smart contract on the blockchain automates and secures this entire procedure.

IV. PROPOSED SYSTEM

Efficient Verification of Educational Credentials through Blockchain:

The conventional method of validating educational documents is notably time-consuming and cumbersome. Transitioning to electronic academic records simplifies this process, removing unnecessary bureaucratic stages. Our solution incorporates blockchain technology to produce dynamic QR codes and unique documents for each student, ensuring secure data validation. The incorporation of smart contracts into the blockchain further streamlines operations. This research revolves around creating a dedicated blockchain system based on an open-source foundation.

System Framework:

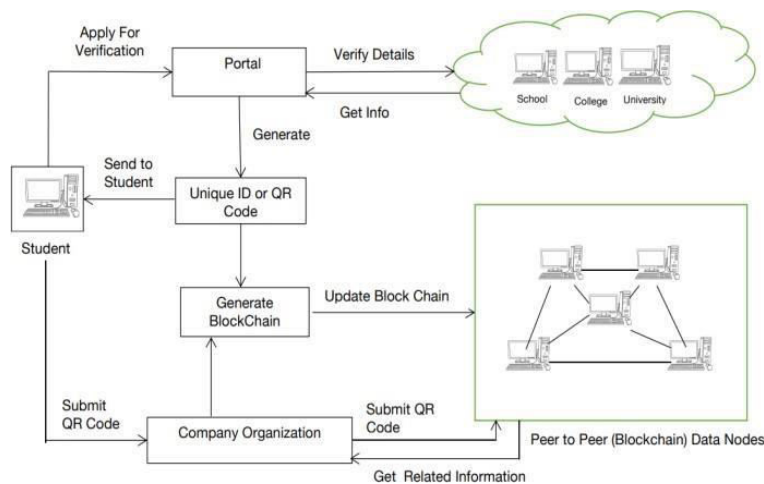


Fig- System Architecture

Proposed System Steps and Features:

- Admin-Centric Document Generation: Using a specialized blockchain, the admin (schools, colleges, universities) can generate documents and integrate them within the blockchain environment.
- Student Application Process: Students initiate the journey by uploading their academic credentials to a dedicated

online platform. The system, acting as a trusted intermediary, works in the background, communicating with the relevant educational institutions for document validation. Once verified, the blockchain stores the data, and a unique document ID or QR code is produced for the student. This QR code or ID acts as a digital representation of the student's educational achievements, eliminating the need for physical papers.

- **Company/ Organization Verification:** Companies or organizations interested in verifying a student's credentials can simply input the provided QR code or ID on the platform. The system fetches the student's records, offering a swift and reliable verification process.
- **Integration of Smart Contracts:** The entire procedure, from student application to company verification, is governed by a smart contract developed by our team. This ensures transparent, tamper-proof, and efficient operations.
- **Security Considerations:** The system's architecture is designed to resist various network threats, such as DOS and MiM attacks, ensuring reliable and secure verifications.

V. MATHEMATICAL MODEL

QR GENERATION CODE

```
public class Create_QR {
    public static void CreateQR(String qrCodeData, String filePath)
    {
        try {
            String charset = "UTF-8"; // or "ISO-8859-1"
            Map <EncodeHintType, ErrorCorrectionLevel > hintMap = new HashMap <EncodeHintType, ErrorCorrectionLevel > ();
            hintMap.put(EncodeHintType.ERROR_CORRECTION, ErrorCorrectionLevel.L);
            BitMatrix matrix = new MultiFormatWriter().encode(new String(qrCodeData.getBytes(charset)), BarcodeFormat.QR_CODE, 200, 200, hintMap);
            MatrixToImageWriter.writeToFile(matrix, filePath.substring(filePath.lastIndexOf('.') + 1), new File(filePath));
            System.out.println("QR Code image created successfully!");
        } catch (Exception e) {
            System.err.println(e);
        }
    }
    public static void main(String[] args) {
        CreateQR("qrCodeData", "C:\\Users\\JP\\Desktop\\QR\\a1.png");
    }
}
```

Explanation:

1. Import Statements:

```
import java.io.File;
import java.util.HashMap;
import java.util.Map;
import com.google.zxing.BarcodeFormat;
import com.google.zxing.EncodeHintType;
import com.google.zxing.MultiFormatWriter;
import com.google.zxing.client.j2se.MatrixToImageWriter;
import com.google.zxing.common.BitMatrix;
import com.google.zxing.qrcode.decoder.ErrorCorrectionLevel;
```

These statements import necessary classes and interfaces from different packages.

For example, classes for handling files (File), data structures like HashMap, and classes from the ZXing library (MultiFormatWriter, MatrixToImageWriter, BitMatrix, BarcodeFormat, EncodeHintType, ErrorCorrectionLevel) are imported.

CreateQR Method:

```
public static void CreateQR(String qrCodeData, String filePath) {
    // Method body
}
```

This method takes two parameters: qrCodeData (the data to be encoded into the QR code) and filePath (the path where the generated QR code image will be saved). It uses the ZXing library to generate the QR code image and save it to the specified file path.

3. Main Method:

```
public static void main(String[] args) {
    CreateQR("qrCodeData", "C:\\Users\\JP\\Desktop\\QR\\a1.png");
}
```

This is the entry point of the program. It calls the CreateQR method with sample data (qrCodeData) and a file path where the QR code image will be saved.

4. ZXing Library:

The ZXing library is used for encoding and decoding various types of barcodes, including QR codes. In this code, it's used to encode the data provided (QRCodeData) into a QR code image and save it to the specified file path.

5. Error Handling:

The code includes a try-catch block to handle exceptions that may occur during QR code generation. If an exception occurs, it prints an error message to the standard error stream.

VI. RESULTS



Fig- Home Page

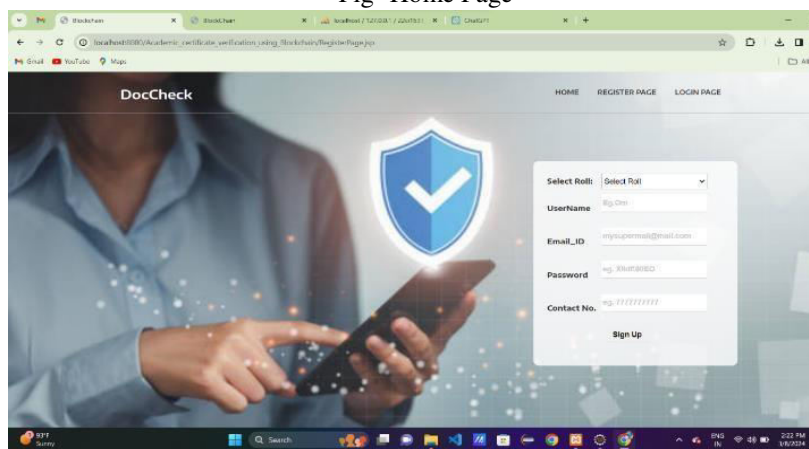


Fig- Registration Page

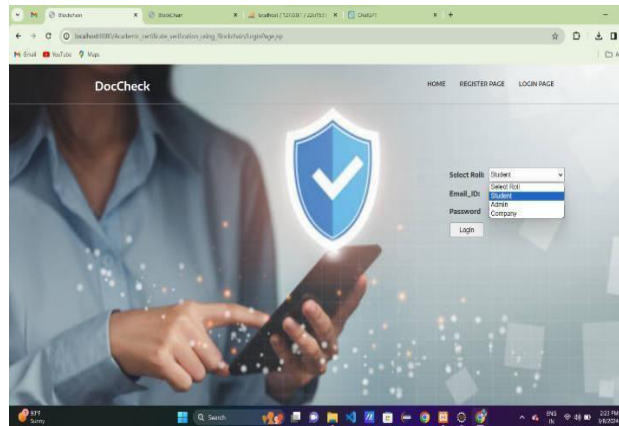


Fig- Login Page

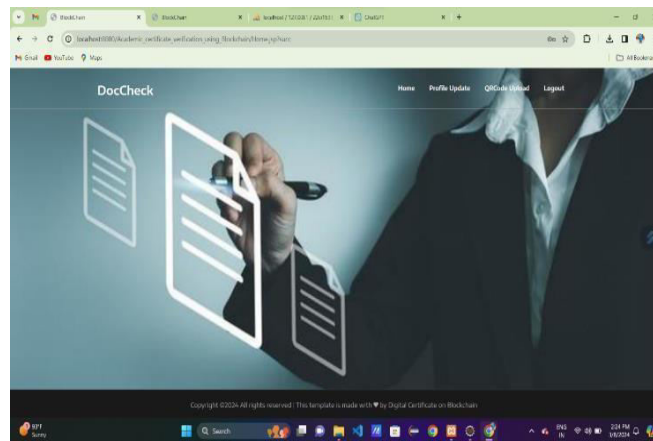


Fig-User (Student)Section

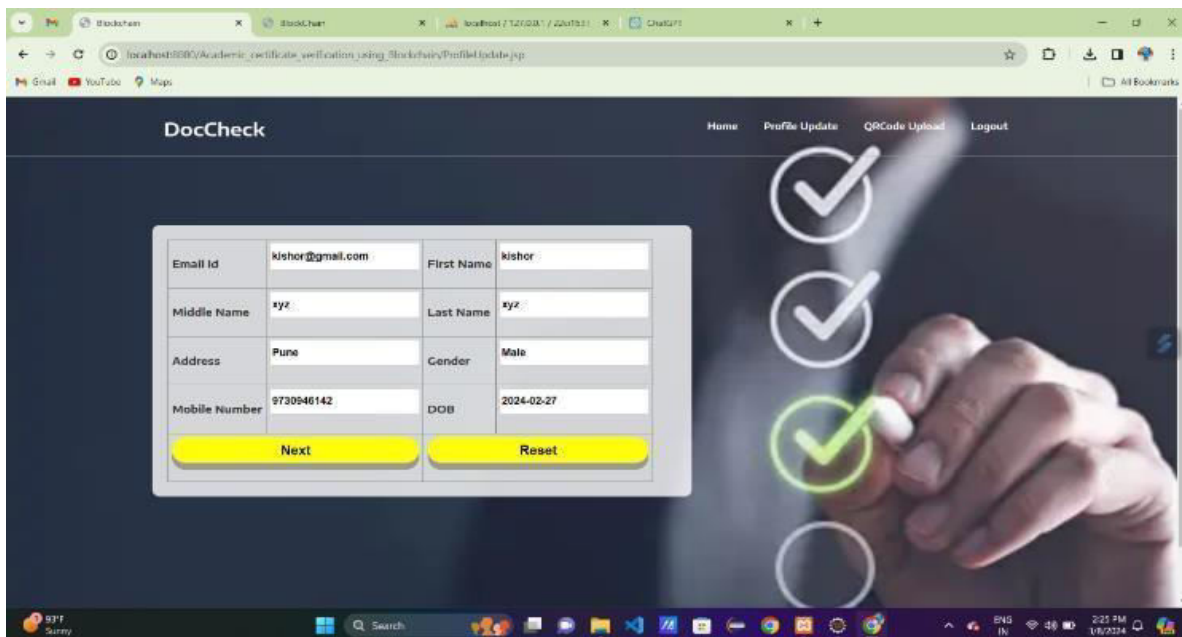


Fig- Profile Update

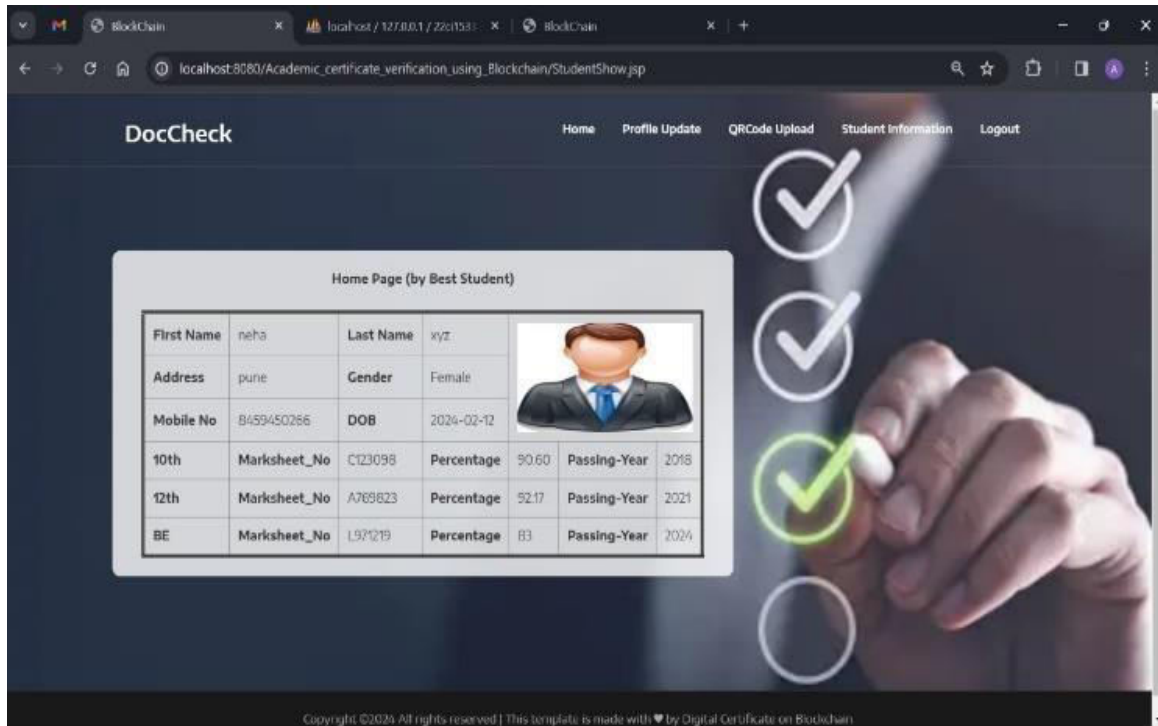


Fig- Education Details

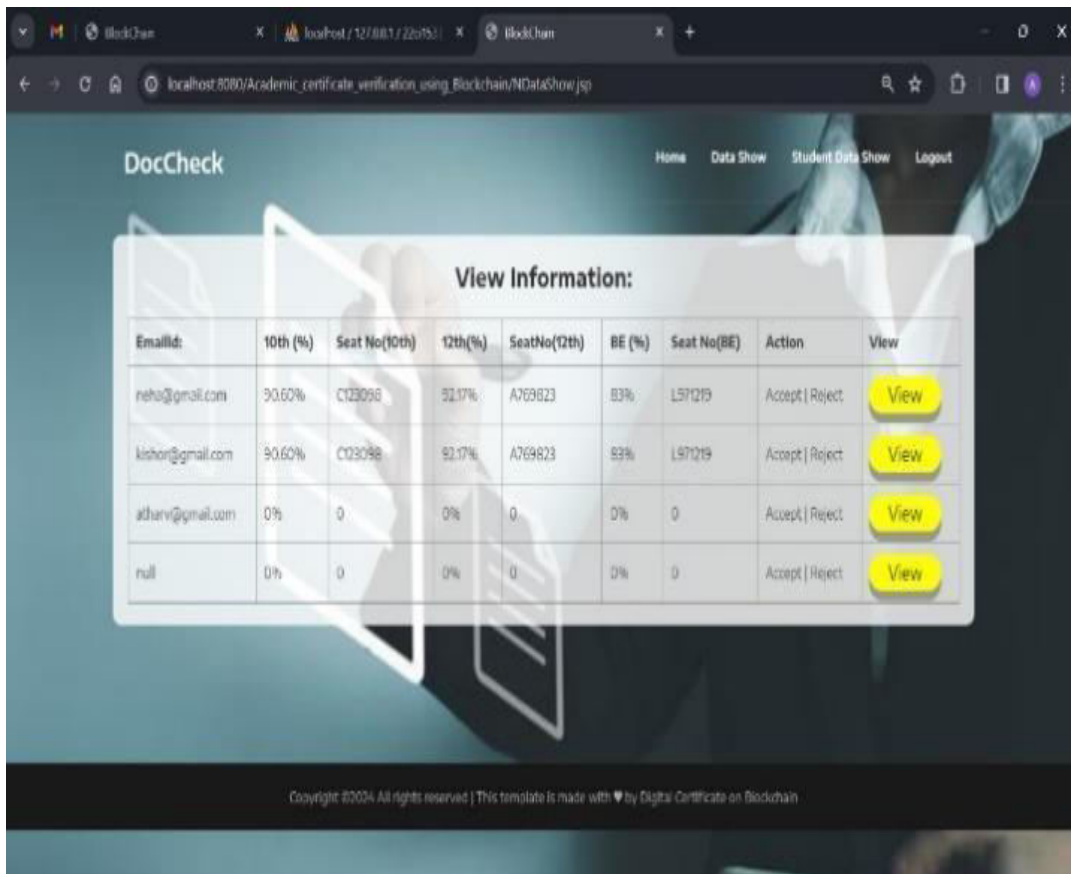


Fig- Admin Section

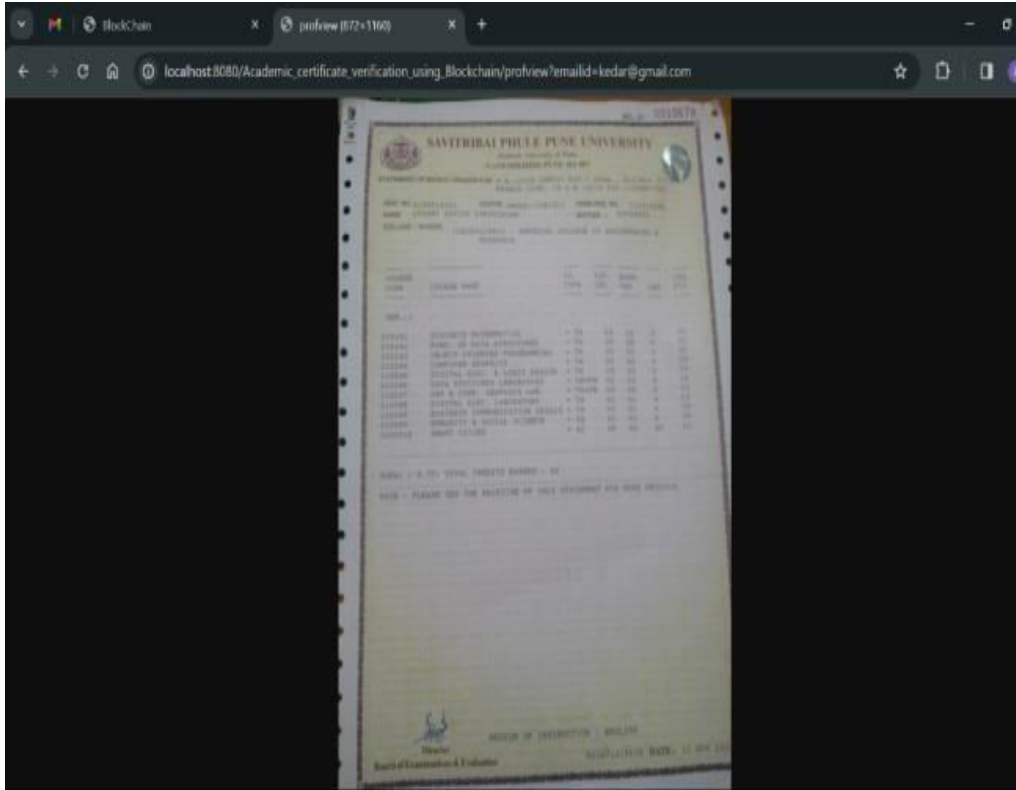


Fig- Admin Side student document

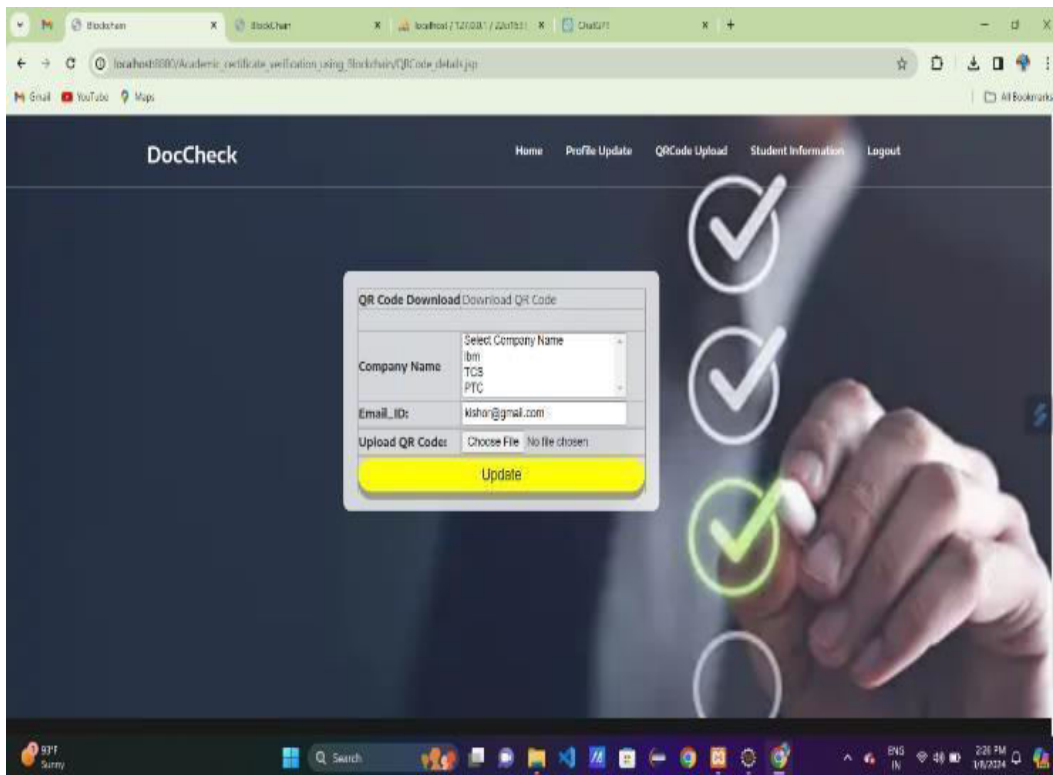
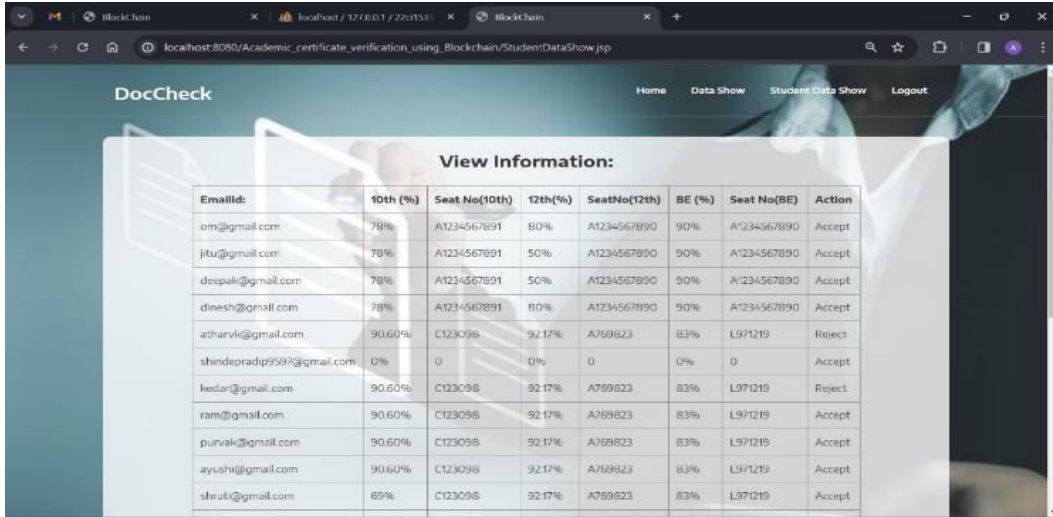


Fig- Student Record



EmailId:	10th (%)	Seat No(10th)	12th(%)	SeatNo(12th)	BE (%)	Seat No(BE)	Action
om@gmail.com	78%	A1234567891	80%	A1234567890	90%	A^234567890	Accept
jitu@gmail.com	78%	A1234567891	50%	A1234567890	90%	A^234567890	Accept
deepak@gmail.com	78%	A1234567891	50%	A1234567890	90%	A^234567890	Accept
dinesh@gmail.com	78%	A1234567891	80%	A1234567890	90%	A^234567890	Accept
atharvk@gmail.com	90.60%	C123098	92.17%	A769823	83%	L971219	Reject
shindepradip9597@gmail.com	0%	0	0%	0	0%	0	Accept
keedar@gmail.com	90.60%	C123098	92.17%	A769823	83%	L971219	Reject
ram@gmail.com	90.60%	C123098	92.17%	A769823	83%	L971219	Accept
purvak@gmail.com	90.60%	C123098	92.17%	A769823	83%	L971219	Accept
ayushi@gmail.com	90.60%	C123098	92.17%	A769823	83%	L971219	Accept
shruti@gmail.com	65%	C123098	92.17%	A769823	83%	L971219	Accept

Fig- Upload QR Code



Fig- Student QR Code

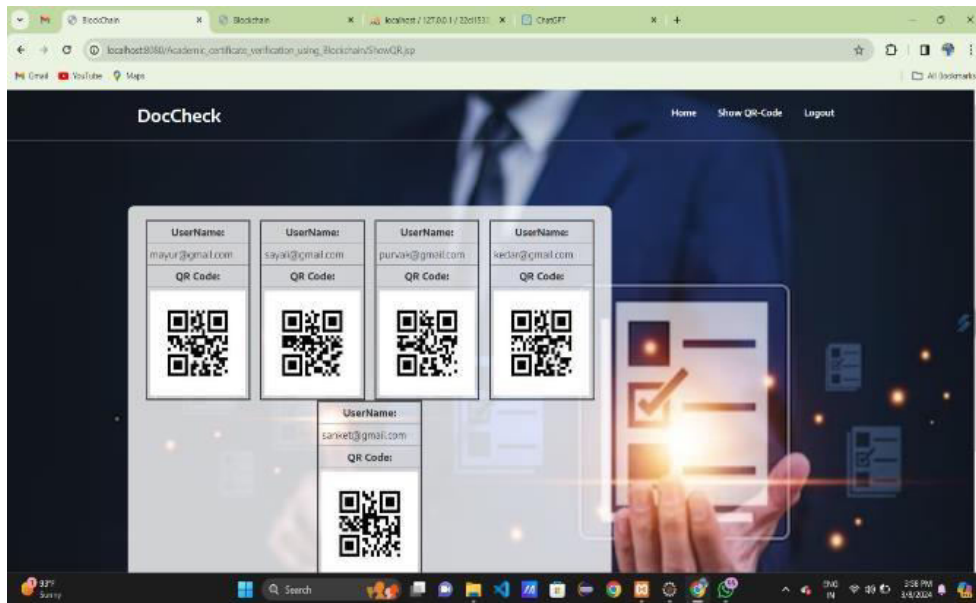


Fig-Company side Student QR code

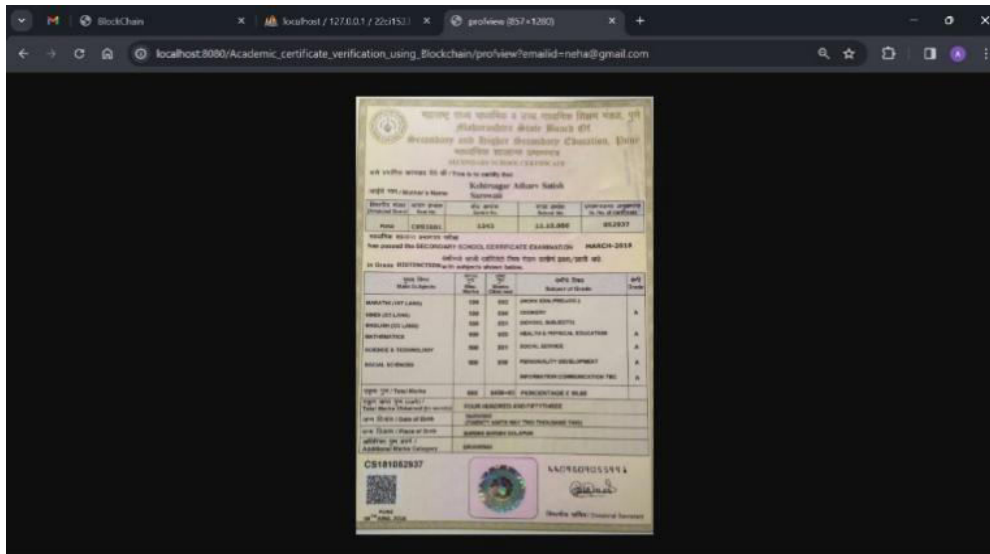


Fig- Company Side Document

VII. CONCLUSION

The field of document verification is complex, and there is a growing interest in making IT systems more reliable and effective. Blockchain technology presents numerous opportunities in this area. Many challenges in document verification, especially those related to data sharing and communication, could benefit from a unified blockchain framework. There is a pressing need to deeply study and design blockchain systems that are both secure and respectful of confidentiality. As we delve deeper into using blockchain for this purpose, it is crucial to understand its strengths and limitations fully. Lastly, to truly gauge its effectiveness, we should compare blockchain-based systems to existing methods, looking at factors like speed, cost, and overall.

REFERENCES

1. Mrs. R. Sugantha lakshmi, Mrs. G. Chandra Praba, Mrs. K. Abhirami, Mrs. S. Puvaneswari "BLOCKCHAIN BASED CERTIFICATE VALIDATION SYSTEM IRJMETS" 07/July-2022
2. Rasha M. Abd El-Aziz, Anis Ben Aissa, Ahmed I. Taloba "EXPERIMENTAL ANALYSIS OF DOCUMENT VERIFICATION SCHEME USING BLOCKCHAIN LOGICS OVER SECURED CLOUD ENVIRONMENT" IAEME - 9, September 2020
3. Aniket vijay Ratnaparakh, Sagar Shankar Jadhav, Shivraj Manikrao Patil, "Education Degree Fraud Detection and Student Certificate Verification Using Blockchain" IJSRED Jan-Feb 2020
4. Jashuva Peyyala, "A Survey on Blockchain Based Documentation Verification" IJRASET- Apr 2022
5. Rohan Hargude, Ghule Ashutosh, Abhijit Nawale, Pro. Sharad Adsure "Generating E-Certificate and Validation using Blockchain" IJCRT - 7 July 2021
6. Rana F. Ghani, Asia Ali Salman Al-Karkhi, Shakir Mahmood Mahdi "Proposed Framework for Official Document Sharing and Verification in E-government Environment Based on Blockchain Technology" Baghdad Science Journal - 2022
7. 1Rohan Hargude, 2Ghule Ashutosh, 3Abhijit Nawale, 4 Sharad Adsure, "Verification and Validation of Certificate Using Blockchain" IJCRT - 2021
8. Jashuva Peyyala, "A Survey on Blockchain Based Documentation Verification" IJRASET - 2022
9. Muhammad Umar Abdullahi, Dr. G. I.O. Aimufua, Adamu Aminu Muhammad "Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code" IOSR- 2022
10. Shantanu Sarode, Utkarsha Khandare, Shubham Jadhav, Avinash Jannu, Vishnu Kamble, Digvijay Patil "Document Manipulation Detection and Authenticity Verification Using Machine Learning and Blockchain" IRJET - 2020
11. Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, Shaikh Akib Shahriyar "A Blockchain Based Authentication System for Digital Documents" researchgate2021
12. Steven P. Chatman, "Comparable Standards for Credit Hour Production" valuative/Feasibility- 1995
13. Miss. Jayashri Rajendra Mahale*, Prof. E.M. Chirchi "Modeling And Simulation for Digital Document Verification Scheme Using Blockchain in P2P Network" IJSRCS - 2021.



15. Cristhian Martinez-Rendon¹ , Diego Camarmas-Alonso¹, Jesus Carretero¹ , Jose L. GonzalezCompean² “On the continuous contract verification using blockchain and real time data” Universidad Carlos III de Madrid – 2021.
16. A.Gayathiri, J.Jayachitra, Dr.S.Matilda. “Certificate validation using blockchain.” IEEE 7th International Conference on Smart Structures and Systems ICSSS 2020, Pavitra Haveri¹ Rashmi U, Narayan D.G., Nagaratna K., Shivaraj K. “Securing Educational Documents using Blockchain Technology” IEEE – 49239.
17. Padmavati E Gundgurti, Kranthi Alluri, Poornima E Gundgurti, Sai Harika K, Vaishnavi G. “Smart and Secure Certificate Validation System through Blockchain” IEEE Xplore Part Number: CFP20N67- ART.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details