

Educational Certificate Verification System Using Block Chain Technology

N sudha laxmaiah¹, Chowdary Ambika², L beaula³

¹Associate professor, Department of CSE, Bhoj Reddy Engineering College for Women, India

^{2,3}B.Tech Student, Department of CSE, Bhoj Reddy Engineering College for Women, India

ABSTRACT

In response to the challenges faced in managing and verifying traditional paper-based educational certificates, our project proposes a transformative solution harnessing the power of blockchain technology. By digitizing certificates and employing the SHA256 algorithm to generate unique hash codes, we ensure the integrity and authenticity of each document. These hashed certificates are then securely stored on a blockchain network, leveraging its decentralized and immutable nature to prevent tampering and unauthorized alterations. Through a dedicated application, authorized parties can easily verify the authenticity of a certificate by comparing its hash code with the one stored on the blockchain. This approach not only streamlines the validation process but also enhances security, reliability, and accessibility in the realm of digital credentialing. By embracing blockchain technology, we pave the way for a future where educational certificates are securely managed and easily validated, ushering in a new era of trust and efficiency in the digital landscape.

INTRODUCTION

Blockchain was introduced in the year 2008 by Satoshi Nakamoto. Blockchain is one of the online ledgers which provide decentralized and transparent data sharing. In this project, we design an android application used to provide secure verification of our certificates. In nowadays, all Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should

not be easily accessible to outside entities. Hence, there is a high need for an efficient mechanism, that can guarantee the information in such certificates is original, which means the document has originated from a reliable and authorized source and is not forged. Various systems have been designed to secure e-certificates for education institutions and to store them securely in cloud-based systems. Blockchain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also helps in eliminating the need for constant verification of certificates. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity, and confidentiality of graduation certificates would be improved. Technologies that exist in security domains include digital signatures, which are used in digital documents to provide authentication, integrity, and non-repudiation. Also with blockchain in play, the storage of certificates are more secure. With these technologies, an application created that facilitates the secure validation of digital certificates.

The project focuses on certificate verification as well as a validation system. For this, we have referred few previously published papers and works of the various individual in this field. Our Literature Survey mainly focused on Blockchain Technology, an advanced Storage System, and Digital Certificate Validations.

An Overview of Blockchain Technology which provided in-depth knowledge regarding Blockchain. It introduced various terms regarding this technology and the most important concept called a smart contract. In the Blockchain, the hash of the data is stored in its preceding block, and it forms a long chain of nodes. If data is changed, its hash will change, and it won't match with the hash value stored in the previous block and hence letting us know about the tampering of data.

PROPOSED SYSTEM

The student's achievements available in the form of degree certificate, mark sheet, value added certificate, etc., will become an important weightage for recruitment or higher studies. The Education institution awards and degree certificates may have only the names of the institution and the student's data. In this scenario there is a lack of effective antiforge mechanism, due to this event many times the graduation certificate to be forged often is found. To solve the problem of fake certificates, the blockchain technology would store the certificate in digital form. The immutability nature of blockchain makes digital certificate in the distributed ledger is very difficult to tamper or modify also it is very easy

to verify the originality of digital certificate.

DESIGN

As the client, handling user interactions, and an Ethereum blockchain functions as the system design involves a client-server architecture where a Flask web application serves decentralized server for storing educational certificate details through smart contracts. The Flask application defines routes for user authentication, certificate creation, and viewing, using HTML templates to render the user interface. The Ethereum integration with the web3 library manages the connection to the blockchain, enabling interactions with deployed smart contracts for storing and retrieving company and certificate information. QR codes, generated by PyQRCode, facilitate certificate authentication, while digital signatures are created using the hashlib library. The system ensures security, transparency, and efficiency in educational certificate verification by leveraging blockchain technology and web development tools. Continuous improvement is recommended for scalability, error handling, and user experience enhancements.

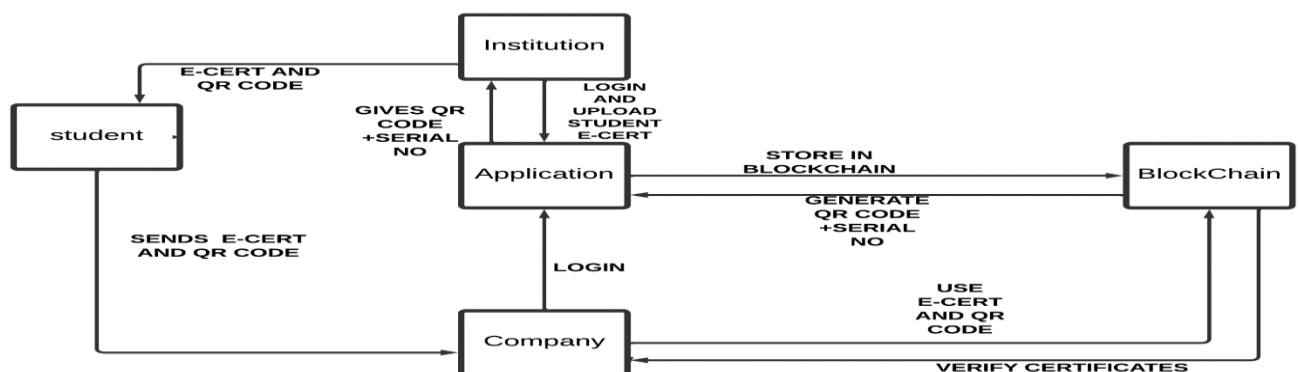


Figure 4.1 System Architecture

METHODOLOGY

In this proposed system the academic, sports certificates are converted into digital certificates. Then the certificates are added with the hash values generated for the digital certificate and store it into the blocks. The SHA256 algorithm used for generating the hash value. Each block consists of the hash value, timestamp, and hash value of the previous block. These blocks are linked together in the form of blockchain. The institution registers the student details in our interface (application) by providing details like name, email id and these are stored in the database. The certificate issued by the registrar is stored in the application and they form a blockchain. The employer or verifier can validate the certificate by entering the student details.

DIGITAL CERTIFICATE CREATION

In this, the student certificates are converted into digital certificates. The academic certificate and sports certificate are issued by the institution are stored in the database. By using the analog image to digital image conversation method, the certificate can be converted into a digital certificate. The value 0's and 1's are created for each certificate. In a digital image, all the coordinates on 2-d function and the corresponding values are finite. Each value considered a pixel. By using admin login, the administrator login to our application to upload the student's certificate in the application then it will convert an analog image to digital image. The next page of the application shows the add student and add a certificate. If an admin clicks the added certificate, the student certificate is uploaded.

HASH CODE GENERATION

The SHA 256 algorithm is used to generate the hash value for the certificate. This algorithm takes input in different size and produces the output in a fixed size.

This algorithm needs to define the mapping scheme, initial condition, and parameters. Verifying process is started by using the same initial condition and parameters to generate the same output. When the certificate is uploaded, the hash value is created for the digital certificate.

DIGITAL CERTIFICATE VALIDATION

In this, the created digital certificate is validated. Certificates that are stored in the blockchain are validated by matching the hash value. The verification of the hash value of the certificate is used to avoid tampering. The employer or verifier can log in to the application using their login id and password. They can select certificate which they want to validate. Then tap the submit button in the application. If the certificate is original the output will be authentication successful. If the certificate is not original or modified the output will be authentication failed.

WORKING OF APPLICATION

In our application the first page is admin login, the next page consists of upload student details and certificate and last verifier page. The admin can log in to our application using the admin username and password. Then the admin can add the student details and their certificates by uploading the student details and certificate and then pressing submit button. Next, the verifier can validate the certificate by logging in to the company signup page using the verifier username and password. Now the verifier can select the certificate and uploads the certificate and tap the submit button. If the uploaded certificates are original then the result will be authentication successful. Otherwise, the result will be authentication failed.

RESULTS

OUTPUT SCREENS

In below screen click on 'Educational Authority Login' link to get below login screen

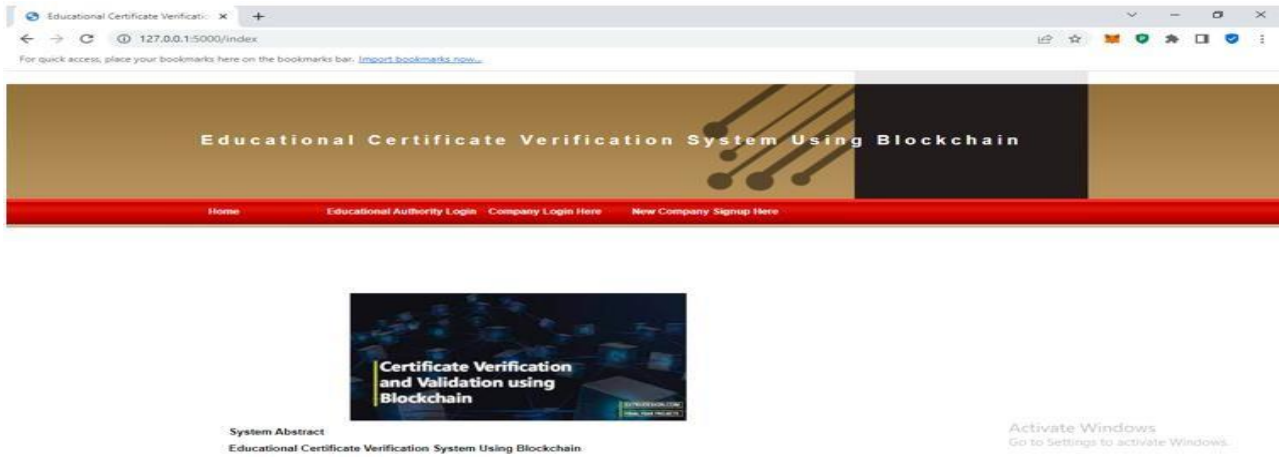


Figure 5.1.Home Page

In below screen admin is login and after login will get below screen

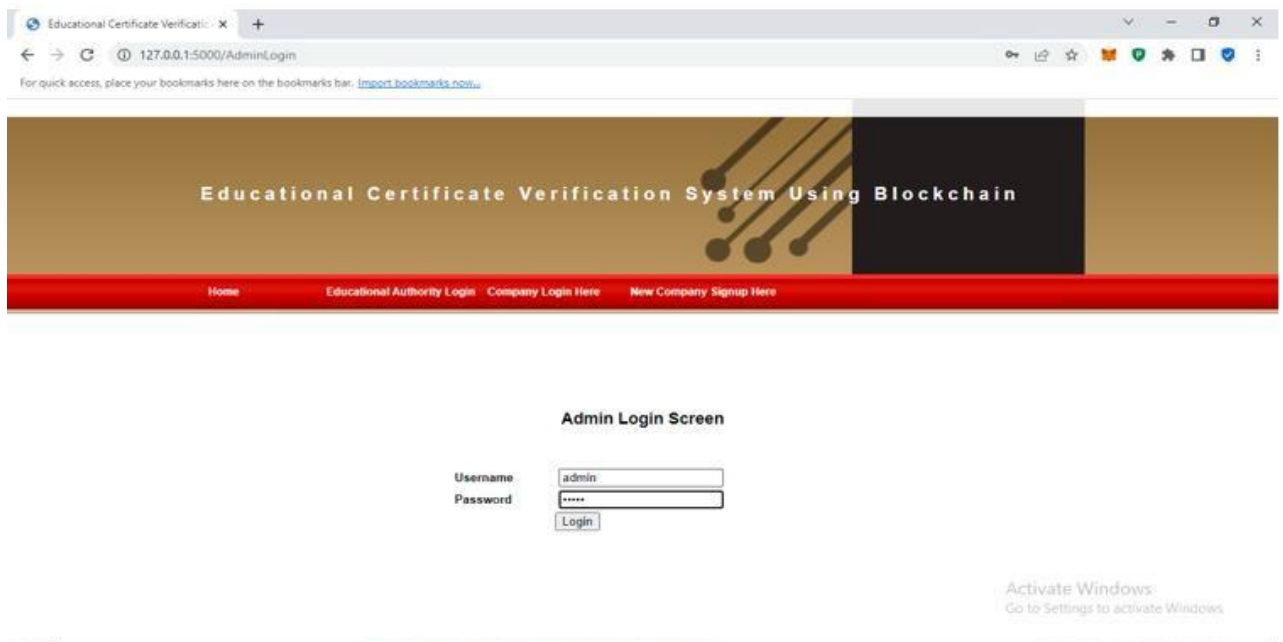


Figure 5.2. Admin Login Screen

In below screen admin can click on 'Upload New Certificates' link to upload certificate

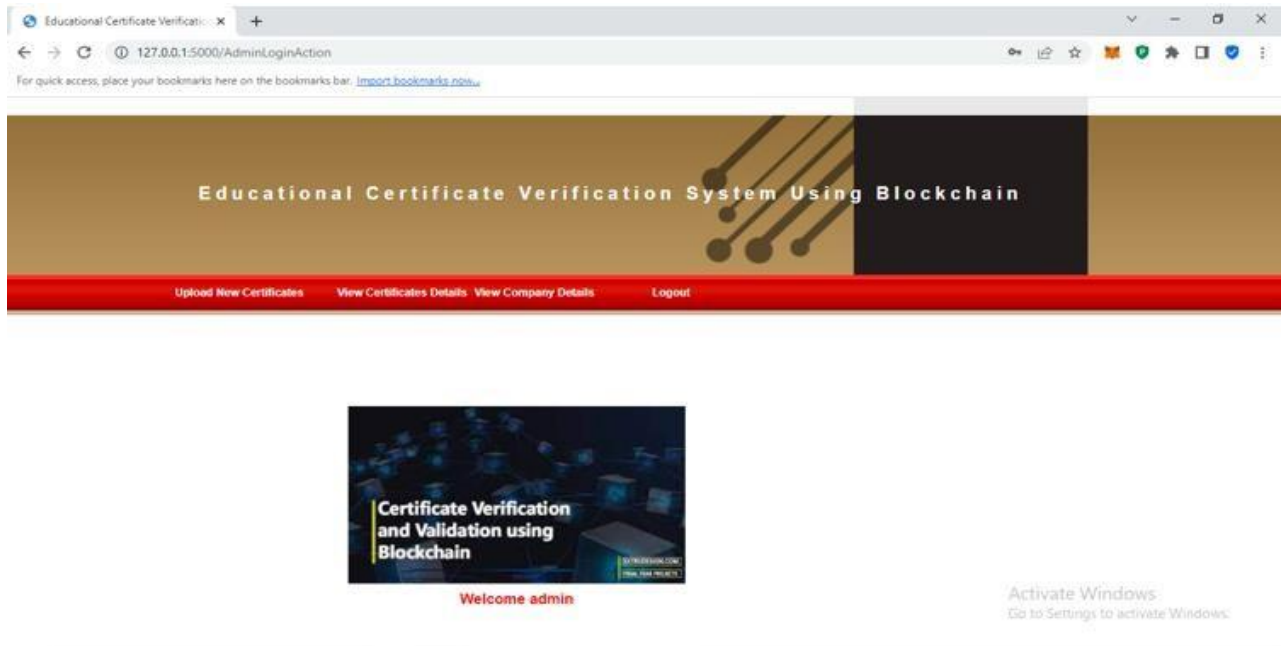


Figure 5.3. Admin Home Page

In below screen admin is adding student details and then uploading certificate and then press ‘Submit’ button to get below output

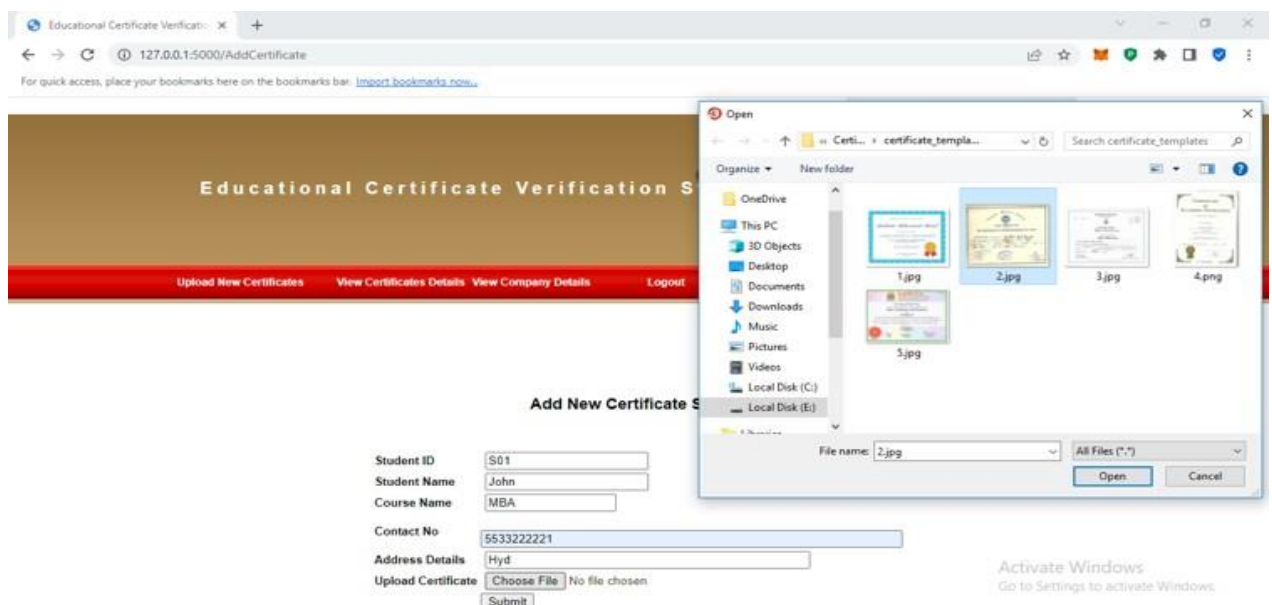


Figure 5.4. Add New Certificate

In below screen student details added and we can see digital signature generated and stored in Blockchain for uploaded certificates and now admin can click on ‘Click Here to Download QR Codeimage’ button to download QR CODE and get below output

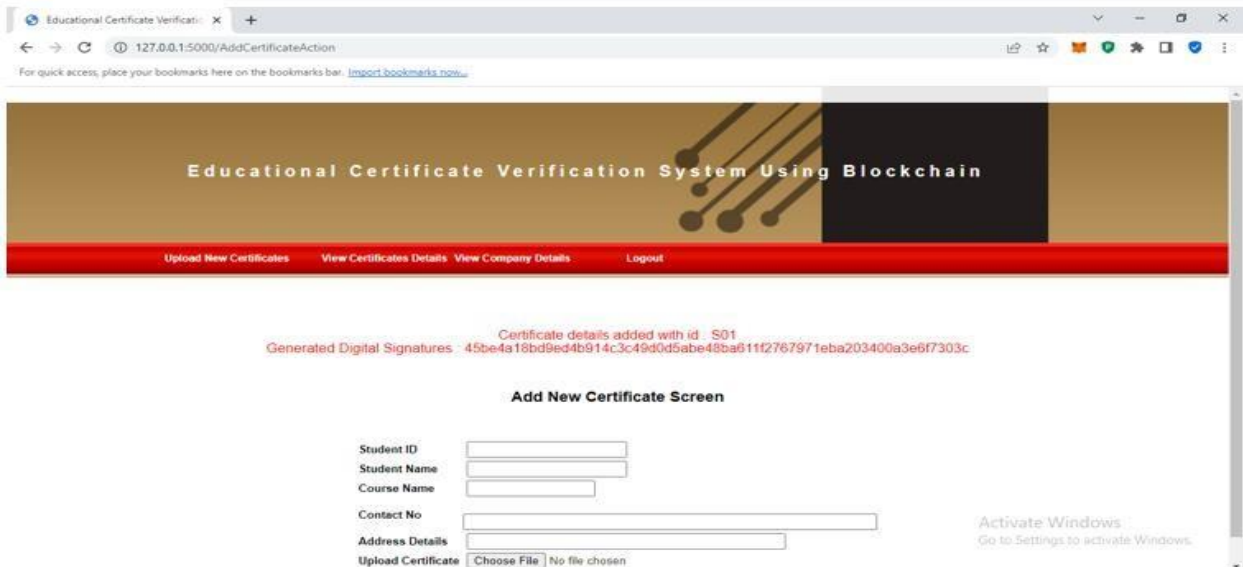
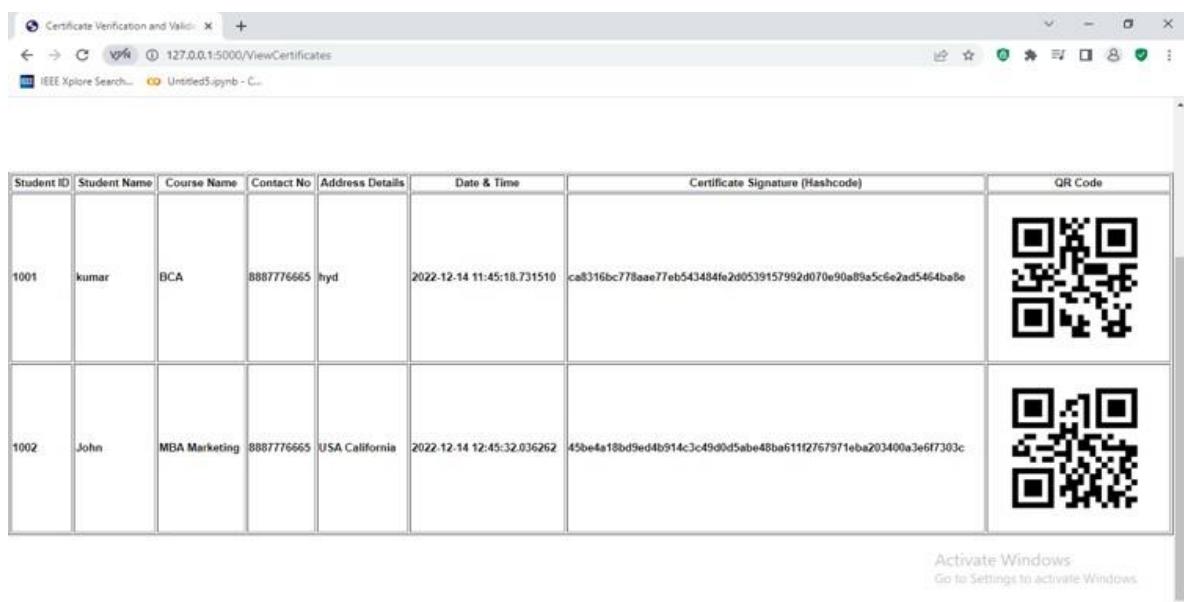


Figure 5.5. Certificate Uploaded

In below screen we can see different certificates of same or new student stored in Blockchain. Now admin can click on “View Companies Details’ to allow admin to view registered companies





Student ID	Student Name	Course Name	Contact No	Address Details	Date & Time	Certificate Signature (Hashcode)	QR Code
1001	kumar	BCA	8887776665	hyd	2022-12-14 11:45:18.731510	ca8316bc778aae77eb543484fe2d0539157952d070e90a89a5c6e2ad5464ba8e	
1002	John	MBA Marketing	8887776665	USA California	2022-12-14 12:45:32.036262	45be4a18bd9ed4b914c3c49d0d5abe48ba611f2767971eba203400a3e6f7303c	

Figure 5.6. Certificate Details

In below screen admin can view list of registered companies

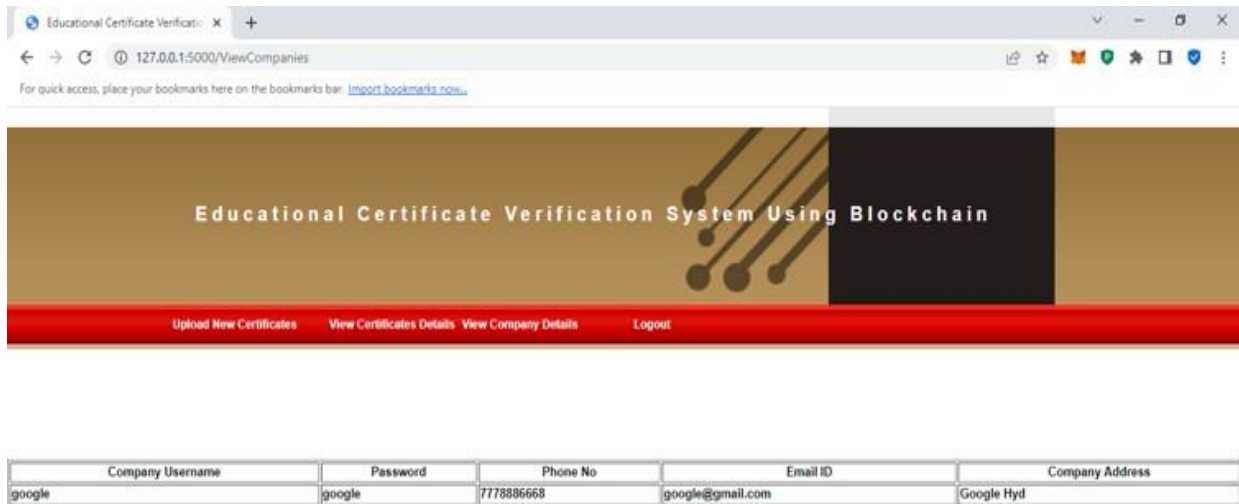


Figure 5.7. Company Details

In below screen company is entering signup details and press button to store details in Blockchain and will get below output

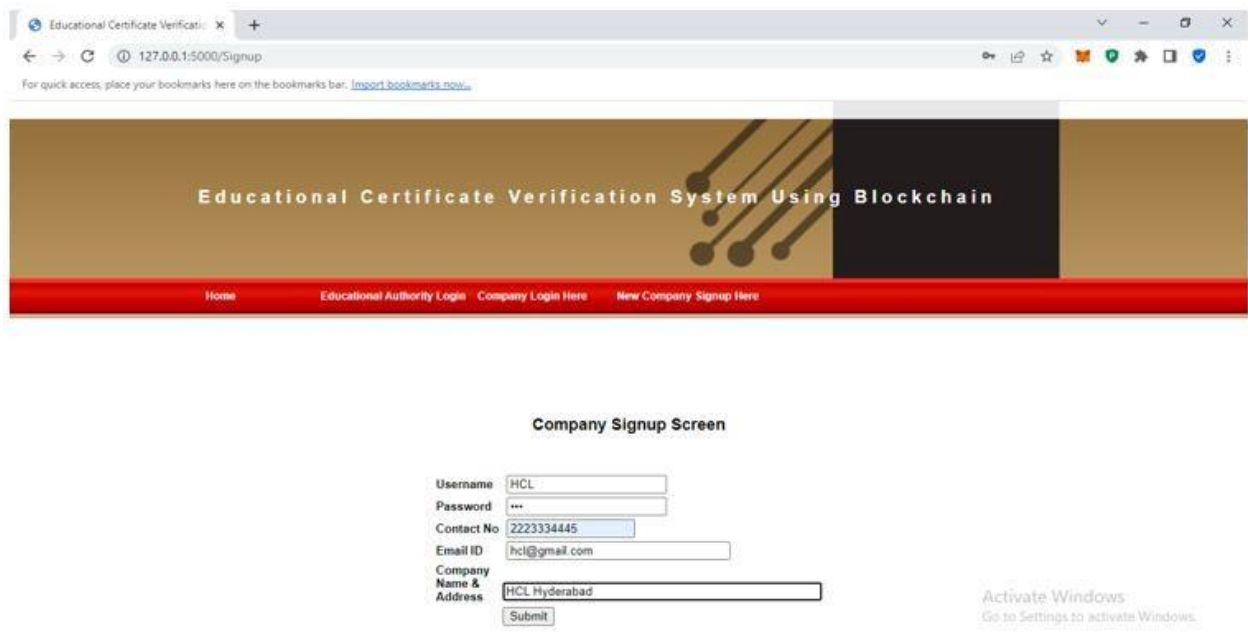


Figure 5.8. Company Signup

In below screen we can see company signup task completed and now click on ‘Company Login Here’ link to get below login screen

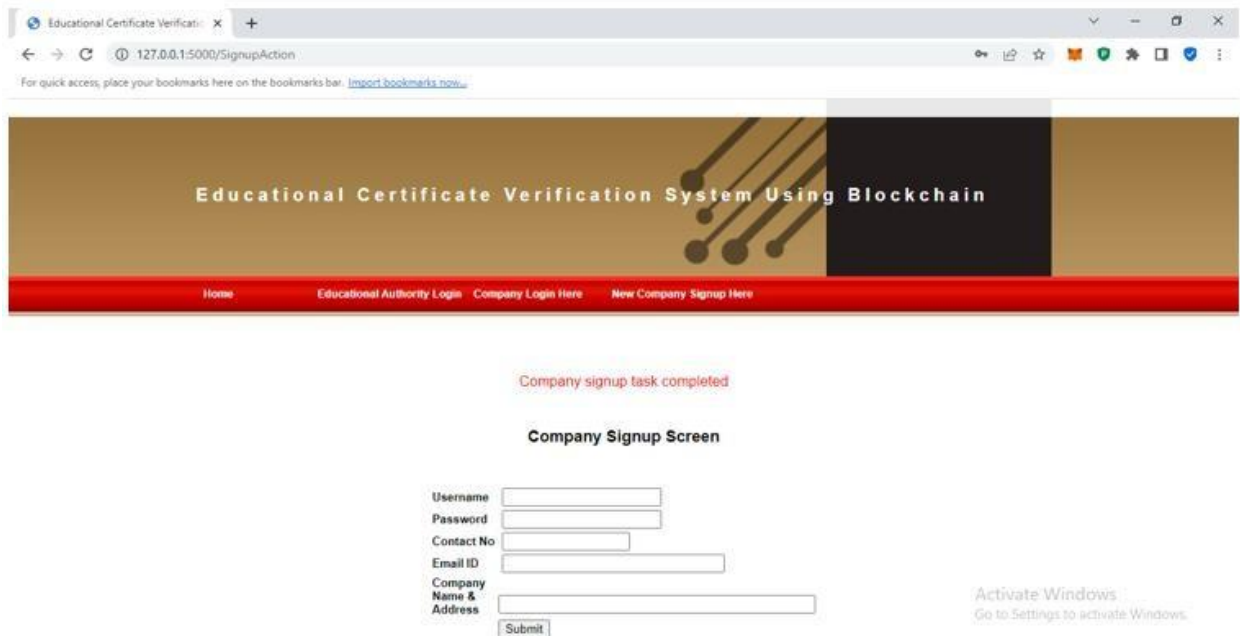


Figure 5.9. Company Signup Task Completed

In below screen company is login and after login will get below screen

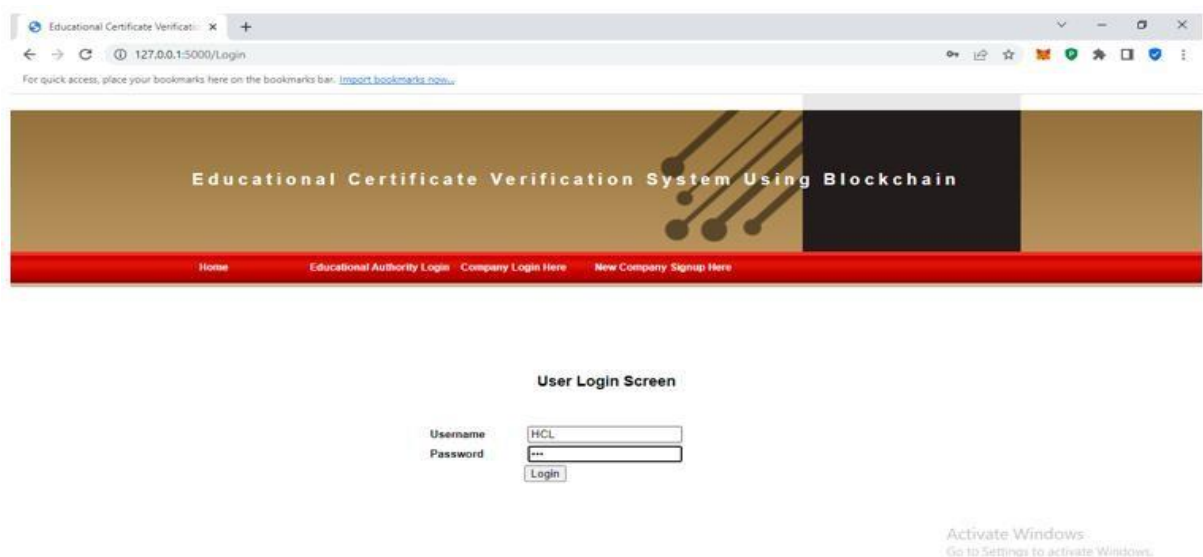


Figure 5.10. Company Login

In below screen company can click on 'Authenticate Certificate' to upload certificate copy received from student and perform verification



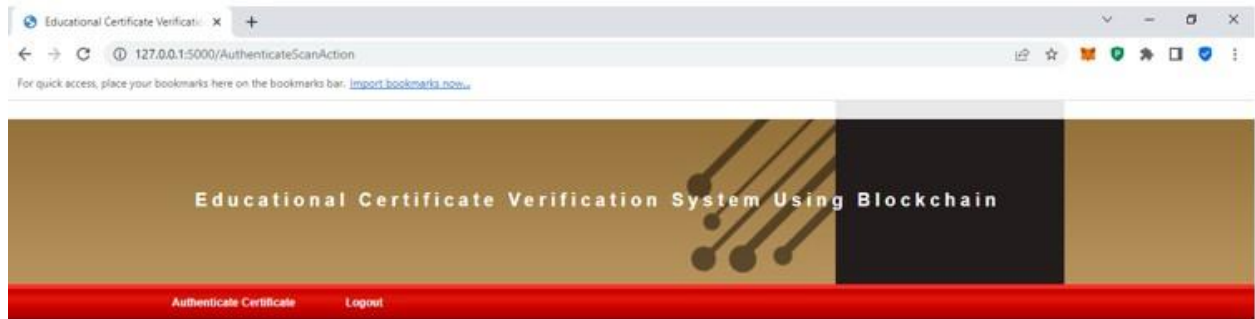
Figure 5.11. Company Home Page

In below screen company can upload certificate and get below details if authenticated



Figure 5.12. Company Authenticate Certificate

In below screen company can view all details of uploaded certificated and in last column we can see authentication successful



Student ID	Student Name	Course Name	Contact No	Address Details	Date & Time	Certificate Signature (Hash Code)	Status
S01	Suresh	BCA	888	Hyd	2022-07-29 11:53:26.710447	ca8316bc778aae77eb543484fe2d0539157992d070e90a89a5c5e2ad5464ba8e	Authentication Successful

Figure 5.13. Company Authentication Successful

In below screen company can upload certificate and get below details if authenticated

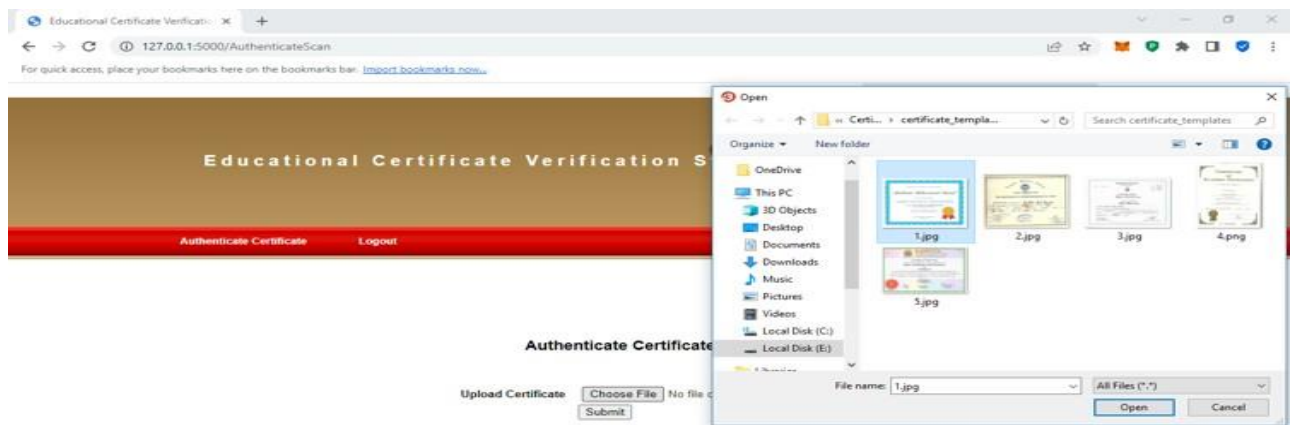


Figure 5.14. Company Authenticate Certificate

In below screen we can see Authentication failed for uploaded certificate. Now company or educational institution can validate certificate by scanning QR code and to do that, just double click on 'RunWebCam.bat' file to get below output

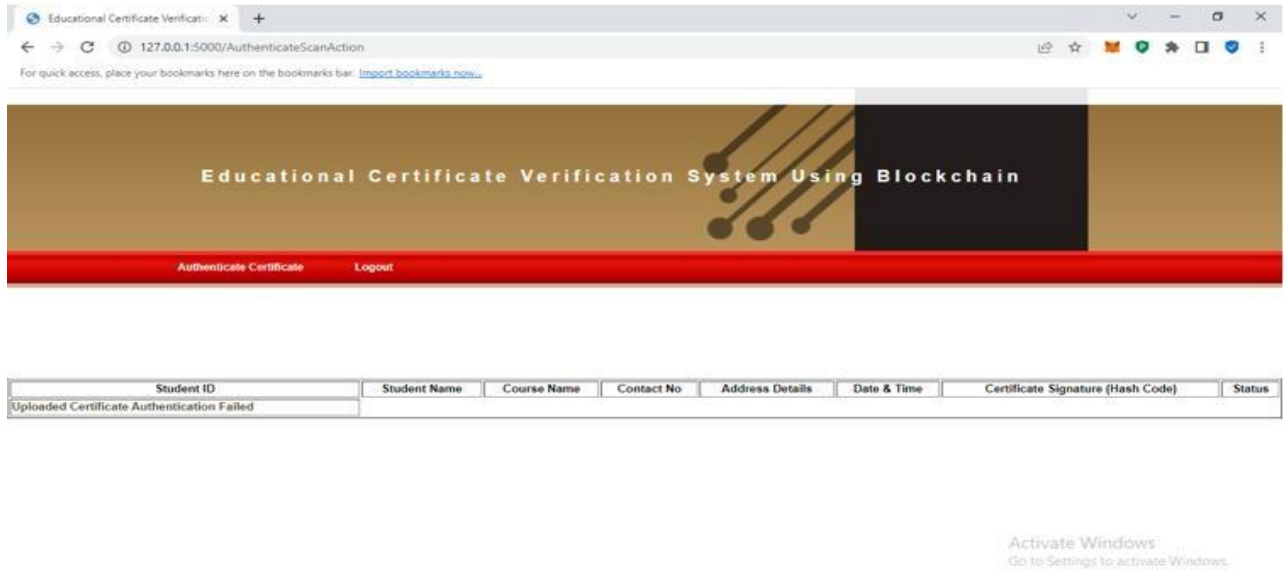


Figure 5.15. Company Authentication Failed

In below screen click on 'Start Webcam' button to start camera and get below output



Figure 5.16. Webcam Home Page

In below webcam from mobile they need to scan QR CODE like below screen

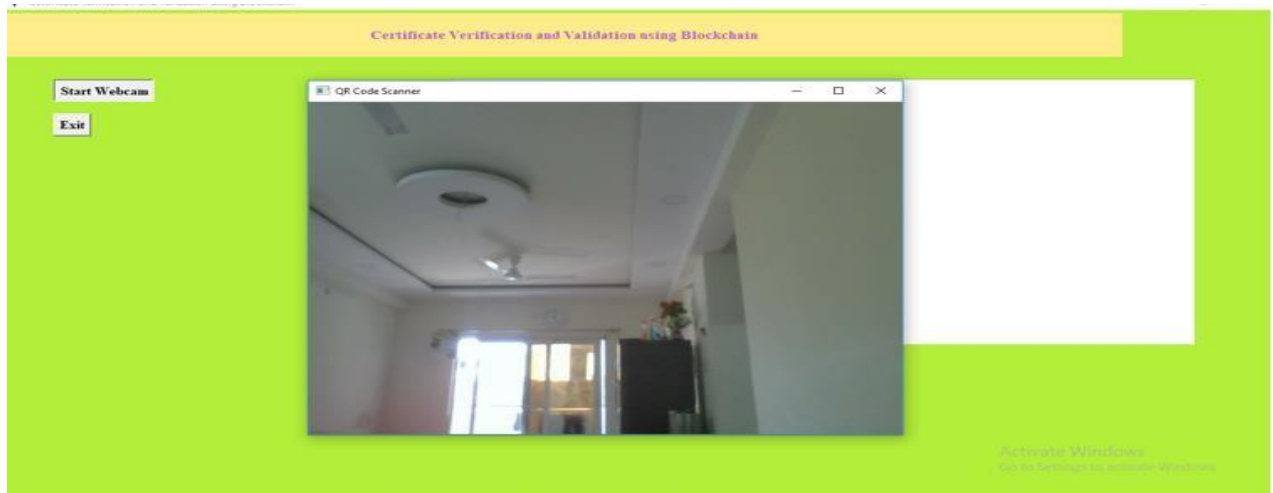


Figure 5.17. Start Webcam

In below screen once we show QR code then all details for that QR code certificate will be retrieve from Blockchain and display in above TEXT area. Similarly, if we scan wrong CODE then will get below output.



Figure 5.18. Certificate Validation Successfull

In below screen we got message as Certificate validation failed as QR code does not exists

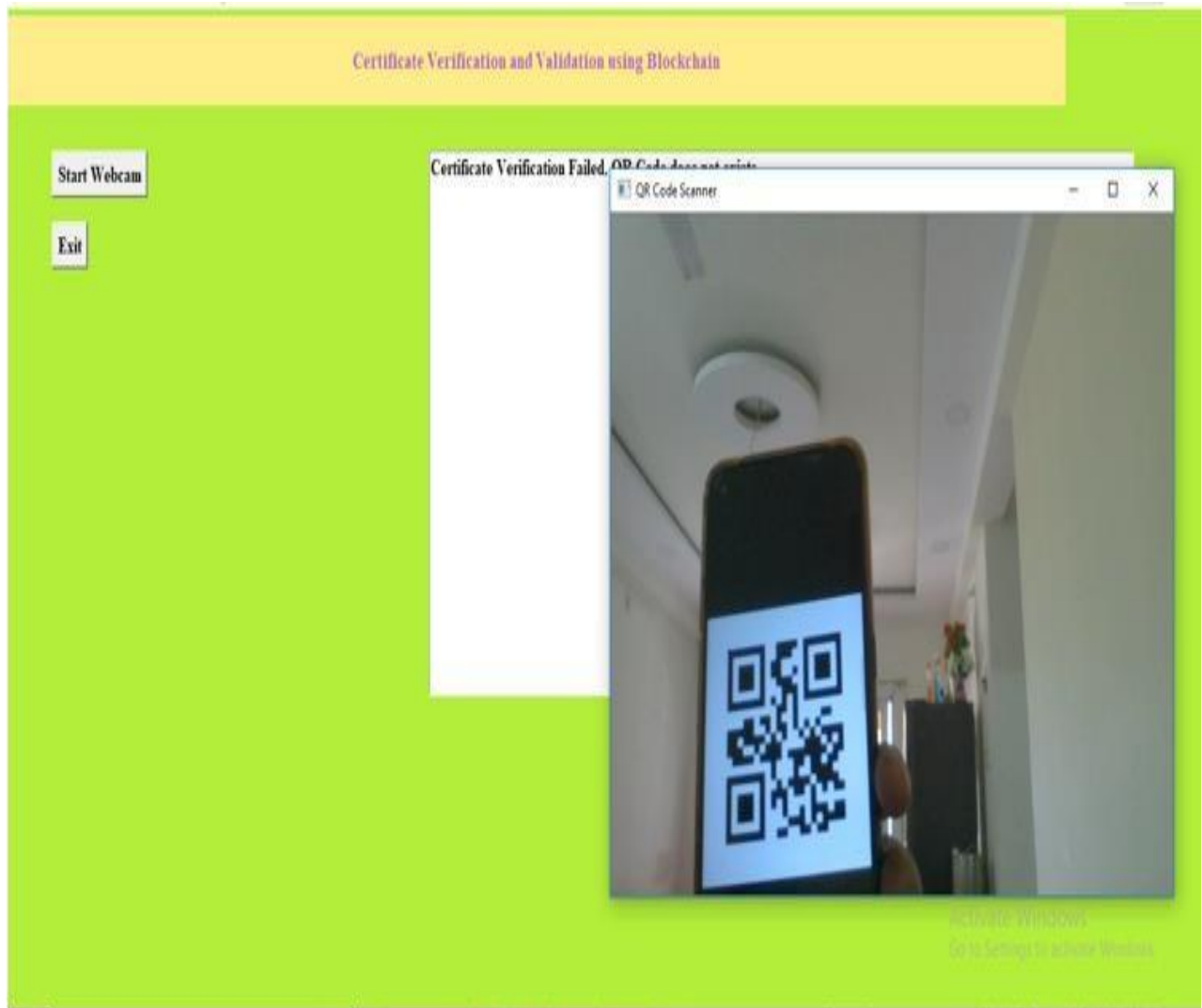


Figure 5.19. Certificate Validation Failed

RESULT ANALYSIS




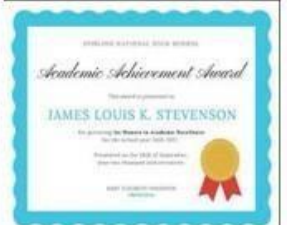


The result analysis for the provided educational certificate verification project involves a thorough evaluation of its key components. Security and tamper-resistance are critical factors, examining the blockchain's efficacy in safeguarding certificate data. User authentication mechanisms and smart contract functionalities are scrutinized for accuracy

and reliability. The success of QR code authentication, ensuring a secure link between codes and certificate details, is pivotal. User experience, including the clarity of instructions and ease of navigation, is assessed. Performance testing gauges system efficiency and scalability under varying loads. Addressing any security vulnerabilities, incorporating user feedback, and refining areas for improvement contribute to an iterative process

aimed at enhancing the overall functionality and user satisfaction of the educational certificate

verification system.

TESTCASE AND SCENARIOS

Test case Scenarios	Expected Output	Actual Output	Status
			PASSED
			PASSED

6.1. Testcase Scenarios

VALIDATION

validation processes are likely embedded within the Flask routes and functions to ensure that userinputs, interactions, and data manipulations adhere to predefined criteria and requirements.

Form Validation

In web applications, user inputs from HTML forms are a common source of data. FlaskWTF orFlask-

Forms extensions can be used to define forms and apply validation rules.

Validators can be applied to form fields to check for data types, required fields, length constraints, and more.**CONCLUSION**

Various technologies have been discussed to reduce the incidence of certificate forgeries and ensurethat the security, validity and confidentiality of graduation certificates, even though there are many

limitations regarding the security and privacy of data. A new blockchain-based system reduces the certificate forgery. Automated certificate granting is open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In the proposed system, we save the cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

FUTURE ENHANCEMENT

To enhance the provided Flask application, consider implementing user roles and permissions for better access control, ensuring that administrators and regular users have appropriate privileges. Improve user authentication by adopting secure practices like password hashing and integrating third-party authentication providers for added security. Extend user profiles to allow users to manage their information and passwords. Implement a certificate revocation system for scenarios where certificates need to be invalidated. Enhance the frontend with modern design principles and responsive layouts using frameworks like React or Vue.js. Introduce comprehensive logging and monitoring to track important events and detect unauthorized activities. Consider exposing API endpoints for external integrations, plan for smart contract upgrades, and conduct regular security audits to address potential vulnerabilities. Additionally, implement localization and internationalization features for a more inclusive user experience. By incorporating these enhancements, the application can become more secure, user-friendly, and adaptable to evolving requirements and technological advancements.

REFERENCES

- [1] References Liou, E., Kao, C., Chang, C., Lin, Y., & Huang, C. (2018). Internet of underwater things: Challenges and routing protocols. 2018 IEEE International Conference on Applied System Invention (ICASI). <https://doi.org/10.1109/icasi.2018.8394494>
- [2] Goyal, V. (2007). Certificate revocation using fine grained certificate space partitioning. *Financial Cryptography and Data Security*, 247259. https://doi.org/10.1007/978-3-54077366-5_24
- [3] Ide, T. (2018). Collaborative anomaly detection on blockchain from noisy sensor data. 2018 IEEE International Conference on Data Mining Workshops (ICDMW). <https://doi.org/10.1109/icdmw.2018.00024>
- [4] Muhamediyeva, D., Khudoyberdiev, A., & Abdurazzokov, J. (2023). Problems of developing a decentralized system based on blockchain technology. *Artificial Intelligence, Blockchain, Computing and Security Volume 1*, 277282. <https://doi.org/10.1201/978100339380-41>
- [5] Santini, P., Gottardi, G., Baldi, M., & Chiaraluce, F. (2019). A data-driven approach to cyber risk assessment. *Security and Communication Networks*, 2019, 18. <https://doi.org/10.1155/2019/6716918>
- [6] Bokariya, P. P., & Motwani, D. (2021). Decentralization of credential verification system using blockchain. *International Journal of Innovative Technology and Exploring Engineering*, 10(11), 11317. <https://doi.org/10.35940/ijitee.k9514.09101121>

[7] K*, M., SafaM., G., G., G, S., & Kanchana J, S.(2020). Music genre classification using lyric mining based onTF-IDF. International Journal of Recent Technology and Engineering (IJRTE), 8(5), 3640. <https://doi.org/10.35940/ijrte.e5011.018520>

[8] References Yaacob, C. M., Abdullah, K., & Omar Fauzee, M. S. (2019). Pengaruh Kefahaman Dan Penerimaan Rakyat Malaysia Terhadap Perjuangan Ideologi DAESH. *Kajian Malaysia*, 37(2),121 45. <https://doi.org/10.21315/km2019.37.2.6>

[9] References Thua Huynh, T., & Khoa Pham, D. (2019). Eunicert: Ethereum based digital certificate verification system. *International Journal of Network Security & Its Applications*, 11(5),15 26. <https://doi.org/10.5121/ijnsa.2019.11.502>

[10] References Digital forensics using blockchain. (2019). *International Journal of Recent Technology and Engineering*, 8(2S11), 182 184. <https://doi.org/10.35940/ijrte.b1030.0982s1119>