



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Block chain Based Certificate Verification System

Sanjay R, Dr. K. Poornapriya, Dr. G. Aarthi, M. Anitha

PG Scholar, Department of Master of Computer Applications, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamil Nadu, India

Principal, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamilnadu, India

Head of the Department, Department of Master of Computer Applications, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamil Nadu, India

Assistant Professor, Department of Master of Computer Applications, Vidyaa Vikas College of Engineering and Technology, Tiruchengode, Tamil Nadu, India

ABSTRACT - Certificates are essential for validating achievements, qualifications, and personal information, acting as gateways to various opportunities such as higher education, career advancement, and promotions. However, the traditional methods of certificate issuance and verification are increasingly vulnerable to fraud and manipulation. Legacy systems are often inefficient, costly, and bureaucratic, making it difficult to prevent certain types of credential fraud. This leads to delays in the verification process, as documents are transferred between institutions and employers, who must spend considerable time ensuring authenticity. Given these challenges, there is an urgent need to modernize the certification and verification process. This project seeks to address these challenges by developing a secure and efficient system for digital credential management, utilizing Blockchain Technology and Capsule Siamese Networks. Certificates are stored with pre-hashes on the blockchain, ensuring their integrity. The certificate holder generates a one-time symmetric encryption key for secure transmission to the verifier.

I. INTRODUCTION

Education verifications are a valuable tool in pre-employment background checks, since they confirm whether or not a candidate has earned the diploma or degree claimed, hence highlighting a candidate's qualifications and possibly revealing information about your candidate's honesty and integrity. An Education Verification search confirms the education, degree, training, or certification claims of a candidate are true and identifies potential discrepancies before you hire. Sometimes referred to as an Education Background Check or an Education Check, this service is used to confirm educational experience at high schools, universities, colleges. To prevent tampering or reproduction by copier machines, most of the genuine educational institutions will have some physical authentication features such as micro-text lines, UV invisible ink, watermark, security hologram, anti-scanning ink, etc. Most probably, fake degree certificate sellers may not put a fake watermark on their fake degrees to give them a real look.

The security hologram, Anti-Scanning Ink, and void features provide an additional feature of anti-scanning and prevent these from making a colour replica. If scanned or photocopied, the matter/design would be far different than the original colour. In case of a void feature, the word COPY appears when an attempt is made to copy a degree. This feature will not be seen in the original document. However, if photocopied, the feature appears on duplicate copy.

II. LITERATURE SURVEY

One of the key responsibilities of the Public Key Infrastructure (PKI) is revocation management. Additionally, the security of any Public Key Infrastructure (PKI) depends on it. Today's revocation methods are susceptible to a single point of failure when network traffic rises due to the growth in the quantity and size of networks as well as the adoption



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

of new paradigms like the Internet of Things and the use of the web. The author uses the strength and resiliency of blockchain to overcome these issues and present a productive decentralized certificate revocation management and status verification system.

The author adds a field that specifies which distribution point the certificate will belong to in the event that it is revoked using the certificate structure extension field. Then, the author carries out a thorough assessment of our plan using performance indicators like execution time and data consumption to show that it can fulfill the demands with high effectiveness and little expense.

Additionally, the author contrasts the effectiveness of our strategy with two of the most widely-used revocation approaches, namely the Certificate Revocation List and the Online Certificate Status Protocol. The data collected demonstrate that our suggested strategy works better than the existing scheme.

III. PROPOSED SYSTEM

Blockchain as a database:

The database (blockchain) does not store any personal data; it only stores public keys, hashes and references to public institutions such as schools and universities. Because it operates multiple nodes, it is fail-safe and can withstand attacks.

Web client for creating certificates

Certificates are generated via a web service that can either run in the browser in the issuing

institution or be integrated into an existing system via an interface. If required, the web service can be integrated into a client program.

Web service for checking certificates

A publicly accessible web service shall be provided to verify the authenticity and integrity of certificate files. This web service can be used by anyone who has a certificate file, that is, by the certificate holder themselves and all third persons and institutions to whom the certificate holder submits their digital certificate file...

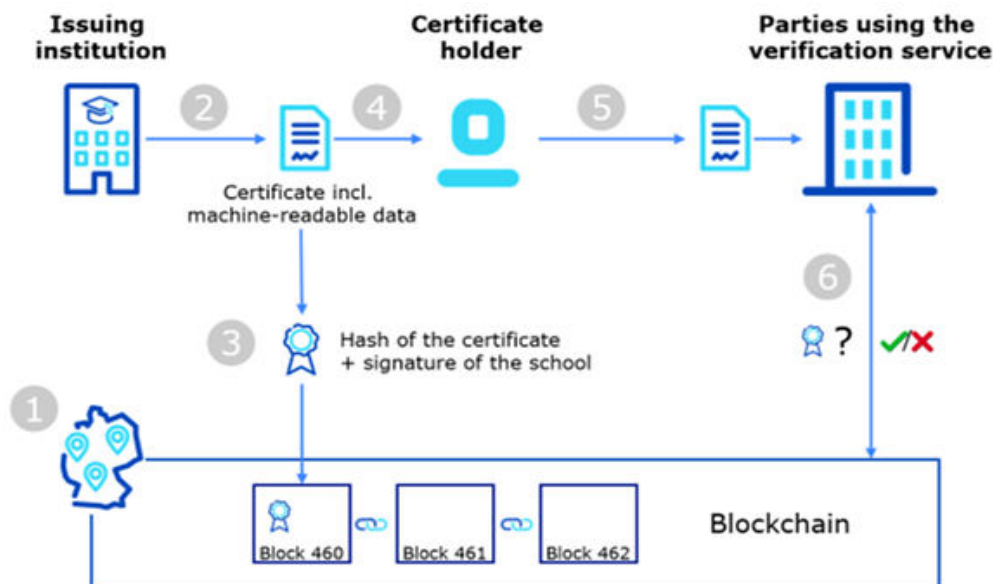
ADVANTAGES

- Automate and ensure compliance for the verification process
- Reduce stress on staff for compliance issues
- Verification review and approval, comment codes and professional judgements
- simplifies and manages workflows
- Faster and efficient certificate verifications to your students.
- Paperless transactions.
- Transparent and can be accessed from anywhere in the world.
- High degree of data privacy.
- Considerable saving on account of courier time, use of paper, defined search parameters.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



IV. MODULES

Certificate Locker Web App :

This secure platform allows users to upload, manage, and share digital certificates. This module comprises a set of integrated modules designed to offer a secure and streamlined experience for users in managing their digital credentials.

BlockChain Integration :

The Blockchain Integration module is designed to ensure the security, transparency, and integrity of digital certificates. This module integrates blockchain technology.

Certificate Fraud Detection :

The Certificate Fraud Detection Modules leverage state-of-the-art Capsule-Siamese Networks, a cutting-edge deep learning architecture meticulously designed to enhance fraud detection efficiency.

Certificate Secure Transmission :

The Certificate Secure Transmission module in the Certificate Locker Web App ensures the secure exchange of certificate data between users or verifiers and the system.

User Interface:

The User Interface outlines the interactions and functionalities for Certificate Issuers, Certificate Holders, and Certificate Verifiers within the proposed system.

Two Way Communication :

The Two Way Communication module used to manage interactions among users, ensuring efficient communication, and providing timely responses to various system requests.

Certificate Integrity Verification :

Using this module, the Certificate Holders have the ability to personally verify the integrity of their certificates by accessing the blockchain transactions associated with each certificate.

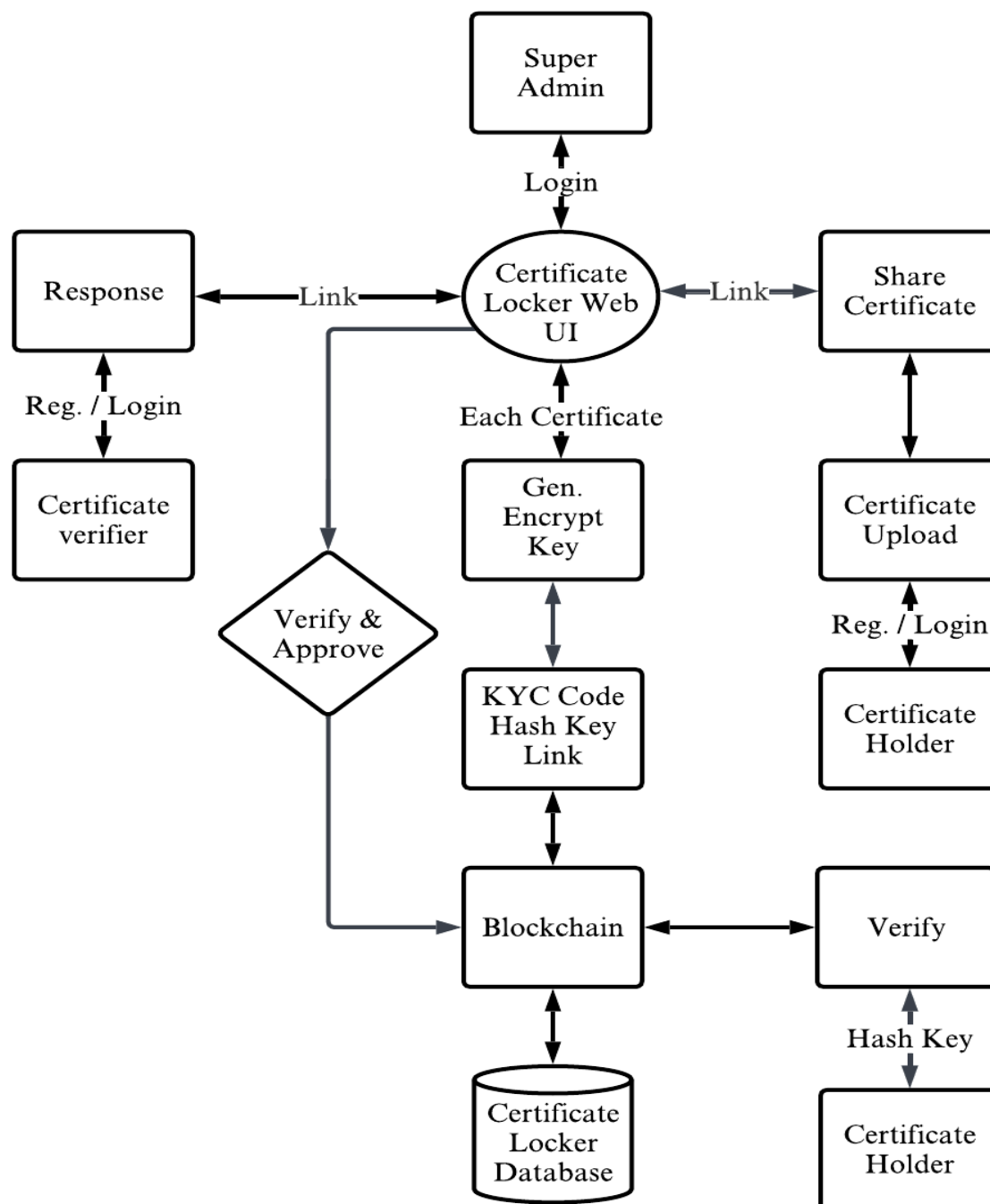
Notification :

The Notification Module ensuring users receive timely alerts and updates. This module delivers real-time notifications through various channels, including email, SMS, and in-app alerts. Users can customize their preferences, acknowledging received alerts for enhanced communication efficiency.



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. EXPERIMENT AND RESULT

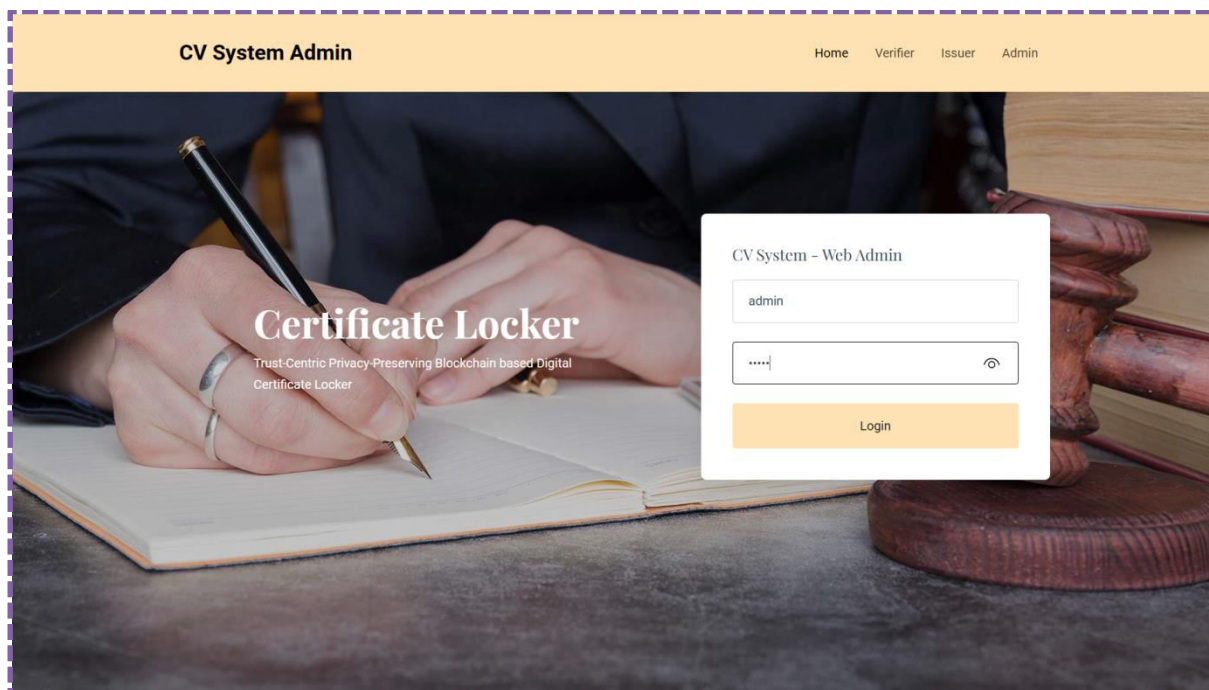


FIGURE 1 : SYSTEM ADMIN

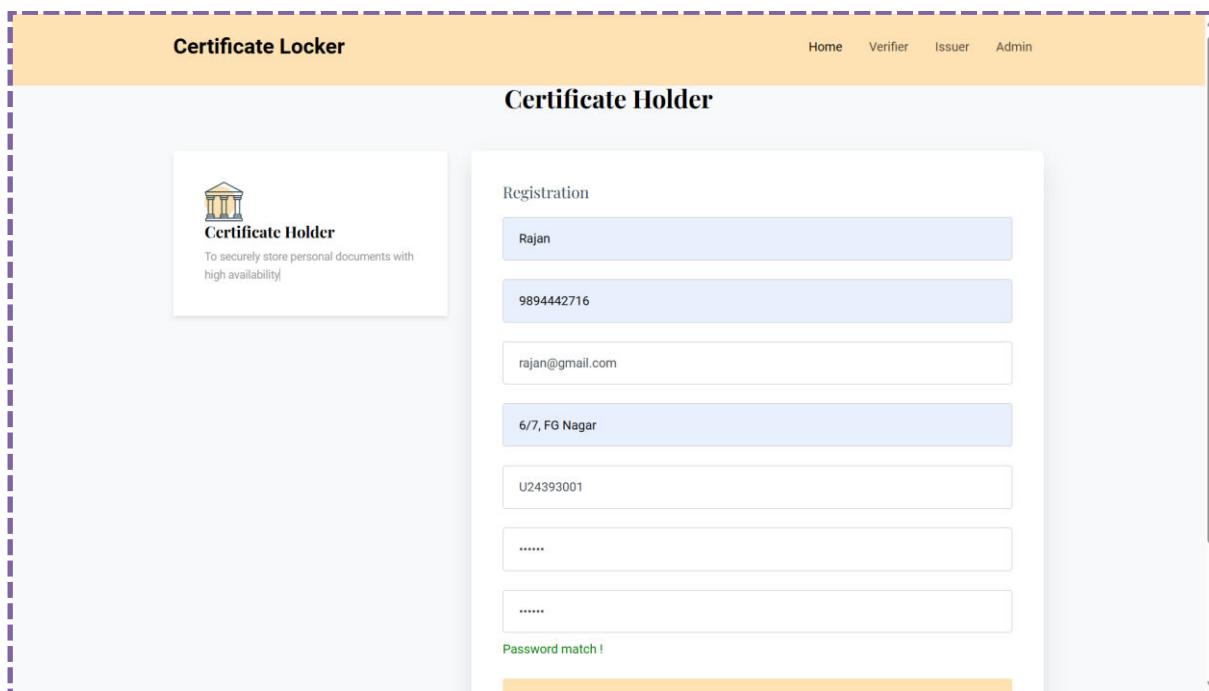


FIGURE 2 : CERTIFICATE HOLDER



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

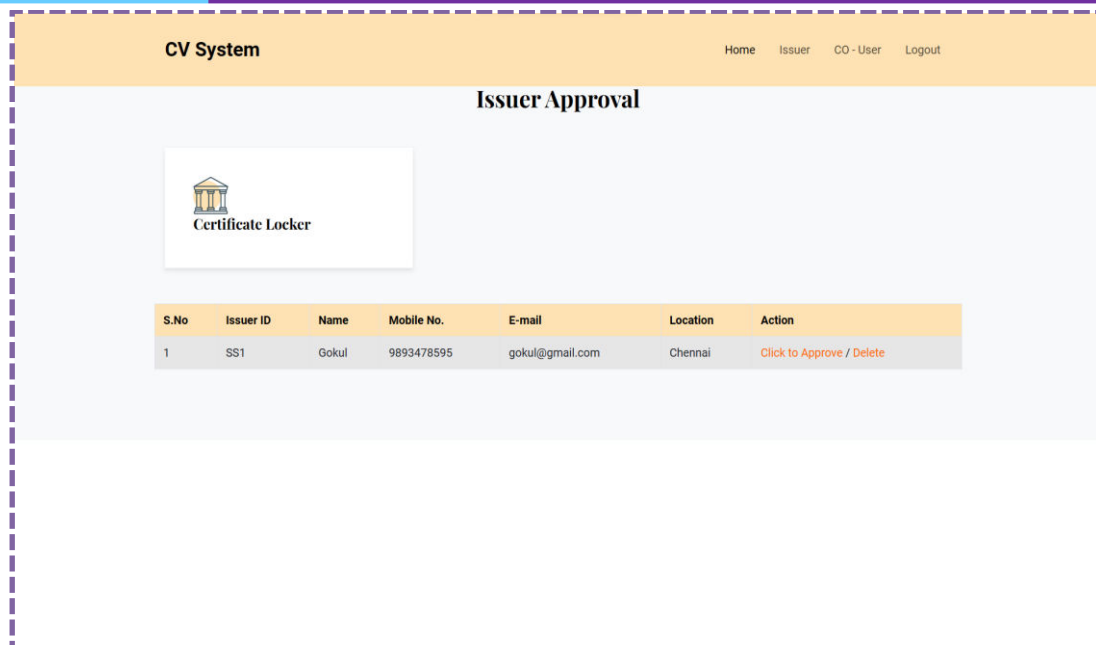


FIGURE 3 : ISSUER APPROVAL

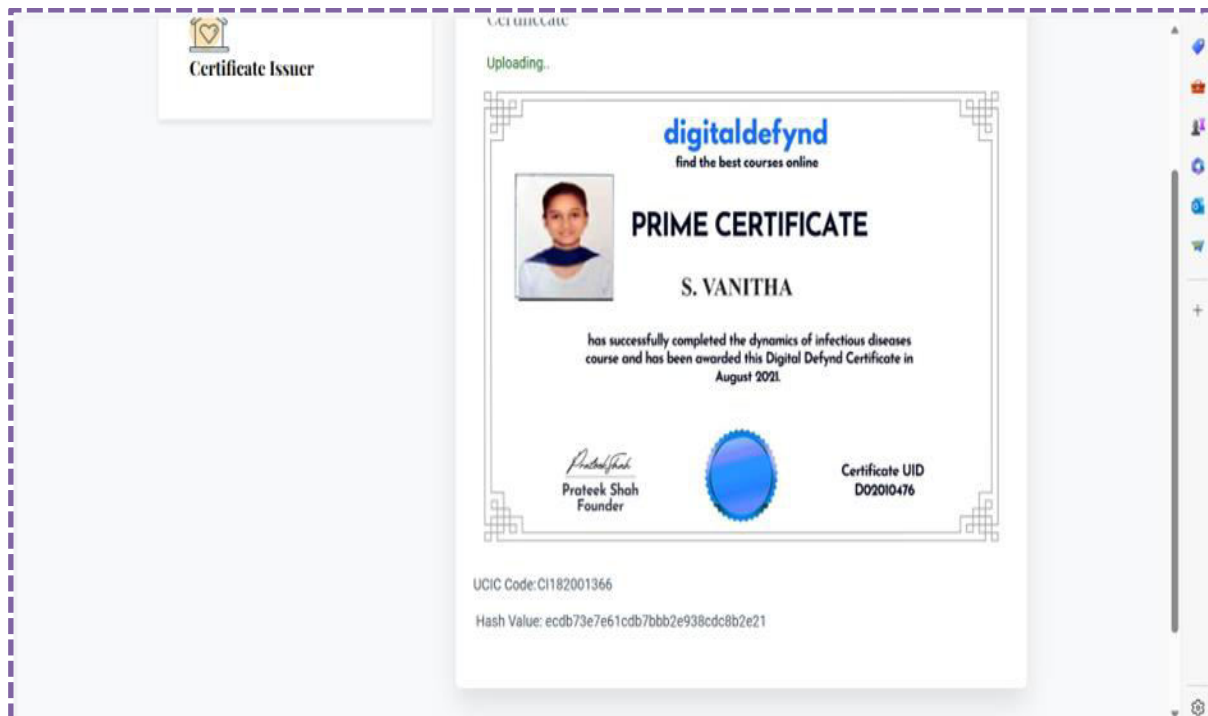


FIGURE 4 : DIGITAL CERTIFICATE



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Certificate Holder
Home Request Verify Identity Logout

Welcome Rajan
Address: 6/7, FG Nagar
Mobile No.: 9894442716
E-mail: rajan@gmail.com

Upload Certificates
UCIC Code

Select Your Certificate
 cr4.jpg
Description

FIGURE 5 : CERTIFICATE UPLOAD

Certificate Verifier
Home Request Logout

Capsule Siamese Network
Tamper Detection and Localization

Original Certificate

Uploaded Certificate

Text Extraction
oho
a]
cm

Face Not Matched!
Text Extraction
digitaldefynd

FIGURE 6 : CERTIFICATE VERIFIER



International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Certificate Holder Home Verify Identity Logout

Block Verify for Integrity

UCIC Code

Ci605001737

Submit

FIGURE 7 : BLOCK VERIFICATION

Certificate Owner Home Verify Identity Logout

Certificate

digitaldefynd
PRIME CERTIFICATE
S. VANITHA
This certificate is issued for the purpose of educational purposes. It is not a legal document and has no legal value. It is a digital certificate issued on 09-03-2024.

Block Information

Block ID	: 1
Data	: 0ade88d9d43fe79f019c5cddb26e014e
Date/Time	: 09-03-2024,20:36:07
Block ID	: 2
Data	: 1d9a56d27575164e0ca50d59f698a5a
Date/Time	: 09-03-2024,20:43:05
Block ID	: 3
Data	: eb58b996d892693e52b6e37f44ff71cd
Date/Time	: 09-03-2024,20:51:27
Block ID	: 4
Data	: afa5ad74558df6e307ec004fe4ab74
Date/Time	: 09-03-2024,20:55:43
Block ID	: 5
Data	: eb58b996d892693e52b6e37f44ff71cd
Date/Time	: 09-03-2024,20:56:38

Traciability

FIGURE 8 : CERTIFICATE INFORMATION

VI.CONCLUSION

In conclusion, the project represents a significant advancement in digital credential management, leveraging modern technologies to enhance security, efficiency, and accessibility. The project has addressed critical challenges associated with traditional certificate issuance and verification methods, such as time-consuming processes, susceptibility to fraud, and lack of transparency. By implementing blockchain technology, Capsule-Siemese Networks, and one-time symmetric key encryption, the system ensures the integrity and authenticity of digital certificates while streamlining the verification process for users and verifiers. The successful development and deployment of the system signify a significant milestone in digital credential management, offering a secure and efficient solution for individuals, educational institutions, and employers.

REFERENCES

- [1] A Alammery, S Alhazmi, M Almasri and S. Gillani, "Blockchain-Based Applications in Education: A Systematic Review", Applied Sciences, vol. 9, no. 12, pp. 2400, 2019, [online] Available: <https://doi.org/10.3390/app9122400>.
- [2] Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE.
- [3] Emanuel Estrela Bessa and Joberto Martins, "A Blockchain-based Educational Record Repository", 2019 CoRR abs 1904.00315.
- [4] A. Alkouz, A. HaiYasien, A. Alarabeyyat, K. Samara and M. Al-Saleh, "EPPR: Using Blockchain For Sharing Educational Records" in 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, pp. 234-239, 2019.
- [5] T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCertBlockChain Imperative for Educational Certificates", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 629-633, 2019.
- [6] Yaoqing Liu, Guchuan Sun and Stephanie. Schuckers, "Enabling Secure and Privacy-Preserving Identity Management via Smart Contract", pp. 1-8, 2019.



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