WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Blockchain Framework for Educational Certificate Verification

Mrs. Y. Suguna[1], V. Tanuja[2], Lalitha Priya Krishnan[3], G. Vijay Simha[4]

[1] suguna.ds@anurag.edu.inAnurag University,Hyderabad
[2] 20eg110129@anurag.edu.inAnurag University Hyderabad
[3] 20eg110115@anurag.edu.inAnurag University Hyderabad
[4] 20eg110108@anurag.edu.inAnurag University Hyderabad

ABSTRACT :

Document verification is a complex domain that involves various challenging and tedious processes to authenticate. Moreover, various types of documents for instance banking documents, government documents, transaction documents, educational certificates etc. might involve customized verification and authentication practices. The content for each type varies significantly, hence requires to be dealt in a distinct manner. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillfully generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, credibility of both the document holder and the issuing authority is jeopardized. Blockchain technology has recently emerged as a potential mean for authenticating the document verification process and a significant tool to combat document fraud and misuse. This research aimed to enhance the document verification process using blockchain technology.

Keywords— Blockchain, Document Verification, Educational Certificates, Authentication, Authorization, Confidentiality.

Introduction :

In the digital era, verifying the authenticity of documents, particularly educational certificates, is critical yet challenging due to the prevalence of fraud. Blockchain technology presents a decentralized and tamper-proof solution, offering transparent and immutable record-keeping. By adopting blockchain for document verification, we can bolster the reliability and credibility of
academic credentials while mitigating the risks of forgery and manipulation. Blockchain technology presents a beacon of hope in addressing the shortcomings of traditional verification processes. Its decentralized architecture ensures that no single entity controls the verification process, mitigating the risk of tampering or manipulation. Additionally, the immutable nature of blockchain guarantees the permanence and integrity of recorded data, instilling confidence in the authenticity of verified certificates.

Literature Review :

In the context of literature on educational certificate verification encompasses various studies and approaches aimed at understanding and addressing the challenges posed by certificate forgery and manipulation.

[1] Blockchain for Digital Certificates: Proposes a blockchain-based system to issue digital certificates securely. Certificates are stored as hash values on the blockchain, enhancing authenticity and reducing forgery risks. QR codes and inquiry strings allow easy verification via mobile or web, leveraging blockchain's immutability.

[2] Certificate Transparency and Revocation Transparency: Introduces blockchain-based Certificate Transparency (CT) and Revocation Transparency (RT) to enhance security in SSL/TLS. Web servers publish their CA-signed certificates and revocation status on a public certificate blockchain, allowing browsers to verify certificate validity independently.

[3] Certificate Transparency Using Blockchain (CTB): Builds upon Google's Certificate Transparency project with blockchain, ensuring domains' consent for certificate issuance. Implements CTB on Hyperledger Fabric, enhancing CA accountability and certificate validation through public logs.

[4] Decentralized Digital Certificate Revocation System: Addresses shortcomings in traditional certificate revocation systems using consortium blockchain. Enables collaborative management of Certificate Revocation Lists (CRLs) by multiple CAs, ensuring reliability and trustworthiness through decentralized consensus and secret sharing schemes.

[5] Certificate Verification System using Blockchain: Focuses on combating counterfeit certificates through blockchain's tamperproof and non-repudiation features. Proposes a model for issuing and verifying certificates securely, aiming to prevent misuse and enhance trust in credential verification processes.

Proposed Method :

A. Blockchain-Based Document Verification Platform:

The system will feature a user-friendly web interface accessible to students, academic institutions, and potential employers.
Students: Can securely access and share their educational certificates on the blockchain.
Academic Institutions: Can issue and authenticate certificates.
Employers/Verification Agencies: Can efficiently verify the authenticity of educational certificates through the blockchain platform, ensuring trust and reliability.

B. Certificate Issuance and Verification:

Academic institutions can securely issue digital certificates onto the blockchain, ensuring their authenticity and immutability.
Employers and verification agencies can easily verify certificates by accessing the blockchain ledger, eliminating the need for manual verification processes.
Smart contracts will automate certificate issuance and verification, ensuring transparency and efficiency in the process.

C.QR Code Generation and Authentication System:

Upon authentication request, the system will generate unique QR codes for students, facilitating secure access to their verified educational certificates. Automated notifications will be sent to students upon QR code generation, ensuring seamless and efficient verification processes.

D. QR Code Matching and Certificate Details Display:

The system will employ QR code matching techniques to authenticate student certificates. Upon verification, the platform will display details of the uploaded certificate in a secure web interface, ensuring transparency and reliability in the verification process. Advance algorithms power the QR code matching mechanism, guaranteeing secure and efficient verification operations. This system enhances accessibility, allowing users to verify certificates from any location with internet access. Additionally, continuous monitoring of verification activities enables administrators to promptly address any irregularities or security concerns, upholding the system's integrity.

E. Blockchain Security Measures:

The platform will implement robust security protocols leveraging blockchain technology to safeguard sensitive certificate data. Encryption techniques will be applied to ensure secure transmission and storage, while regular security audits and updates will be conducted to address potential vulnerabilities and uphold the integrity of the system.

F. Blockchain Integration, Scalability, and Continuous Monitoring:

The system prioritizes scalability to accommodate varying user demands and seamlessly integrates with existing educational management systems for efficient data flow. Continuous monitoring mechanisms ensure system reliability and security, enhancing the effectiveness of document verification processes.

G. Integrative Development and Feedback-driven Enhancements:

The system adopts an iterative development approach to enhance authentication success through improvements in digital signature evaluation and verification system development. User feedback is central to driving enhancements, the system evolves to meet evolving verification standards.

IV. Implementation

Nowadays all peoples are opted for education to get good job and they are generating fake certificates to achieve their goals and existing technologies has no support to verify such certificates. In the implementation we are introducing Blockchain technology which store immutable data and its data cannot by modify in any manner. While giving certificate to student, admin user will store certificate copy in Blockchain and obtained its digital signature and then generate QR code on that signature and affix that code on student certificate. This certificate can be scanned by other companies or institution to verify and extract details from Blockchain. If QRCODE exists in Blockchain then certificate validation will be successful.

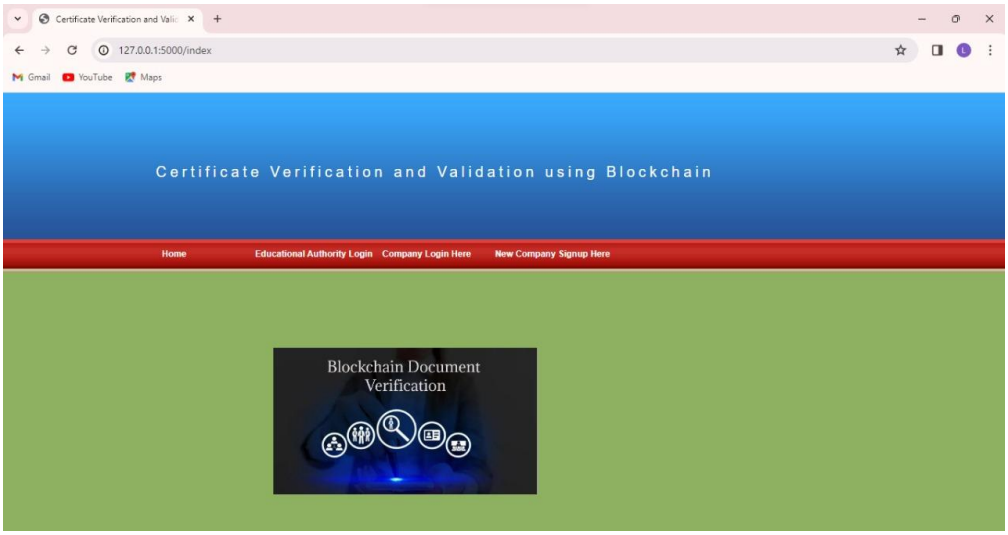

Figure: 1 HOME PAGE

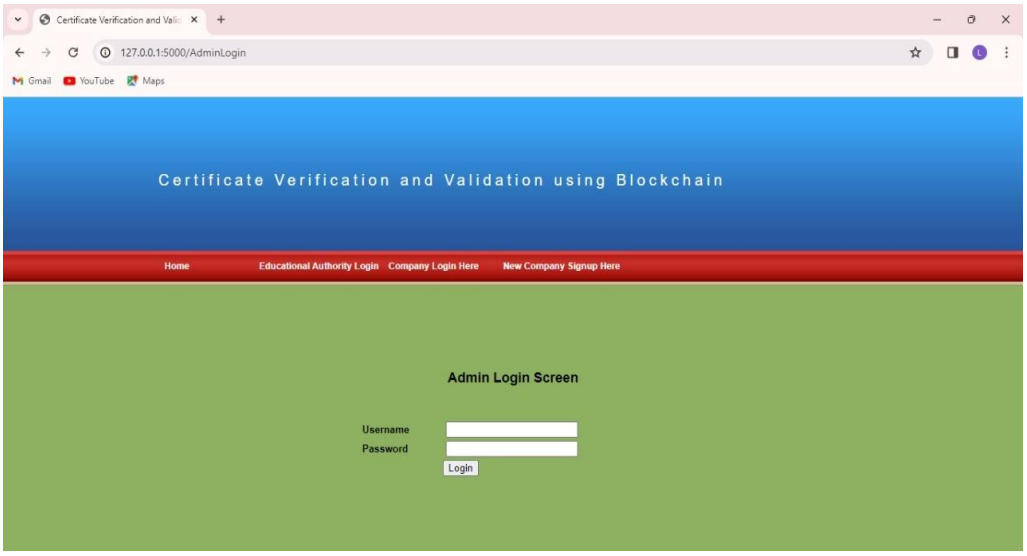

Figure:2 ADMIN LOGIN SCREEN

In the above screen admin can click on 'Upload New Certificate' link to upload certificates.

Figure: 3 CERTIFICATE UPLOAD PAGE

In the above screen, the admin can upload student details and certificates. Then the following screen appears.

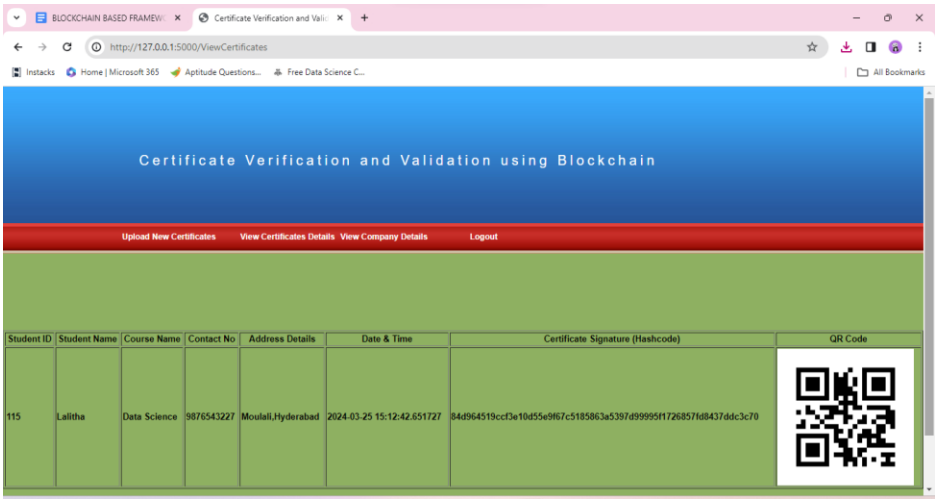

Figure 4: STUDENT CERTIFICATE DETAILS

In the above screen, a unique QR code will be generated for the submitted certificates.

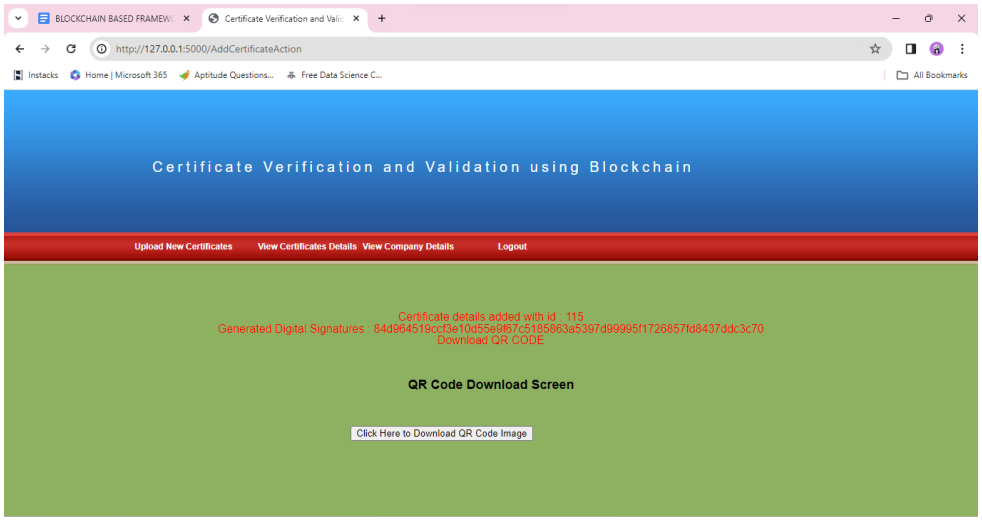

Figure:5 QR DOWNLOAD SCREEN

In the above screen, student details have been added, and a digital signature has been generated and stored in the Blockchain. And QR code can be downloaded.

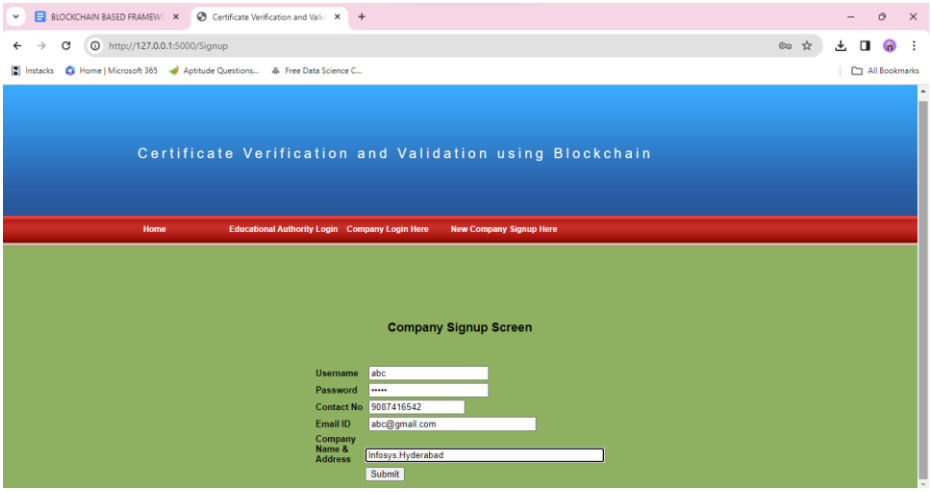

Figure:5 COMPANY SIGN-UP SCREEN

In the above screen, companies can enter signup details, which are then stored in the blockchain.

Figure:6 CERTIFICATE QR SCANNER

The above screen is used by the company for scanning the QR of the certificates submitted by the candidate.

Figure:7 QR SCANNER CAMERA

The above screen represents the webcam that is being initialized for scanning the QR.

Figure:8 MISMATCHED QR

The above screen represents the QR that is being scanned by the company. Here the QR of the certificate that is uploaded by the educational authority and the QR of the certificate that the candidate has uploaded in the company profile are not matched, so, the verification has failed.

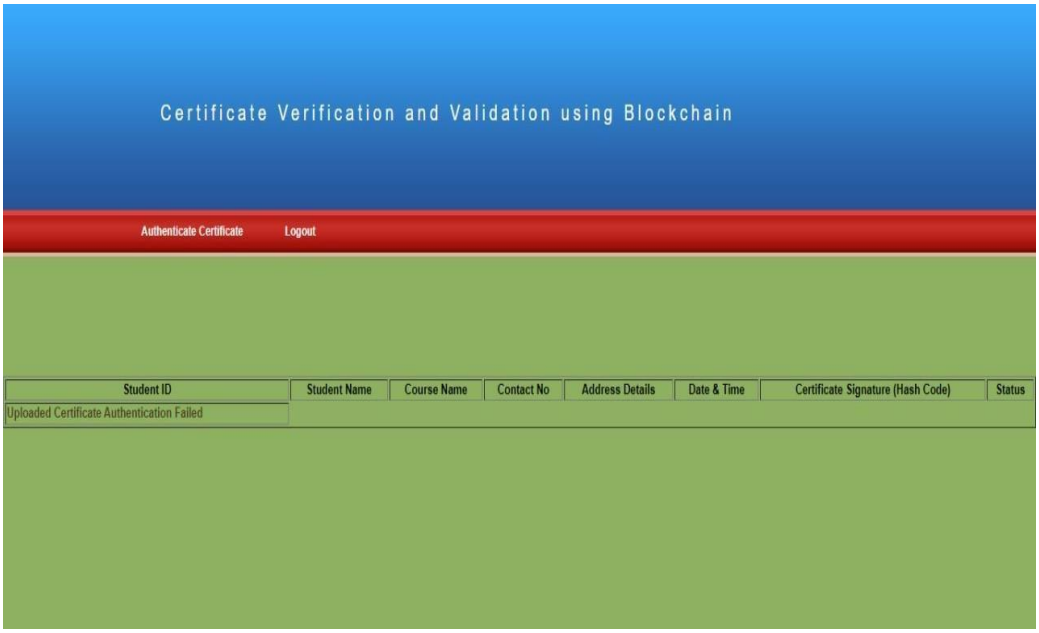

Figure:9 FAILED AUTHENTICATION

Once the company has recognized that the verification has failed, it updates the same in the webpage as shown below. So, now the company will not be proceeding with the respective candidate's profile.

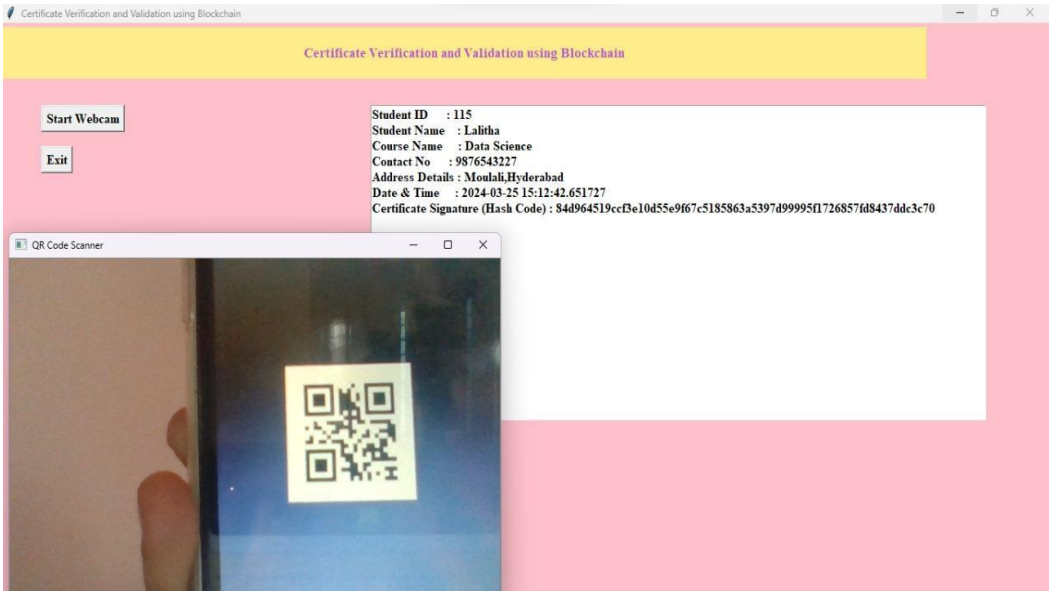

Figure:10 MATCHED QR

In the above screen we can see that the scanned QR has generated the candidates details along with Certificate signature (Hash Code). This indicates that the certificate is not fake and the verification is successful.

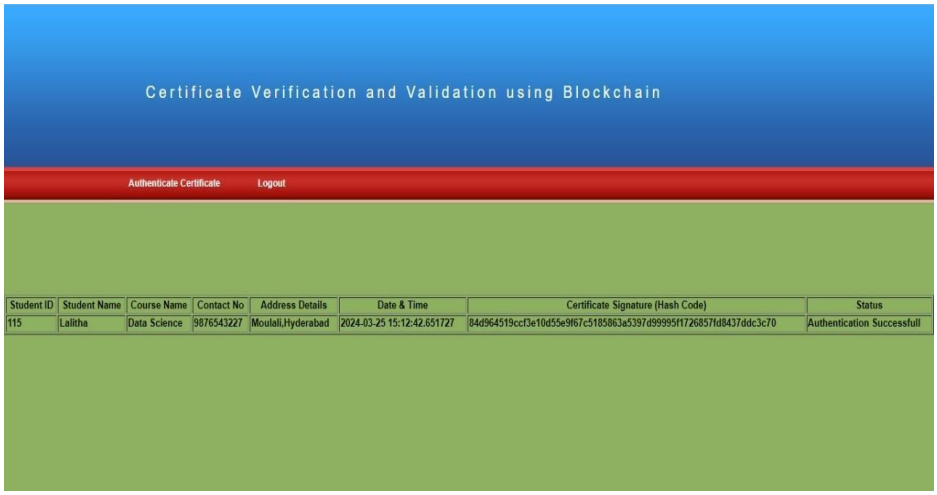

Figure:11 SUCCESSFUL AUTHENTICATION

Once the company has found out that the QR has been scanned successfully, they update in the website about successful authentication and proceed with the candidature of the respective job applicant.

V. Conclusion :

Data security is a paramount feature of blockchain technology, characterized by its decentralized and immutable nature. In a blockchain-based system, each node stores and verifies the same data, ensuring transparency and integrity. By leveraging this technology, the likelihood of certificate forgery is significantly reduced. The process of certificate application and automated granting is transparent, allowing companies and organizations to inquire about any certificate within the system. Ultimately, the system guarantees information accuracy and security, bolstering trust and reliability in certificate verification processes. Furthermore, blockchain technology provides a decentralized consensus mechanism, ensuring that data stored on the ledger cannot be altered without consensus from the network participants. This enhances the security and integrity of the certificate verification process, as it prevents any single entity from maliciously manipulating the data.

VI. Acknowledgment:

We extend our sincere gratitude to our dedicated team members for their invaluable contributions and unwavering commitment to this research endeavor. Their collaborative efforts and hard work have been instrumental in the successful completion of this project. We would like to express our deepest appreciation to our mentors and advisors for their guidance, support, and expertise throughout the research process. Their insightful feedback and encouragement have been crucial in shaping the direction and outcomes of this study. Special thanks are extended to the individuals who generously shared their knowledge, expertise, and time to support this research initiative. Furthermore, we are grateful for the support and resources provided by our institution, which have greatly facilitated the execution of this research. This research represents the culmination of collective efforts and collaboration, and we extend our heartfelt appreciation to all who have contributed to its realization. Finally, we are grateful for the support and resources provided by Anurag University, which made this project possible.

VII.REFERENCES :

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," IEEE International Conference on Applied System Invention (ICASI), 2018.

[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[4] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain,"

[5] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[6] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, "Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.

[7] S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology-SRM Institute of Science and Technology.

[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.

[9] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/ 10.1109/ATC.2018.8587428.

[10] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).

[11] Song, L., Wang, B., Zhang, X., & Wang, H. (2018). Research on Blockchain Technology in Electronic Certificate. In 2018 7th International Conference on Computer Sciences and Automation Engineering (ICCSAE) (pp. 740-744). IEEE.

[12] Atakan, M. H., Gencer, E. A., & Baser, S. E. (2019). A Blockchain-Based Approach for Digital Certificates: A Case Study. In 2019 5th International Conference on Computer and Technology Applications (ICCTA) (pp. 180-183). IEEE.

[13] Nguyen, T. Q., Dang, L. H., & Nguyen, D. C. (2020). A secure e-Certificate verification system using blockchain and deep learning techniques. In 2020 IEEE 4th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (pp. 1-6). IEEE.

[14] Roy, M., & Hemalatha, R. (2021). Secure Digital Certificate Management System Using Blockchain Technology. In Proceedings of the International Conference on Inventive Research in Computing Applications (pp. 1-6). Springer, Singapore.

[15] Solanki, A., Desai, K., & Tanna, R. (2020). Secure Certificate Verification Using Blockchain and Smart Contract. In Proceedings of the International Conference on Intelligent Computing and Communication (pp. 713-721). Springer, Singapore.