BLOCKCHAIN-BASED ISSUE & CERTIFICATE VERIFICATION SYSTEM

Submitted in Partial Fulfillment of the Requirements for the Award of Bachelor of Science in Information Communication Technology (ICT)

ALEX GACHUGU KANYI

SC/ICT/1150/21

Laikipia University

School of Science and Applied Technology.

Department of Computing and Informatics.

13th March 2025

DECLARARTION

I declare that this work has not been previously submitted for a degree at this or any other institution. All sources are appropriately acknowledged.

Name: Alex Gachugu Kanyi

Signature…… Date……

This research project proposal was submitted for examination with my approval as the University appointed supervisor.

Name: Dr. Evans Ombati

Signature…….Date…….

RECOMMENDATION

The research proposal entitled **"Blockchain-Based Certificate Issue & Authentication System"** has been presented to the Institute of Undergraduate Studies of Laikipia University. I have reviewed the research proposal and recommend it be accepted in partial fulfillment of the requirements for the award of the Bachelor's degree in Information Communication Technology (ICT).

COPYRIGHT

DEDICATION

I dedicate this project to my family members and friends for their continuous support throughout my academic life and experience. I give thanks to all that have supported me till this far with my writing and completion of this project.

ACKNOWLEGEMENT

Special thanks to Dr. Evans Ombati for guidance, my parents for financial and moral support, and Laikipia University for resources.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The research will follow a descriptive and experimental approach, using Solidity for smart contracts**,** Python and Js for the frontend, and Firebase for secure user authentication. The expected outcome is a tamper-proof, scalable, and efficient system that restores trust in certificate verification processes.

This project addresses the inefficiencies and vulnerabilities in traditional certificate verification by proposing a **Blockchain-Based Issue & Certificate Verification System**. Leveraging Ethereum blockchain and IPFS, the system ensures tamper-proof storage and instant verification of academic and professional credentials. Smart contracts automate issuance and validation, while QR codes enable quick authenticity checks. The system enhances transparency, reduces fraud, and streamlines verification processes.

CHAPTER ONE: INTRODUCTION

1.1 Background

This project endeavours to modernize the conventional methods of verifying academic certificates by harnessing the potential of blockchain technology. In today's digital era, the proliferation of counterfeit certificates poses a substantial obstacle for educational institutions, students, and employers. This project addresses this pressing concern by furnishing a secure, transparent, and tamper-proof platform for validating the authenticity of academic credentials. By operating through a decentralized blockchain network, the system ensures that verified student details are securely stored.

Each certificate undergoes encryption and receives a unique identifier before being added to the blockchain. This guarantees the immutability and tamper-resistance of certificate data, thereby serving as a reliable source of truth for all parties involved. One of the standout advantages of this system is its heightened security. Employing blockchain technology ensures that the integrity of certificate data remains intact, significantly mitigating the risk of fraudulent activities. Additionally, the system fosters transparency and traceability, empowering users to effortlessly verify the legitimacy of certificates. Furthermore, the system streamlines the verification process, enhancing efficiency manifold. Through the utilization of QR codes, companies can promptly scan and validate certificates, obviating the necessity for laborious manual verification techniques. This not only saves time but also alleviates administrative burdens and reduces associated costs.

Moreover, the system champions global accessibility, facilitating seamless verification procedures across diverse geographical locations. Whether it pertains to a student exploring job prospects overseas or an employer verifying the credentials of a potential candidate, the system offers a universally accessible platform for certificate validation. In essence, "Blockchain based Certificate Issue & Verification system" proffers a robust remedy to the pervasive issue of counterfeit certificates in the education sector. By amalgamating the security and transparency of blockchain technology with the efficiency of QR code- based verification, the project endeavors to uphold the integrity and credibility of academic credentials for all stakeholders

1.2 Problem Statement

The current system for issuing and verifying certificates suffers from several limitations:

- **Fraud and Forgery**: Fake certificates are prevalent, leading to a loss of trust in educational institutions and professional qualifications.
- **Inefficient Verification**: Manual verification processes require institutions to respond to individual requests, causing delays and increased administrative costs.
- **Corruption**: Manual verification processes vulnerable to manipulation and bribery, blockchain based verification is secure and has an automatic verification process.

This research aims to develop a blockchain-based certificate issue and verification system to solve these issues by removing intermediaries, ensuring security, and enabling instant verification.

1.3 Objectives

1. Develop a blockchain-based system for issuing and verifying certificates.
2. Ensuring unchangeable and authentic certificates by securely storing them on the blockchain.
3. Create a user-friendly web interface for institution and employers/verifiers to interact with the system.
4. Utilize IPFS for decentralized certificate storage.

1.4 Scope of the Project

- Developing a smart contract to issue and verify certificates.
- Creating a web-based frontend for institutions and verifiers.
- Using Ethereum blockchain for storing certificate metadata.
- Add qrcode that will be used and helpful to verify certificates via pdf.
- Integrating IPFS for storing the actual certificate files (e.g., PDFs).

1.5 Research Questions

- How does blockchain technology ensure the immutability and tamper-proof nature of certificates compared to traditional centralized databases?
- How does decentralized storage (e.g., IPFS) improve data retrieval efficiency compared to centralized cloud storage for certificate verification?
- Does blockchain-based verification reduce fraudulent certificates in higher education or corporate sectors?
- How user-friendly are blockchain interfaces for non-technical stakeholders (e.g., employers, students)?

1.6 Significance of study

This research addresses critical gaps in traditional certificate verification systems and introduces transformative benefits through blockchain technology. The key areas where this study adds value include academic contribution, practical benefits, societal impact, technological, innovation, policy and governance.

CHAPTER TWO: LITERATURE REVIEW

Blockchain Technology

There is a recent study focusing on the application of blockchain technology to create certificate transparency mechanisms that constitute a public log for every authority certificated. The major goal behind these transparency measures is to improve the conventional SSL/TLS protocol's X.509 certificate validation processes, thus making it more accountable and trustworthy as far as certificates issuing is concerned.

Advancing Security with Blockchain-based Certificate Transparency:

Blockchain-based certificate transparency solutions enhance security by providing an immutable record of issued certificates and mitigating potential risks associated with the certificate authority system. These systems allow for transparent and decentralized verification of certificates, ensuring the integrity and authenticity of online communications and transactions.

Decentralized Certificate Revocation Systems:

In the traditional setup, digital certificate revocation systems have struggled with operational challenges, mainly due to the lack of mutual trust, access stability, and data synchronization among certification authorities (CAs). A cutting-edge solution to tackle these issues is the utilization of decentralized certificate revocation systems. Leveraging consortium blockchain technology, these systems facilitate collaborative management of digital certificate revocation lists (CRLs) among multiple CAs, ensuring improved reliability, security, and real-time updates in the certificate ecosystem.

Enhancing Trust and Security in Certificate Issuance:

The increasing number of fake certificates has become a significant concern, affecting education, employment, and various other sectors. Implementing blockchain technology for certificate issuance and verification ensures tamper-proof, transparent, and secure processes. By utilizing blockchain's decentralization and encryption features, institutions can streamline certificate management and build a trusted ecosystem for validating credentials.

Blockchain technology offers unprecedented opportunities for enhancing certificate verification and validation processes, revolutionizing traditional approaches to certification management. By leveraging blockchain-based certificate transparency mechanisms and decentralized revocation systems, organizations can ensure the authenticity and integrity of academic credentials, mitigating the risks associated with counterfeit certificates and fraudulent activities. Through continued research and innovation in this field, blockchain-based solutions have the potential to redefine certificate authentication in the digital age, fostering greater trust and confidence in certification processes.

IPFS (InterPlanetary File System)

IPFS (InterPlanetary File System) is a peer-to-peer distributed file system that allows for secure and efficient storage. Instead of storing certificate files on centralized servers, IPFS provides a distributed and encrypted storage system. Certificates stored on IPFS has hashes that are recorded on the blockchain for verification.

CHAPTER THREE: PROPOSED SYSTEM

Methodology

In this proposed system, the academic certificates are generated, send to students via email providing students with certificate id and download link from IPFS cloud storage. The institute logs in and inputs the students details for certificate generation be it single certificate of bulk certificate generation. The consensus algorithm is used for generating the hash values. In the Blockchain, each block consists of hash value, timestamp, previous hash value and they connected together. The user verifies the certificates by using verification page through either uploading certificate in pdf format or using certificate hash-id.

Certificate Verification

1. The retrieved IPFS hash is matched against the stored document hash to ensure authenticity.
2. The system retrieves the metadata from the blockchain.
3. The student share authenticity token and certificate with the employer.

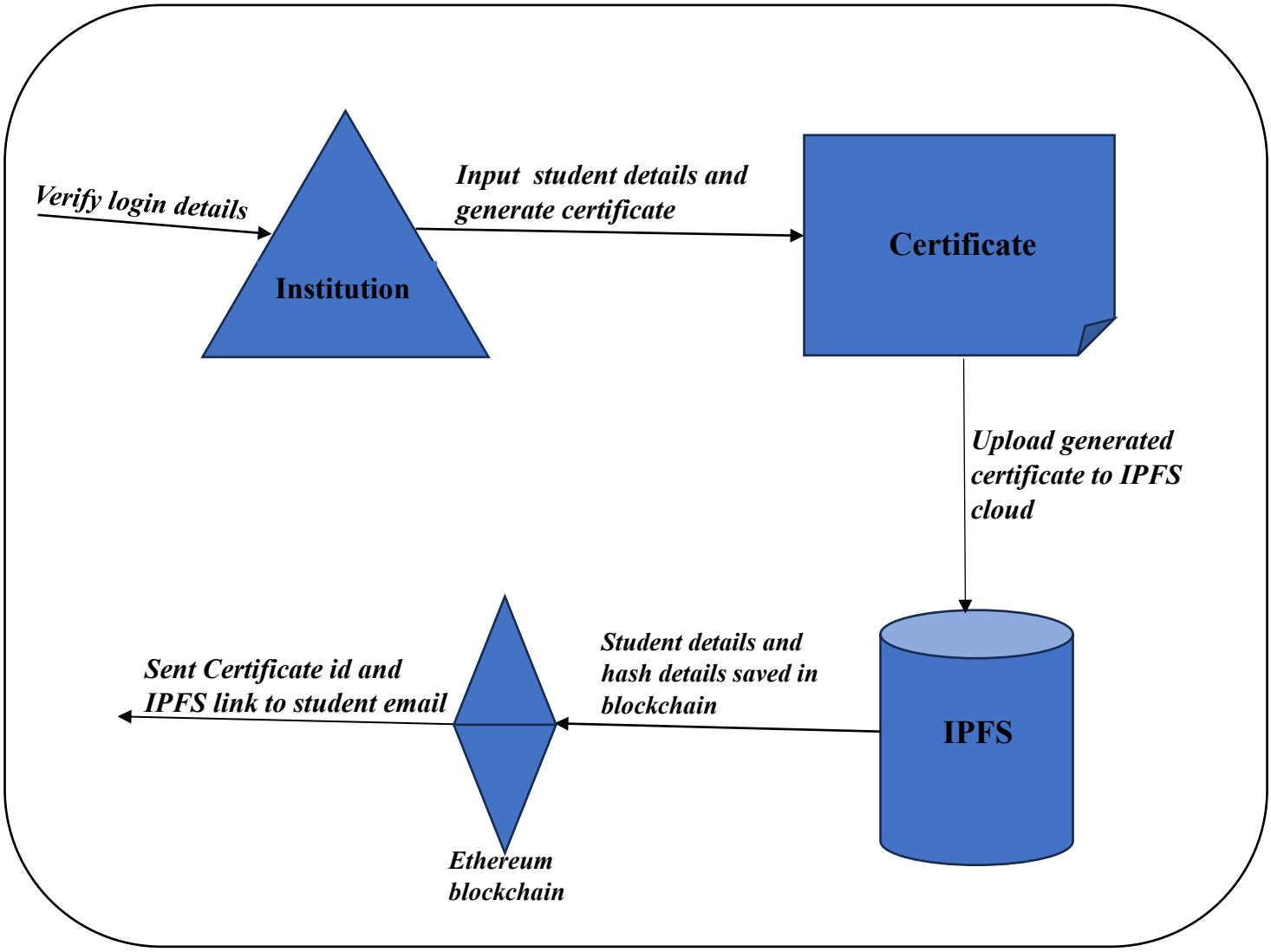


Figure 1: Certificate Generation

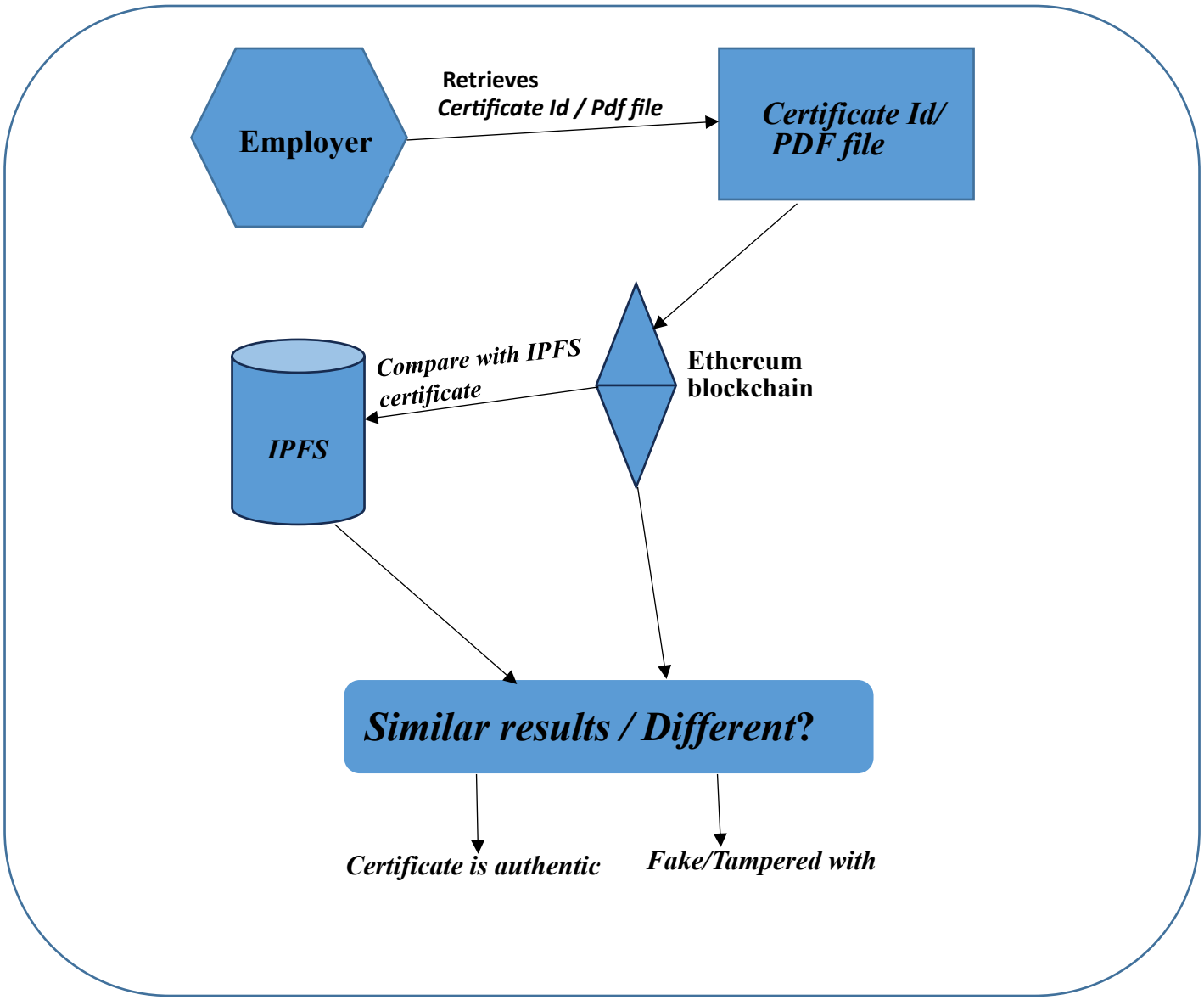


Figure 2: Certificate Verification

- ***Certificate Storage on Blockchain:*** When a certificate is issued to a student, the admin user initiates the process by storing a digital copy of the certificate on the Blockchain. This digital copy undergoes hashing and encryption processes to ensure its integrity and security.
- ***Digital Signature Generation:*** Following the storage of the certificate on the Blockchain, a digital signature is generated for the certificate data. This digital signature acts as a unique identifier and provides assurance of the certificate's authenticity.

- ***QR Code Generation and Affixing:*** Subsequently, a QR code is generated using the digital signature of the certificate. This QR code encapsulates the digital signature and serves as a tangible link to the Blockchain-stored certificate data. The QR code is then affixed to the student's certificate.
- ***Verification Process:*** When external entities, such as companies or institutions, need to verify the certificate, they can easily scan the QR code using a QR code scanner. The scanner decodes the QR code and extracts the embedded digital signature.
- ***Validation from Blockchain:*** The extracted digital signature is then used to query the Blockchain. If the digital signature exists on the Blockchain, it confirms the validity and authenticity of the certificate. The certificate details associated with the digital signature are retrieved from the Blockchain and presented to the verifying party.
- ***Successful Certificate Validation***: If the QR code exists on the Blockchain and the digital signature matches, the certificate validation is deemed successful. The verifying party can confidently trust the authenticity of the certificate, as it has undergone secure storage and validation on the Blockchain
- ***Revoke Certificate process***: Only the Institute that has issued the certificate are the ones to revoke it, if it is revoked by the institute the certificate will no longer be valid when trying to validate it and it will be deemed as fake.

CHAPTER FOUR: RESULTS & DISCUSSIONS

4.1 Institution Login

i. Registration

- To create the block chain based unmodifiable certificates, initially the college needs to get registered.
- After successful login the institution navigates to the add institution page and add the college name.

4.2 Certificate generation

- The institution either uploads the students' details for bulk generation or fill details for single certificate generation.
- For bulk generation, the uploaded document containing student details are processed and certificates are generated systematically.
- Qr-codes are embedded in each certificate that will carry the full details of the students.
- Certificates are uploaded to IPFS for safe keeping and future retaining.

4.3 Student access

- After successful certificate generation the IPFS link to the certificate and the blockchain certificate Id are emailed directly to students email address provided by the student.
- Students download their certificates using the link they have received from the institution by clicking on it.

4.4 Verification

- Access the verification page, it requests for either the pdf format of the certificate or the certificate Id.
- The qr code embedded in the certificate is then used to verify the certificate by calling the certificate id and the ipfs document and comparing it.
- The institution either uploads the students' details for bulk generation or fill details for single certificate generation.

4.5 Revoking Certificate

- The Institute page has an option to revoke certificate by pasting the certificate id.
- Also, an option to revoke all certificate generated is available for easily revoking all generated certificates.

Figure 3: Project Homepage

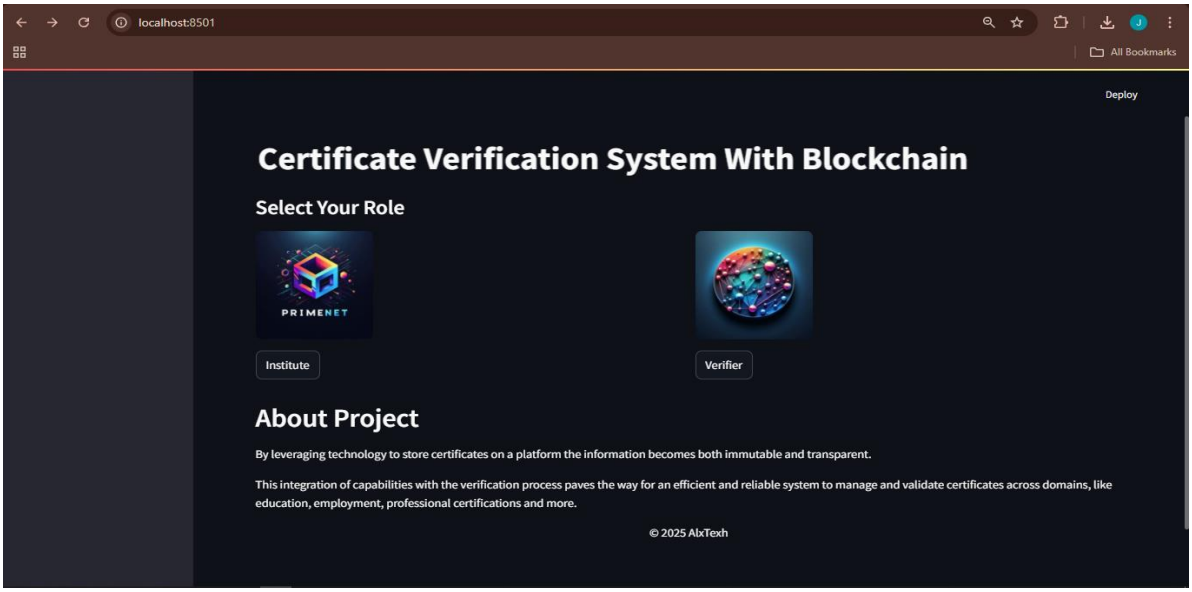


Figure 4: Institute Login page

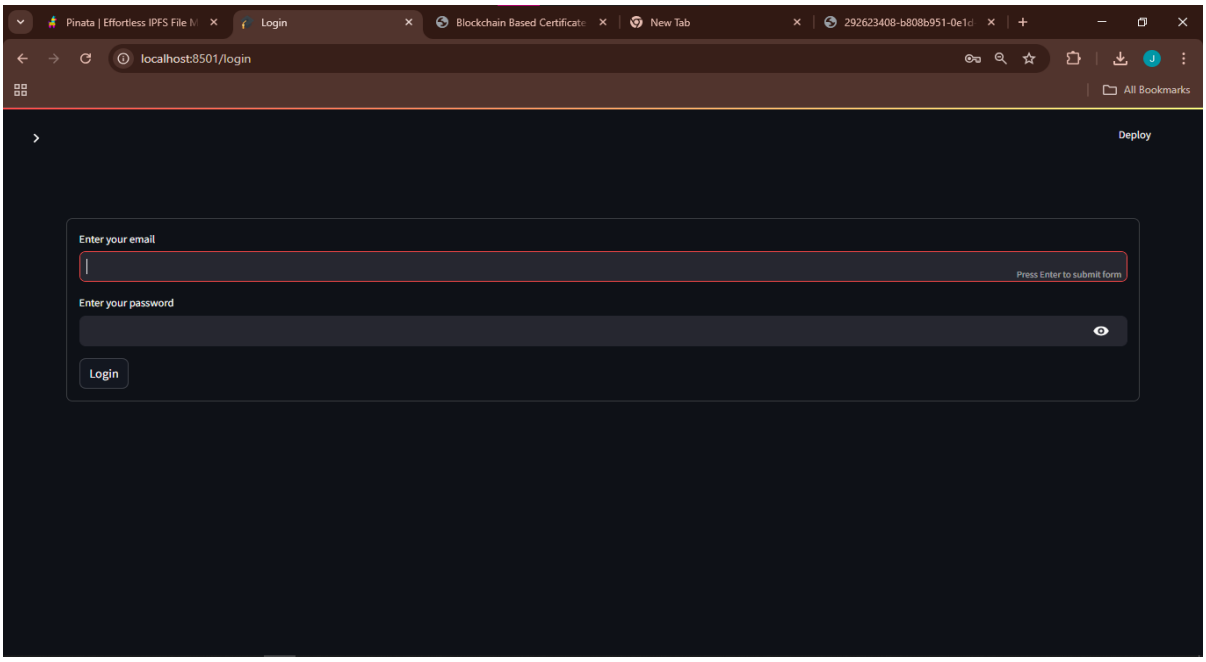


Figure 5: Certificate generation (Single generation)

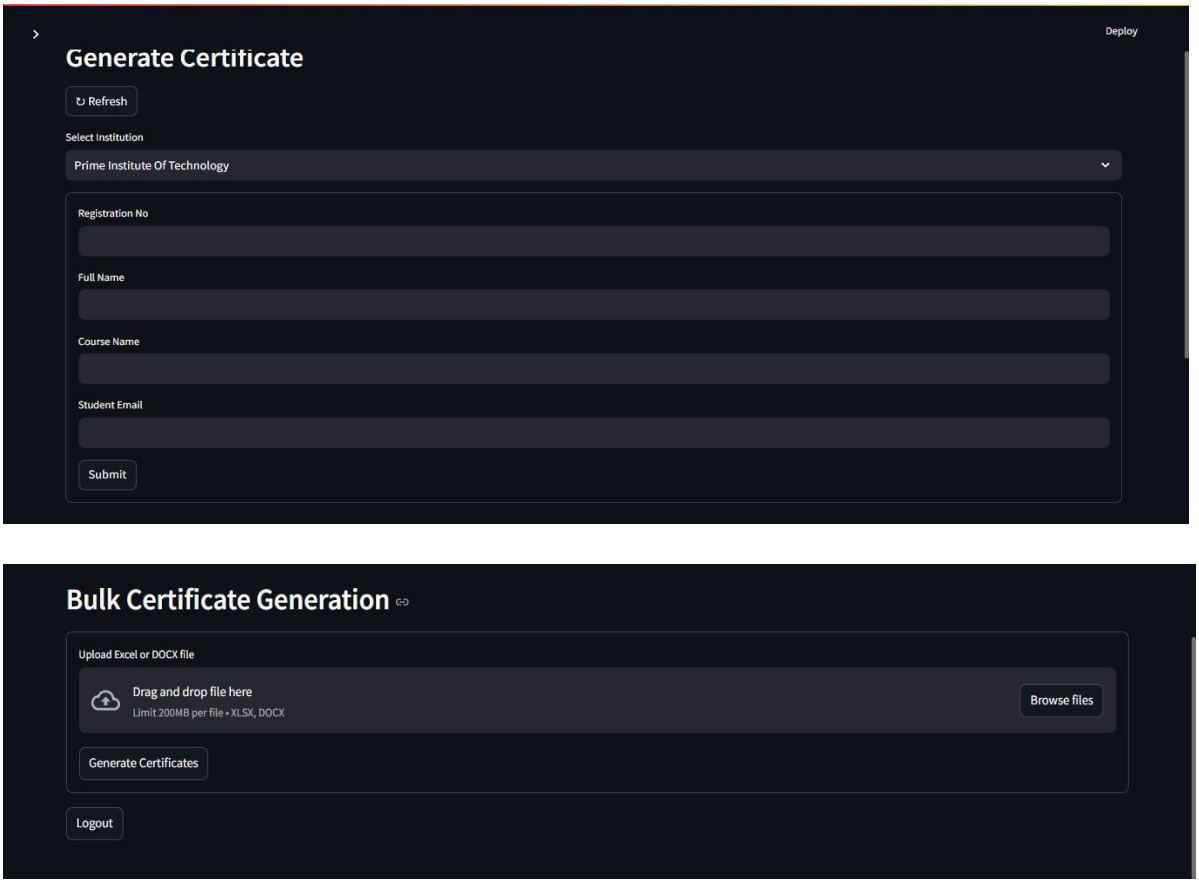


Figure 6: Revoke Certificate

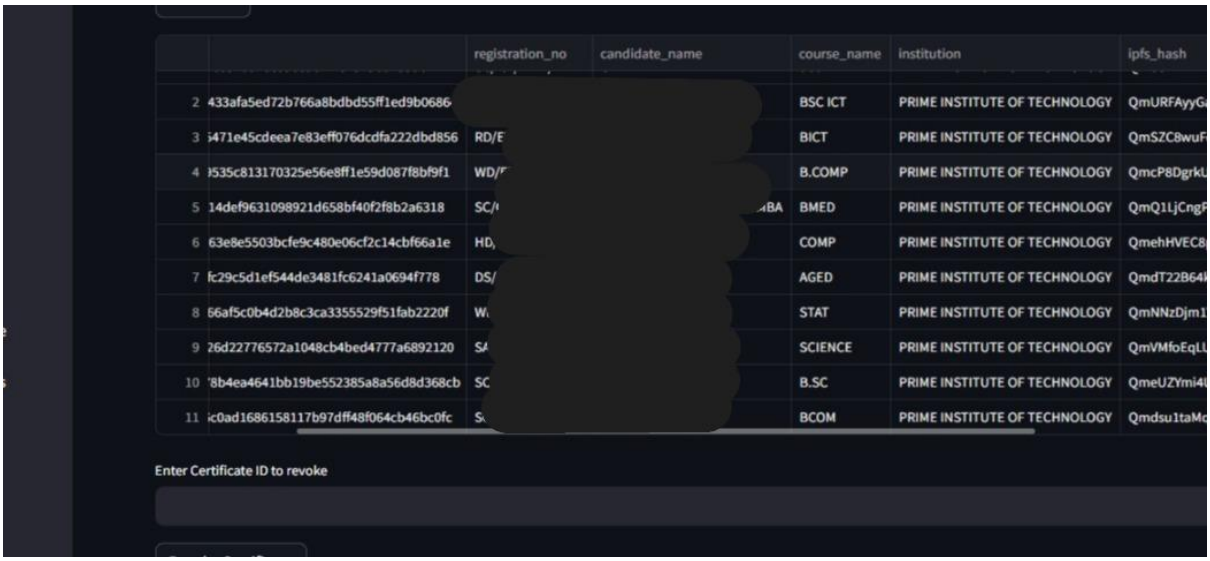
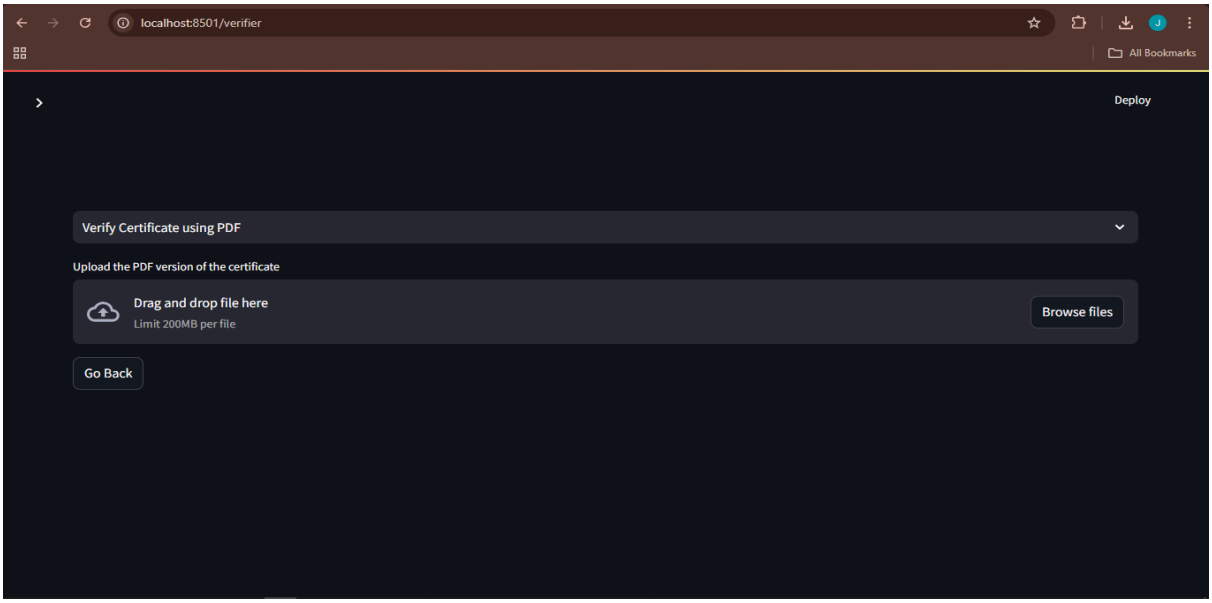


Figure 7:Verification page



CONCLUSION

The research proposes creating a blockchain-based certificate issue and verification system automation architecture to avoid the falsification of digital assets as a framework for accelerating the digital transformation to secure and maintain data confidentiality in a document. So that validation of a document maintains authenticity. The application of cryptography using the Blockchain method helps to keep our documents secure with a shared storage system and if there are changes or updates only agree if there is mutual agreement and agreement from all parties.

REFERENCES

C. K. Wong and S, S. Lam “Digital signatures for flows and multicasts”, WEEE/ACM Transactions on Networking, 7(4): 502- 513, 1999.

A. M. Antonopoulos, Mastering Bitcoin: Unlocking Digital. Sebastopol, CA, USA: O’Reilly Media, 2015.

Benyuan He, “An Empirical Study of Online Shopping Using Blockchain Technology“, Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

Chris Dannen, Introducing Ethereum and Solidity, https://www.apress.com/br/book/9781484225349 [5] J. Clark and P. C. van Oorschot, “SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements,” in proc. IEEE S&P’13, May 2013, pp. 511–525.

L. Zhang, D. Choffnes, D. Levin,et al., “Analysis of SSL certificate reissues and revocations in the wake of Heartbleed,” in proc. ACMIMC’14, Nov 2014, pp. 489– 502.

M. Carvalho and R. Ford, “Moving-target defenses for computer networks,” IEEE Security & Privacy, vol. 12, no. 2, pp. 73–76, Mar.-Apr.2014.

apazoglou, M., Service-Orientated Computing: Concepts, Characteristics and Directions, in International Conference on Web Information Systems Engineering. 2003, IEEE: Rome.

D. Ferraiolo, R. Kuhn, and R. Sandhu, “Rbac standard rationale: Comments on ”a critique of the ansi standard on role-based access control”, ”IEEE Security Privacy, vol. 5, no. 6, pp. 51–53, Nov 2007.

A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, “Towards a novel privacy- preserving access control model based on blockchain technology in IOT,” in Europe and MENA Cooperation Advances in Information and Communication Technologies. Springer, 2017, pp. 523– 533.

L.Y. Chen and H. P. Reiser, “Distributed applications and interoperable systems, 17th ifip wg 6.1 international conference, dais 2017, held as part of the 12th international federated conference on distributed computing techniques, discotec 2017, neuchtel, switzerland, June 1922, 2017.” Springer, 2017.

Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “Medshare: Trust-less medical data sharing among cloud service providers via blockchain,” IEEE Access, vol. 5, pp. 14 757–14 767, 2017.

S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008.

A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction", Princeton University Press, 2016.

A. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names", in proc. of the ACM Internet Measurement Conference (IMC), 2013.

V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", https://ethereum.org/en/whitepaper/, 2013.