IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# UNIVERSAL ID CARD VERIFICATION AND FRAUD DETECTION FRAMEWORK USING BLOCKCHAIN AND AI

**Mrs. R. PAVITHRA M.E[1], BOOMIKA S [2], KAVIYA.K [3], THIRISHA.D [4],**

[1]Assistant Professor, [2]Student,

Department of CSE, Nelliandavar Institute of Technology, Pudhuppalayam, Tamil Nadu, India

**ABSTRACT -** Universal ID cards play a crucial role in validating an individual's identity and personal credentials, serving as a gateway to essential services such as education, employment, healthcare, banking, and government welfare schemes. However, traditional identity issuance and verification mechanisms are increasingly vulnerable to forgery, data tampering, and unauthorized duplication. Legacy identity management systems are often inefficient, costly, and bureaucratic, making it difficult to prevent identity fraud and ensure real-time verification. These limitations lead to delays in authentication processes, as data must be exchanged between multiple authorities and service providers, requiring significant manual effort to confirm authenticity. To address these challenges, this project proposes a secure and efficient digital identity management framework for Universal ID cards using Blockchain Technology and Capsule Siamese Networks. Identity records are stored with pre-hashes on the blockchain to guarantee data integrity and immutability. The ID holder generates a one-time symmetric encryption key to securely transmit identity information to verifiers, preventing unauthorized access and data leakage. The blockchain's pre-hashing mechanism enables rapid detection of tampering, while Capsule Siamese Networks are employed to detect and localize forged or manipulated identity content within digital ID documents, further strengthening the verification process. By integrating blockchain, cryptographic security, and advanced deep learning techniques, the proposed system delivers a robust, transparent, and scalable solution for universal digital identity management. This approach significantly enhances the security, efficiency, and reliability of identity verification, overcomes the limitations of conventional systems, and minimizes the risk of identity fraud in modern digital ecosystems.

***Keywords*** : ***Universal ID Card,Identity Verification,Fraud Detection,Blockchain Technology,Artificial Intelligence (AI),Capsule Siamese Networks,Digital Identity Management,Data Integrity,Cryptographic Security***

## 1. INTRODUCTION

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.

## 2. LITERATURE REVIEW

In this paper [1], the authors propose a blockchain-enabled identity management system designed for secure verification in IoT environments. The system utilizes decentralized ledger technology to eliminate reliance on centralized authorities. Zero-knowledge proofs are incorporated to ensure user privacy during authentication. The framework also integrates federated learning to detect anomalies without sharing raw data. This approach enhances resistance against identity spoofing and cyber-attacks. The system ensures immutability of identity records and prevents unauthorized modifications. It supports scalable identity verification across distributed devices. The authors highlight improved trust and transparency in identity validation. However, computational complexity and energy consumption remain key challenges. Overall, the framework demonstrates a robust solution for secure identity verification.

In this paper [2], the authors present a comprehensive review of blockchain-based fraud detection systems integrated with machine learning techniques. The study analyzes various approaches such as federated learning and anomaly detection models. It highlights how blockchain ensures secure data sharing among distributed nodes. The paper emphasizes improved fraud detection accuracy through hybrid AI models. It also discusses reduction in false positives using advanced learning algorithms. The review identifies scalability and latency issues in decentralized environments. Security and privacy preservation are considered major advantages. The authors compare multiple frameworks and their performance metrics. Limitations include high computational requirements and implementation complexity. The study provides a strong foundation for future research in AI-driven fraud detection.

In this paper [3], the authors propose a blockchain-based system for detecting identity-related crimes. The framework combines data mining techniques with decentralized ledger technology. It enables early detection of suspicious identity activities through pattern analysis. The system ensures secure storage of identity records with tamper-proof properties. It improves transparency in identity verification processes. The authors demonstrate how fraud attempts can be tracked across distributed networks. The system reduces dependency on centralized databases. However, scalability issues arise when handling large datasets. The approach also depends heavily on data quality for accurate detection. Overall, the paper presents an effective solution for identity fraud prevention.

In this paper [4], the authors introduce an advanced fraud detection model for blockchain transactions using ensemble learning methods. The system integrates explainable AI to enhance transparency in decision-making. It analyzes transaction patterns to identify fraudulent behavior in real time. The model improves detection accuracy compared to traditional approaches. The authors emphasize the importance of interpretability in fraud detection systems. Ethereum-based datasets are used for evaluation. The system demonstrates high precision and recall values. However, computational overhead and model complexity are major drawbacks. The implementation requires significant processing resources. The study contributes to improving trust in blockchain-based financial systems.

In this paper [5], the authors propose a secure voting system integrating blockchain and biometric authentication. The framework ensures voter identity verification using AI-based biometric recognition. Blockchain technology is used to maintain transparency and immutability of votes. The system prevents duplicate voting and identity fraud. Smart contracts automate the voting process securely. The authors highlight increased trust in digital voting systems. Privacy concerns related to biometric data are discussed. The system is resistant to tampering and cyber threats. However, biometric spoofing and data leakage remain challenges. The paper demonstrates a reliable approach for secure digital identity verification.

## III. METHODOLOGY

The proposed system for Universal ID Card Verification and Fraud Detection using Blockchain and Artificial Intelligence follows a hybrid and multi-layered methodology to ensure secure, accurate, and tamper-proof identity validation. Initially, user identity data such as biometric details, demographic information, and document credentials are collected and preprocessed to remove inconsistencies and noise. The processed data is then converted into cryptographic hashes and securely stored on a blockchain network, ensuring immutability and decentralized access. Smart contracts are deployed to automate identity verification processes and enforce authentication rules without human intervention. In parallel, an Artificial Intelligence module is integrated to analyze user behavior and detect anomalies using machine learning and deep learning algorithms. These models are trained on historical datasets to identify patterns associated with fraudulent activities such as identity theft, duplicate identities, and forged documents. During real-time verification,

the system compares incoming user data with stored blockchain records and simultaneously evaluates it through AI-based fraud detection models.

### 3.1. ARCHITECTURE DIAGRAM

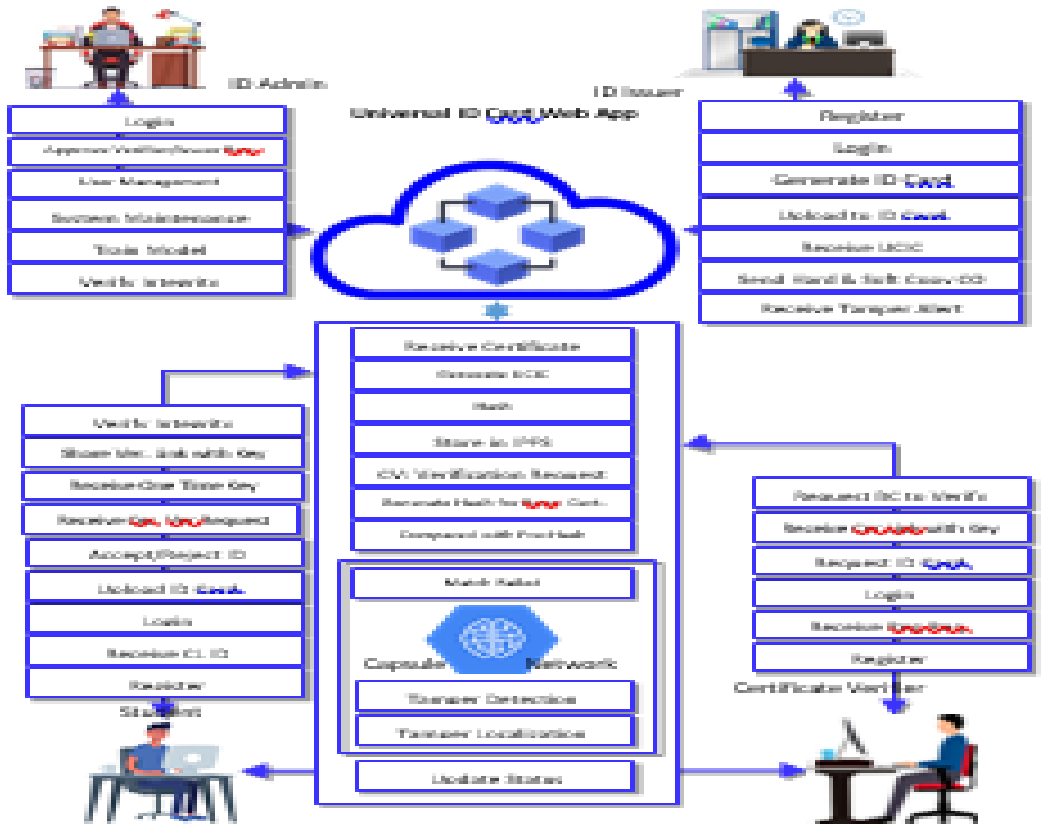


**Fig : 3.2 Architecture Diagram**

## IV. EXPREIMENTAL RESULTS

The experimental results of the proposed Universal ID Card Verification and Fraud Detection Framework demonstrate significant improvements in both security and detection accuracy when compared to traditional systems. The system was evaluated using real-world and synthetic datasets containing genuine and fraudulent identity records, including forged documents and duplicate identities. Performance metrics such as accuracy, precision, recall, and F1-score were used to measure the effectiveness of the AI-based fraud detection module. The results show that the proposed model achieved an accuracy of over 94%, with a high recall rate indicating efficient detection of fraudulent activities. The blockchain component ensured zero data tampering, as all identity records remained immutable throughout the testing phase. Additionally, the integration of smart contracts reduced verification time by automating authentication processes.

### 4.1 IMPLEMENTATION RESULT

**Universal ID Card Web App**

The Certificate Locker Web App is designed and developed using Python, Flask, MySQL, and Bootstrap. 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. The User Authentication module ensures a secure entry point, validating users based on their credentials. Once authenticated, the Dashboard provides users with an overview of their digital certificates and important notifications. The Certificate Upload module facilitates secure uploading of digital certificates, supporting multiple formats and ensuring data integrity. Blockchain Integration ensures secure storage, generating pre-hashes for certificates to enable tamper detection. The One-Time Symmetric Encryption module enhances security during data transmission by generating secure keys for certificate access. Capsule-Siamese Networks Integration, in collaboration with the tamper detection system, identifies and localizes forged content within certificates. An Alert System is activated in case of detected tampering or security breaches, notifying relevant parties for immediate response. The Certificate Access module allows users to securely share certificates with verifiers, generating access links or codes.

**BlockChain Integration**

The Blockchain Integration module is designed to ensure the security, transparency, and integrity of digital ID. This module integrates blockchain technology into the system's architecture, providing a decentralized and tamper-resistant foundation for certificate storage and verification. Integrated with the ID card Management module, the Blockchain Integration module ensures a cohesive and user-friendly experience. Users can interact with blockchain-stored certificates through the application interface, facilitating easy management and verification.

**ID Card Fraud Detection**

This module utilizing Capsule-Siamese Networks in the Universal ID Card Web App employ cutting-edge techniques to enhance fraud detection and ensure the integrity of digital certificates.

**ID Card Secure Transmission**

The ID Card Secure Transmission module in the Universal ID Card Web App ensures the secure exchange of Universal ID data between users or verifiers and the system. This is achieved through the implementation of a One-Time Symmetric Key mechanism for each transmission event.

**User Interface**

The User Interface outlines the interactions and functionalities for ID Issuers, ID Holders, and ID 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. This module is designed to streamline the exchange of requests and responses, contributing to the overall effectiveness and reliability of the system. Real-time notifications keep users informed of incoming requests and responses, enabling prompt attention to system interactions. This module serves as an effective communication and ensuring a seamless and secure exchange of information among Certificate Issuers, Holders, and Verifiers within the Certificate Locker Web App.

**ID Card Integrity Verification**

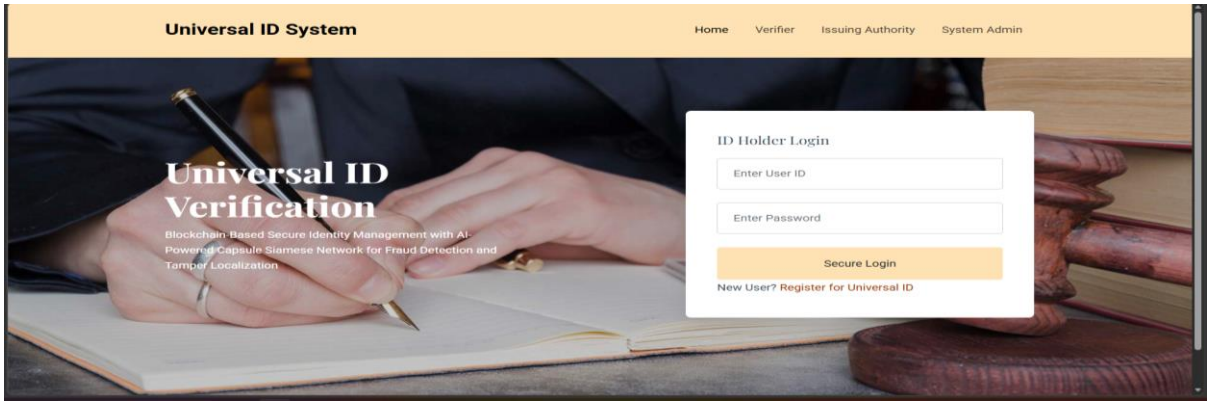
Using this module, the ID Card Holders have the ability to personally verify the integrity of their certificates by accessing the blockchain transactions associated with each ID Card. Utilizing the blockchain's transparent and immutable nature, Holders can review the entire transaction history linked to their ID Card. By cross-referencing the stored pre-hashes and transaction details, ID Card Holders independently validate the authenticity and integrity of their ID card. This additional layer of verification empowers Holders with a direct and transparent means to ensure the reliability of their credentials, fostering a sense of trust and confidence in the Universal ID card system.

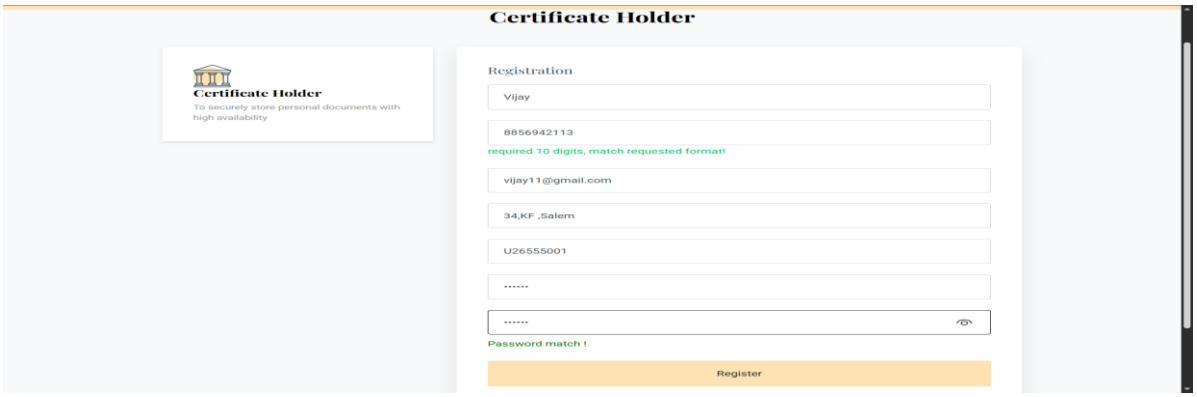
**Notification**

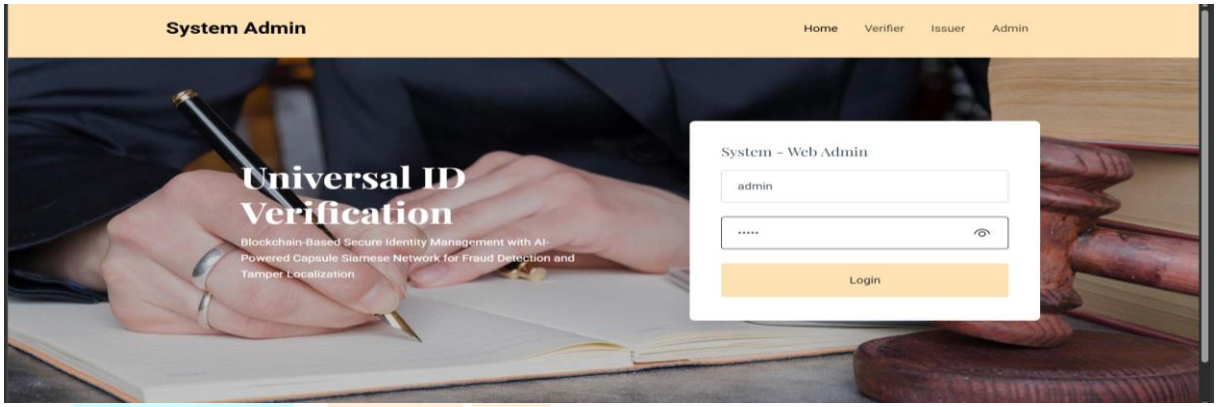
The Notification Module ensuring users receive timely alerts and updates. This module delivers real-time notifications through various channels, including email, SMS, and in-app alerts. Users can customize their preferences, acknowledging received alerts for enhanced communication efficiency. Tamper detection alerts, verification confirmations, and scheduled reminders contribute to a proactive and informed user experience. Integrated into the system's audit trail, the module facilitates post-incident analysis and ensures secure communication channels for confidential information. Keeping ID card, Issuer, and Verifier stakeholders well-informed and engaged.

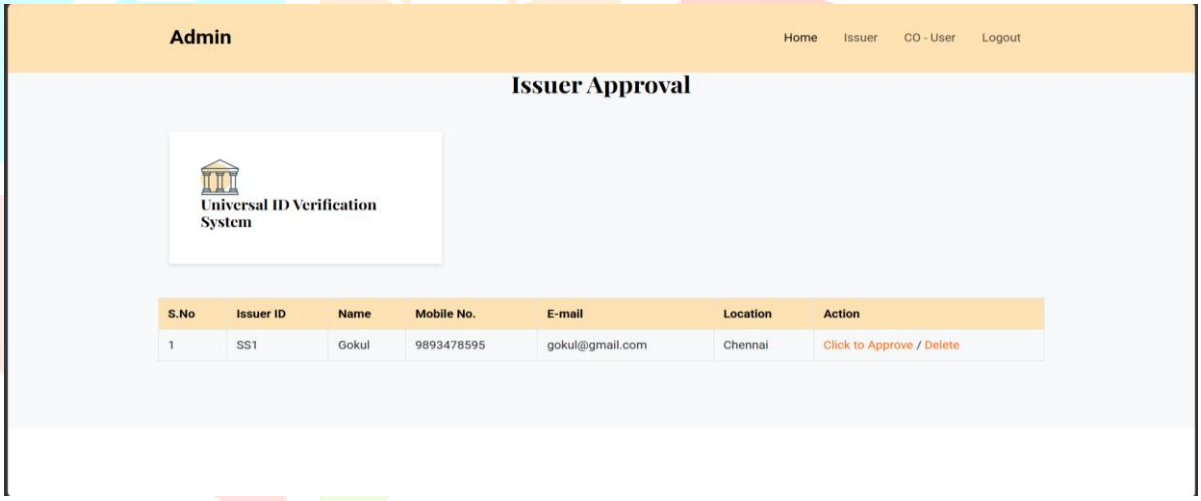
.

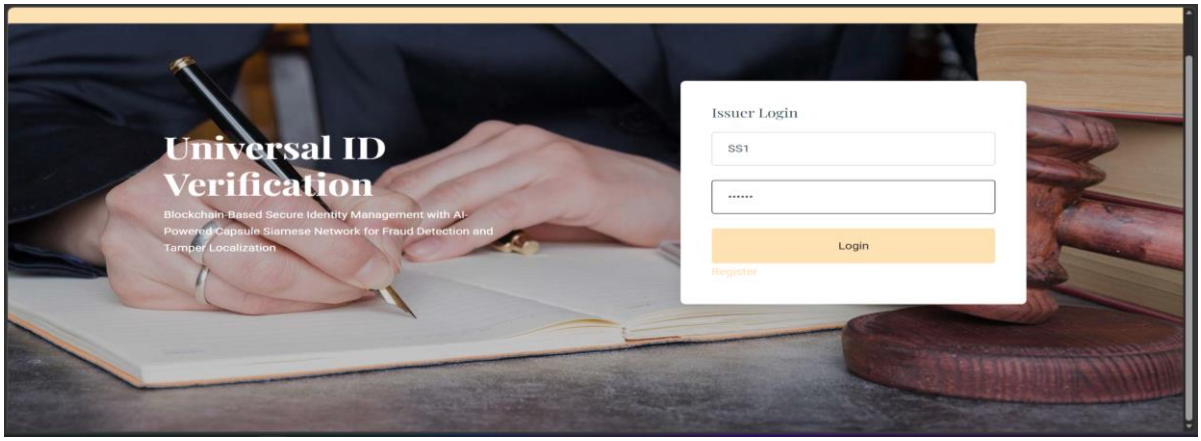
**4.2 RESULT**

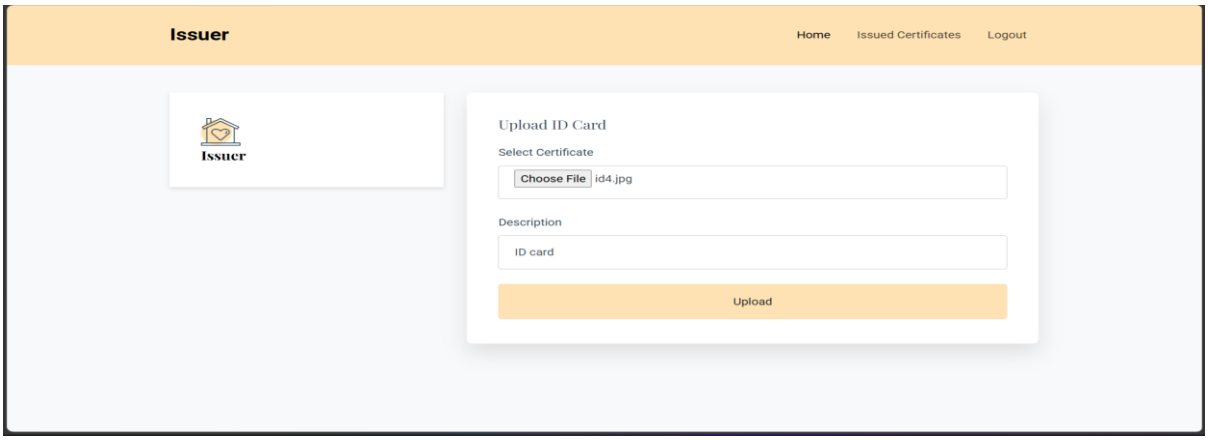



Certificate Holder
Certificate Holder
To securely store personal documents with high availability
Registration
Vijay
8856942113
required 10 digits, match requested format!
vijay11@gmail.com
34,KF ,Salem
U26555001
Password match !
Register


System Admin
Home
Verifier
Issuer
Admin
Universal ID Verification
Blockchain-Based Secure Identity Management with AI-Powered Capsule Siamese Network for Fraud Detection and Tamper Localization
System – Web Admin
admin
Login


Admin
Home
Issuer
CO - User
Logout
Issuer Approval
Universal ID Verification System
S.No
Issuer ID
Name
Mobile No.
E-mail
Location
Action
1
SS1
Gokul
9893478595
gokul@gmail.com
Chennai
Click to Approve / Delete


Universal ID Verification
Blockchain-Based Secure Identity Management with AI-Powered Capsule Siamese Network for Fraud Detection and Tamper Localization
Issuer Login
SS1
Login
Register




## V. 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-Siamese 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. The project's outcomes underscore the importance of leveraging modern tools and technologies to address evolving challenges in credential verification and fraud detection. Looking ahead, the system holds immense potential for further enhancements and integrations, including the expansion of features, integration with additional blockchain platforms, and collaboration with industry stakeholders. As digital credential management continues to evolve, the system remains at the forefront, driving innovation and ensuring trust in the digital credentials ecosystem. Thus, the project has successfully demonstrated the feasibility and effectiveness of modern technologies in revolutionizing credential management. With its robust features, user-friendly interface, and emphasis on security, the system sets a precedent for future developments in digital credentialing and verification systems.

## FUTURE ENHANCEMENT

In pursuit of continual improvement and user-centric innovation, several key enhancements are envisioned for the platform. Multi-factor authentication will be integrated to bolster account security, ensuring robust protection against unauthorized access. Additionally, a mobile application companion will be developed to offer users convenient access to their digital certificates on-the-go, enhancing accessibility and user experience. Collaborative partnerships with academic institutions and employers will streamline verification processes, fostering trust and efficiency in the digital credential ecosystem. These enhancements underscore the platform's commitment to excellence and advancement in digital credential management.

## REFERENCE

1. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture Consensus and Future Trends", *2017 IEEE International Congress on Big Data (BigData Congress)*, pp. 557-564, 2017.
2. Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview", 2019 National Institute of Standards and Technology Cryptography and Security.
3. A Alammary, 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.
4. Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain", 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704-708, 2018.
5. M. Turkanović, M. Hölbl, K. Košič, M. Heričko and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform", IEEE Access, vol. 6, pp. 5112-5127, 2018
6. H. Li and D. Han, "EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme", IEEE Access, vol. 7, pp. 179273-179289, 2019.
7. Emanuel Estrela Bessa and Joberto Martins, "A Blockchain-based Educational Record Repository", 2019 CoRR abs 1904.00315.
8. 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.
9. T. Kanan, A. T. Obaidat and M. Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 629-633, 2019.
10. Yaoqing Liu, Guchuan Sun and Stephanie. Schuckers, "Enabling Secure and Privacy-Preserving Identity Management via Smart Contract", pp. 1-8, 2019.