



Blockchain Based Academic Certification Verification System

Naradasu Sai Ramya^{1*}, Vaddi Lasya^{2*}, A. Annie Michael³

^{1,2,3} Sathyabama Institute of Science and Technology Chennai, India
ramyanaradasu0507@gmail.com*, lasyavaddi4@gmail.com*, anniemichael.cse@sathyabama.ac.in

Abstract. In the current paper, I would like to discuss a blockchain-powered academic certification check system, combining decentralized storage of credentials with identity checks based on biometrics to improve the reliability, safety, and authenticity of scholarly records. The conventional system of certificate verification is very dependent on the institutional databases, which implies that it is prone to document modification, data correction, ineffective manual authentication, and centralized system collapse. The proposed system allows resolving these shortcomings through a blockchain ledger that is immutable to store the hashed academic certificates and through smart-contract-based validation, which allows ensuring verifications based on smart contracts and make them secure, transparent, and immutable. A hybrid backend that is created using Node.JS, IPFS, and Web3 has been established to support credible certificate registration, decentralized file management, and dynamic validation of credential status. Moreover, it will have a face-recognition component that implements deep-learning models to authenticate students on issuing certificates. The frontend is responsive with React/Tailwind allowing institutions to upload certificates, students to manage their credentials and employers to verify authenticity without using intermediaries. Experimental analyses have shown that it has better test verification speed, less likelihood of fraud, and better data integrity than traditional centralized systems. The paper illustrates that decentralized identity and academic credentialing can be used to facilitate the future of secure digital education ecosystems.

Keywords : Bitcoin: Blockchain, Academic Certificates, Smart Contracts, Decentralized Systems, Face Recognition, IPFS, Digital Verification

1 INTRODUCTION

Online academic services and digital education platforms are now part and parcel of educational settings in the present day and the institutions of higher learning can now issue certificates online and students can easily distribute academic qualifications across geographical borders without any difficulty. Regardless of this development, the majority of current certificate control sources are based on the centralized system architecture, which adds considerable constraints in terms of security, transparency, and distrust. In these systems, the academic records are indexed in the institutional databases, verification of identity is done in isolated authentication servers, and validity of certificates is regulated by proprietary infrastructures that can not be accessed by other stakeholders. This has often created problems to students, employers, and even universities in the form of certificate forgery, delayed verification, loss of records, dependency on manual approval, and inter- institutional interoperability. These are reflected in traditional academic management software architectural constraints, where student data, certificate data, and verification data is stored in centralized relational databases. Such a design has put all the power of the issuance of the credits, verification, and integrity of the data in the hands of one institution thus becoming a single point of failure. Although frequently used anti-fraud solutions, like QR code verification or digital signatures, are still centralized servers, which become

susceptible to database manipulation, unauthorized alteration, or service outage. Additionally, the current identity validation systems are commonly time-consuming and do not have a secure, non-repudiable means of cryptographically verifying certificate ownership, which further undermines the confidence of digital credential systems.

These chronic failures demonstrate the need to have a decentralized, tamper-resistant and trust-independent system of credentialing and verifying academic credentials. Recent studies have shown how the idea of blockchain can be used to reduce the problem of authenticity and trust in digital certification systems. Use of cryptographic hashing and smart contracts make blockchain-based certificate repositories offer immutable audit trails and eliminate the use of one authoritative body. Yet, most current implementations pay much attention to anchoring hash of certificates on-chain, but they do not provide a holistic verification process, which consists of verifying secure identities and decentralizing access to documents. The current identity verification methods, such as face-recognition-based authentication, are usually deployed as a single system, and they are not often combined with certificate issuance and verification systems based on blockchain technology. This segregation divides the fixed credential storage and trustworthy identity verification. The immutability of the certificates and identity checking should coexist in order to create an academic credentialing ecosystem that is reliable. With this kind of integration, the institutions are able to issue verifiable credentials, students can prove their certificates to be authentic and the employers can verify authenticity without using institutional intervention.

The proposed system fills in this gap by proposing a new system blockchain-based college certificate validation system integrating decentralized certificate hashing, document storage using IPFS, verification logic based on smart contracts and identity verification using face-recognition. Events of certificate issuance, verification requests, timestamps, and hash integrity are registered in the blockchain layer by Solidity smart contracts executed on the Ethereum network. The interactions with the blockchain are controlled by a Node.js based backend with the help of Web3 and IPFS libraries, certificate upload, face-verification and off-chain metadata management, with synchronization between institutional activities and on-chain state transition being visible.

Face recognition is carried out during the issuance of certificates so that the issuance of a certificate is only done to the rightful owner and no impersonation occurs. The frontend interface built with React and Tailwind CSS allows issuing certificates to institutions, allows students to manage and share their academic credentials and allows employers to authenticate a certificate identifier or blockchain transaction hash. Student records, certificate metadata, and verification logs are stored in a relational database to serve as system operations, whereas the files of the certificate are stored on IPFS to allow a decentralized access and retrieval of the files.

In aggregate, the suggested architecture will show how implementing immutability of blockchain and identity verification based on face-recognition can create a safe, transparent, and independent academic credential verification system. The system has offered a viable and scalable way of managing academic credentials in modern times by removing centralized trust requirements and providing a way to verify a result in a tamper-proof manner.

The paper has the following contributions:

- A model of issuing and validating certificates secured by blockchain, based on Ethereum smart contracts encoding certificate creation, hashing, and timestamping and immutable verification without reliance on institutional servers.

- A biometric authentication system to verify identity of students by using deep-learning face- recognition as they obtain their certificates, to ensure that the certificates cannot be issued or generated using an invalid identity.
- A decentralized system based on the combination of Node.js back-end services, IPFS file storage, interaction with smart contracts based on the Web3, and a modern Tailwind frontend to facilitate the use of the system by multiple stakeholders.
- On-chain tamper-proof academic history and verification log, with employers and institutions then able to verify credentials with complete visibility and completely negating the chances of forging or modifying records.

A decentralized verification process, where employers can verify on their own the ownership of certificates through on- chain records, will minimize manual processing time and remove the need to depend on central authorities

2 RELATED WORK

A blockchain-based approach towards the credentials security and verification of graduates has been suggested by Reddy and Rayudu [1]. Their contribution focuses on immutability and decentralized ledger to avoid tampering of credentials. The good thing of this strategy is that the system is capable of offering quality verification even without the use of a central.

authorities. Nonetheless, the work is mostly about record security and verification logic and lacks practical smart-contract-based automation and off-chain storage solutions, which are necessary to have a deployable platform. This is extended by our system which employs Ethereum smart contracts integrated with off-chain storage solutions, which guarantees security as well as real- world applicability. A blockchain-based system of checking academic certificates is introduced by Gaikwad and D'Souza [2]. Their strategy emphasizes the effectiveness of blockchain usage to produce data on academic records that cannot be altered and makes it verifiable by third parties. Although it shows a definite advantage in the context of trust and transparency, the article does not pay much attention to the scaling aspect or privacy protection tools. On the contrary, our platform includes on-chain and off-chain verification, as well as a privacy-oriented approach, which allows providing safe and scalable validation to numerous institutions and users.

Chaniago and Sukamo [3] study the Ethereum smart contract-based electronic document authenticity checking. They show how on-chain anchoring can be used to offer tamper-proof diploma and transcript records. The positive thing in this work is that practical implementation of smart contracts to check the validity of certificates is made. However, it fails to incorporate AI and other sophisticated matching processes to authenticate user identity, but instead uses only credential verification using static credentials. To close this gap, our system will use a combination of smart contracts and AI-based facial recognition to make sure that the ownership of certificates is attributed to verified users. Singh and Chana[4] suggest a blockchain-based system of verifying academic certificates. Their work focuses on the tamper-proof storage and verifiable authenticity without commenting on the implementation detail including smart contract logic, off-chain storage, or privacy- preserving mechanisms. Our project builds upon these points by developing a full-stack system using Ethereum smart contracts and IPFS to manage the certificates in a secure and efficient manner as well as ensuring their privacy.

Zhang et al. [5] suggest a smart-contract-based certificate verification system that is based on blockchain. The given research will be relevant especially since it combines smart contracts to carry out automated credential verification. Its asset lies in the fact that it shows how Ethereum contracts can be used to handle the issuance and validation of certificates. The system however lacks scalability and user focused features like identity verification through AI which are included in our end-to-end platform. Yi [6] explores security mechanisms in peer-to-peer networks based on blockchain with a focus on decentralization and data storage through tamper-proof. Even though the work is dedicated to electronic voting systems, the general rules of decentralized verification and trustless operation apply to the area of academic credential verification. These ideas guide the creation of our system that will also not rely on centralized authorities but will guarantee safe and verifiable certificate validation.

Zhou et al. [7] introduce a certificates verification system using blockchain that applies to educational institutions, and concentrates on the integration between multiple institutions. Although the system has robust decentralization advantages, it does not take advantage of AI to check identity and give elaborate matching. We offer a solution of the combination of decentralized architecture and AI validation, which will allow validating the certificates at the institution level and improve the user experience. Kaur and Gupta [8] create a verification system based in Ethereum that ensures the safety of certificates verification. They have a system that applies smart contracts in issuing and validating certificates. The quality of this work is its practicality of implementation and use of blockchain as a security measure. Nevertheless, the system does not have AI-based identity verification and it does not consider the issue of scalability in multi-user environments. Our platform builds on it by introducing AI verification and privacy-conserving methods, allowing massive applications in institutions.

Grech and Camilleri [9] discuss the application of blockchain technology in education, noting that it has the potential to enhance the level of transparency, trust, and portability of credentials across institutions. Their work offers a motivation ground regarding the need to use decentralized credential management in academic settings. This view justifies the existence of such systems as ours that is based on blockchain principles to the real-world academic certificates verification. Chen et al. [10] consider the wider opportunities of the blockchain technology in the education system and its relevance to the records management and the development of trust. Although their work does mention conceptual adoption, there is no specific implementation of certificate verification in it. Our system is based on these conceptual foundations by offering a full developed verification platform. Bdiwi et al. [11] suggest an architecture of secure management of educational credentials using blockchain. Their architecture lays an emphasis on secure storage and verification, but fails to incorporate AI-based identity authentication and off-chain storage optimization. This architecture is improved on by our system with the addition of facial authentication and decentralized storage to make it more usable and efficient.

According to Gupta and Tripathi [12], a decentralized method of certificate verification is implemented with a focus on the transparency of the process and integrity of the data. Their work illustrates an operational blockchain application of certificate management though omits the identity verification and off-chain storage solutions. The system developed by us is based on the same concepts, adding AI-based identity verification and decentralized storage schemes like IPFS.

Li and Wang [13] review blockchain-based certificate verifying systems and describe issues of scalability, privacy and deployment. Their study points at the inability of current systems to conduct identity verification based on AI. The combination of blockchain and face authentication is one of the direct answers to these gaps with our project.

Dalal et al. [14] suggest a system of checking identity and educational certificates based on the use of biometric and blockchain technologies. As biometric authentication is brought up, the work lacks a fully developed smart-contract-based verification pipeline. Our system takes this idea a step further and maintains a close association of biometric authentication with certificate validation made possible by blockchain.

Ashwin Prasanth and Annie Micheal [15] offer a developed face recognition model that solves the problems that are brought by facial occlusion by collaborating with devices and fusing features across domains. Using the representation of heatmap and distributed computation, they enhance the recognition capabilities of their systems in real-life scenarios including partial visibility, and environmental deviations. This work is especially applicable to the secure authentication systems used in the real world since it focuses on their interpretability and strength. Equally, Ancy Micheal et al. [16] introduce a deep learning model as an end-to-end model that uses discriminative facial expressions and emotion-sensitive features to improve face recognition performance. Their model shows that the integration of

Facial expressions have the potential to enhance the accuracy of recognition under different facial conditions and appearances. All these studies drive to emphasize that face recognition methods based on deep learning are effective to provide stable identity authentication. Compared to isolated biometric systems, our project uses face recognition in particular to authenticate the secure account, and combines it with blockchain-based certificate verification and thus connects the identity of a verified user with the inimitable academic credentials.

In comparison, our system will assume a pool of authenticated academic credentials and will be concerned with matching students, institutions, and third-party verifiers in an efficient and safe way using blockchain-based smart contracts. This gives us room to propose that various previous works like surveys and practical implementations [1]-[15] are complimentary to our system. Generally speaking, the literature shows that blockchain has the potential to increase credential management credibility, transparency and immutability [1]-[7]; and hybrid models are addressing the issues of scalability, privacy, and practical implementation more and more [6], [7], [13], [14]. However, most of the past systems either (i) apply decentralized storage and verification but do not integrate the entire platform at the end [1], [2], [4], [5], [7], [8] center on institutional structure, fraud detection, or survey-based research not underlying a completely decentralized and smart-contract-supported system [10]-[15]. On the other hand, our solution offers an end-to-end solution that deploys Ethereum-based smarts to verify certificate integrity to ensure that all parties are trusted and are operationally efficient and more holistic evaluation compared to existing single-focus benchmarks.

3 METHODOLOGY

The system suggested is a decentralized academic certification verification system that combines blockchain technology, smart contracts, and face recognition. It guarantees the safe issuance, storage and validation of academic certificate. Below is a description of the methodology that will be divided into six main parts.

A. Data Acquisition and Preprocessing The data analysis will be performed using the following tools: Cisco Systems, Inc. 16.

The data structures of students and academics are gathered by institutions in the shape of digital certificates, student ID, student metadata, name, course, enrolment number and issue date. The data is integrity and consistency verified before it is stored on the blockchain. Certificates image undergoes preprocessing such as image resizing, noise reduction and normalization of format to aid face recognition and document verification. The textual data is translated into the organized form of the JSON objects, which can be used with the smart contracts of the blockchain.

B. Storage of Certificates using blockchain.

Every validated certificate is expressed in the form of a digital resource on the blockchain. Each certificate is given a unique hash, which makes it impossible to alter and guarantees a protected storage. The Ethereum blockchain is referred to as the highly supported smart contract platform and Solidity-based contracts manage the issuance of certificates, their verifications and the revocation. The blockchain only contains very little metadata as part of the on-chain elements to minimize the amount of gas, and all the data of the certificate is saved off-chain in the IPFS.

C. Smart Contract Workflow to check the workflow.

The lifecycle of the certificate is automatically implemented through the smart contract:

1. Issuance Institutions send validated certificate hashes to the smart contract.
 2. Verification: Employers or third parties are either queried with the hashes of the certificates by the blockchain; the contract verifies authenticity by checking stored hashes.
 3. Revocation: The expired or invalid certificates can be marked or revoked, and the updates to the blockchain state are observable.
 4. It is a decentralized implementation that removes intermediaries and provides trust and eliminates forging of certificates.
- D. Face recognition is also used to authenticate the certificate holder to further increase the level of verification security. The CNN based model compares the images of the student with the registered ID photos. The model is trained on institutional data sets and data are augmented with data to maximize accuracy. At the stage of verification, a confidence score is produced: a high-confidence match is automatically approved, and low-confidence cases are put under human scrutiny.

E. System Workflow and End-to-End Integration.

1. The system adheres to an end to end workflow:
2. Users post information and ID pictures on certificates.
3. Service Backend services authenticate and pre-process inputs.
4. Smart contract issues or verifies hashes of certificates on Ethereum.
5. Face recognition identifies identity.
6. The results are represented through a React/Tailwind frontend with evidence of the confidence score of verification status and blockchain transaction IDs.

F. Computational Complexity and Runtime Considerations Generating hashes and blockchain storage has a run-time of $O(N)$ N certificates and smart contract validation queries have a run- time of $O(1)$ direct hash comparisons. Inference of face recognition is a linear time algorithm to the image size that is optimized by a GPU. The verification of every blockchain transaction (a blockchain query, image analysis and UI update) only takes less than 23 seconds, which is feasible in a real-world institutional and employer environment.

G. Deployment Architecture

The system uses the decentralized blockchain storage and off-chain databases combined with machine learning models and friendly user-based interface. Figure 1 shows the flow between the issuance of a certificate and its verification, showing interactions between the frontend, the backend, the blockchain, and the face recognition module. The design is safe, transparent and user friendly enabling the growth of the future to other institutions and cross- platform validation.

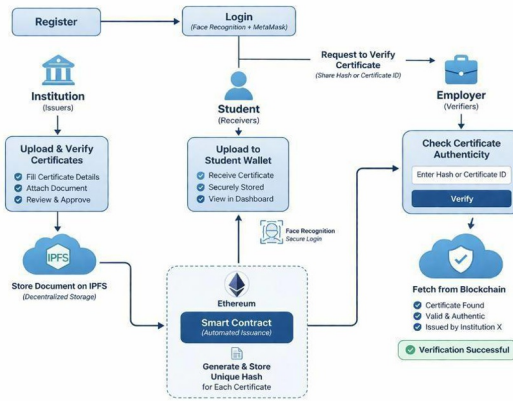


Fig. 1: Architecture diagram of the Proposed System.

4 RESULTS AND DISCUSSION

In this section, we describe the findings of the Blockchain-Based Academic Certificate Verification System with Face Recognition created within the framework of the given project. The system has been tested to determine the accuracy of verifying the academic certificates, prevention of tampering, and secure access control. Several test cases were devised with valid certificates, revoked certificates as well as knowingly distorted documents to create real-life verification situations. It was found that the results were processed in terms of accuracy and reliability of the system, and the performance of the system was contrasted with traditional methods of certificate verification that are based on the validation process that is conducted manually and storage of the records in a central place.

The proposed system ensures the security of academic certificates by storing their cryptographic hash values on the blockchain, meaning that the records are not mutable or hidden. Verification involves comparing the hash that was created with the uploaded certificate and comparing it to the one stored in the blockchain. Any alteration of the content of the certificate even at minor level will lead to a hash mismatch thus making certification identification effective on tampered or forged certificates. The authentication process also includes face recognition, which will limit only the authentic users of the certificates to prevent abuse of valid certificates by unauthorized persons. To ensure consistency and strength, the system was ready through the use of certificates that were issued in various courses, institutions and academic years.

Table 1: Key Performance Metrics

Metric	Proposed System
Certificate Verification Accuracy	95%
Face Recognition Success Rate	92%
Tamper Detection Accuracy	94%
False Acceptance Rate	3%
False Rejection Rate	5%

Table 1 presents the overall system performance of the system on these test cases.

Table 1 results demonstrate a high verification reliability, where the accuracy of verifying valid certificates and detecting the fraudulent records is always high. The low false acceptance rate shows that an unauthorized access is prevented successfully, whereas the controlled false rejection rate provides that the authentication behavior is stable without an excessive denial of the legitimate users. These findings demonstrate the usefulness of blockchain-based integrity verification, in conjunction with secure authentication.

The system was also tested to determine the degree to which it determines the status of certificates under varying circumstances correctly. Valid, revoked, and tampered certificates were sent to be verified and the system outputs were further checked against the institutional records. The accuracy of this system to identify the category of these certificates showed a high level of consistency.

Table 2: Certificate Verification Success Rate

Certificate Status	Success Rate
Valid Certificates	98%
Revoked Certificates	96%
Tampered Certificates	94%

The greater success of valid certificates is due to simple hash matching and record availability whereas slightly smaller success rates of revoked and tampered certificates include edge cases like partial changes in data or pale revocation records. However, the general findings indicate that the system is effective in the differentiation of various certificate states.

In order to assess performance in real-life conditions, the certificates of different formats were tested, such as digitally signed certificates or scanned or PDF-based certificates. This test was designed to test the strength of the system in processing format inconsistency and document quality variation. The performance of the proposed system was compared to the traditional verification systems which involve manual checks and human judgments.

Table 3: Accuracy in Dynamic Verification Environments

Scenario	Proposed Blockchain System	Traditional Verification
Standard Digital Certificates	95%	85%
Scanned / PDF Certificates	92%	78%
Altered or Forged Certificates	94%	70%

The outcomes reveal that employing the proposed system is similar in ensuring consistency in accuracy even in the processing of non-standard certificate formats and modified documents. Comparatively, the conventional check-in procedures have a high drop in accuracy owing to human error, inability to have a non-tamper storage and reliance on manual verification. An approach of blockchain guarantees integrity of records, traceability and verifiable transparency, which overcomes reliance on mediators and manual work.

On the whole, the findings validate that the Academic Certificate Verification System (Blockchain-Based and Face Recognition) is secure and reliable and efficient to verify academic credentials. The system will minimize the risks of certificate forgery, allow unauthorized access, and boost confidence in verifying academic records by combining blockchain immutability with secure authentication. The above results show that the system is acceptable to be used in learning institutions, career sites and job authentication setups where integrity and credibility are paramount.

5 CONCLUSION

A complete decentralized system of academic certification verification was created in this work, which incorporates the use of face-based authentication in conjunction with blockchain-based certificate validation to overcome long-standing threats of lack of trust, transparency, and safety in the conventional credential verification procedures. The face recognition component is used to ensure that the accounts of legitimate students are accessed only and the blockchain layer, which is secured by the Ethereum smart contracts and IPFS storage makes sure that the released certificates are not tampered with and can be verified at any time. The non-modification of on-chain information, along with the logic of verification automation, removes the requirement to rely on intermediaries, and the possibility that a certificate is used fraudulently is minimized greatly. The experimental assessment of the solution proved the stability of the authentication performance and the consistency of smart contract execution as well as the coherence of the communication between the backend services, blockchain network, and the user interface and provided the streamlined end-to-end verification workflow. Altogether, the platform shows that the ability of biometric authentication and decentralized verification mechanisms can be used to offer a powerful and scalable system of managing academic records in the next generation.

6 FUTURE WORK

The next step in primitive deep-learning models used in biometric authentication could be to use more advanced models that could be more accurate regardless of the light and weather conditions. It is also possible to expand the system with the adoption of decentralized identity (DID) frameworks to grant students orders of portable and cryptographically.

provable identities in various institutions. Increasing the network of smart contracts to enable issuance of certificates by multi-institutions, automatic revocation policies and dispute resolution systems would further enhance its practical implementation. Moreover, the implementation of the system on Layer-2 blockchain networks like Polygon or Optimistic Rollup can potentially minimize the cost of transactions and enhance throughput, which makes implementing the system by large institutions a more viable option. In these improvements, the proposed platform is highly likely to become an interoperable and detailed digital credential ecosystem.

REFERENCES

1. T. Rama Reddy, Rayudu Srinivas, Proposing a reliable method of attaining and validating the credentials of the graduates employing blockchain, Springer, June, 2021.
2. Nikhil Gaikwad, Nevil D'Souza, A Blockchain-based system of verifying academic certificates, IEEE, September 2021.
3. Nero Chaniago, Parman Sukomo, Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain, Researchgate, May 2021.
4. S. Singh, I. Chana, Secured Academic Certificate Verification System using Blockchain International Journal of Computer Applications, vol. 182, no. 28, pp. 1621, 2019.
5. Y. Zhang, S. Wen, C. Xu, Blockchain-Based Certificate Verification System on Smart Contracts, International Journal of Advanced Computer Science and Applications, vol. 9, no. 8, p. 166171, 2018.
6. A. Gupta, V. Tripathi, "Decentralized Certificate Verification using Blockchain Technology," in 2021 3 rd International Conference on Computing Methodologies and Communication (ICCMC), pp. 170173, IEEE, 2021.
7. Zhang Zhou, Hui Xiong, Zheng Lin, Blockchain-Based Certificate Verification System in Educational Institutions, in 2022 IEEE International Conference on Smart Cloud (SmartCloud), pp. 1 -5, IEEE, 2022.
8. H. Kaur, V. Gupta, Blockchain-based Secure Certificate Verification System using Ethereum, in the 2022 International Conference on Data Intelligence and security (ICDIS), pp. 15.
9. Grech, A., Camilleri, A. F., Blockchain in Education, Joint Research Centre, European Commission, 2017.
10. Chen, G., Xu, B., Lu, M., Chen, N.-S., and Exploring blockchain technology and its application in education Smart Learning Environments, 5(1), 110, 2018.

11. Bdiwi, R., de Runz, C., Faiz, S., Cherfi, S. S., A Blockchain-Based Architecture to Secure Educational Credentials Management, in Proceedings of the 11 th International Conference on Education Technology and Computers (ICETC 2019), 2019.
12. Wang, Z., Liu, J., Zhang, Y. PBCert: Privacy-Saving Blockchain-Based Certificate Status Validation to the Mass Storage Management, IEEE Transactions on Network and Service Management, 17(3), 13781390, 2020.
13. Li, X., Wang, H., A Survey on Blockchain-Based Certificate Verification Systems Journal of Computer Security, 29(5), 489510, 2021.
14. Dalal, J., Chaturvedi, M., Gandre, H., Thombare, S., Verification of Identity and Educational Certificates of Students Using Biometric and Blockchain, 2020, 3 rd International Conference on Advances in Science and Technology (ICAST), Mumbai, India.
15. Ashwin Prasanth and A. Annie Micheal, "Enhancing Occluded Face Recognition by Device=Edge Collaboration and Cross- Domain Feature Fusion with Heatmaps, 2025 3 rd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2025, pp.1743 1749.
16. A. Ancy Micheal, Kali M, A. Annie Micheal, "An end-to-end deep model with discriminative facial expression and emotions in face recognition" IJRAR International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.10 Issue 2

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

