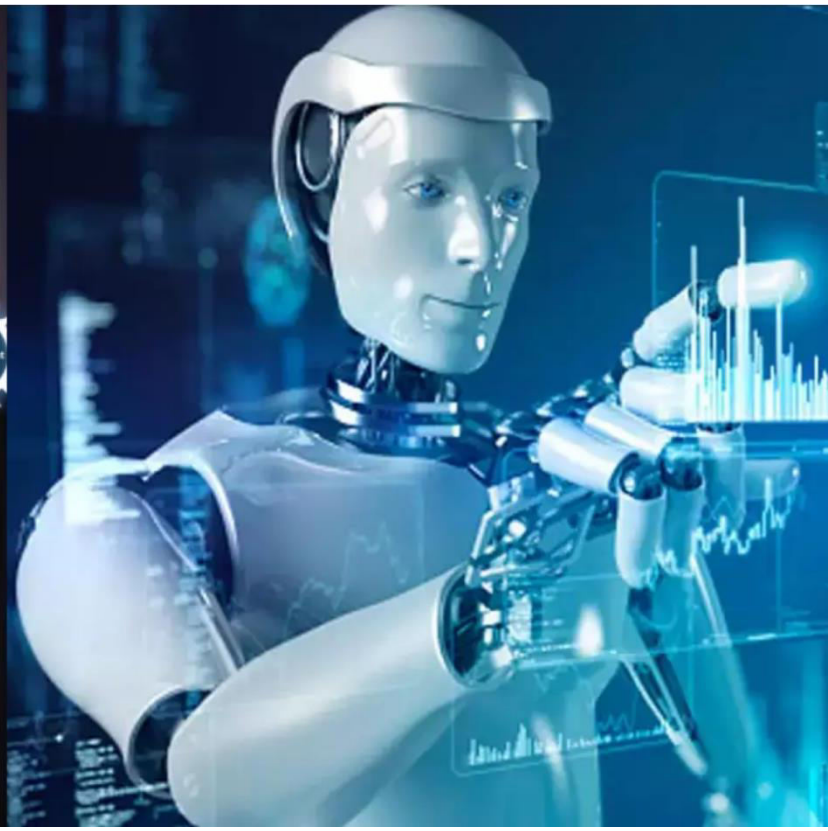
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

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



Impact Factor: 9.935

Volume 15, Issue 5, May 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

AI-Based Digital Identity Verification System

D.Manikanda Prabu ME (PHD) [1], S.Rohini[2], Bharathi R[3], Dinesh S[4], Kathiravan S[5], Monish S[6]

Assistant Professor & Project Coordinator, Department of Information Technology, Gnanamani College of Technology, Pachal, Namakkal, Tamil Nadu, India[1]

Assistant Professor & Team Guide, Department of Information Technology, Gnanamani College of Technology, Pachal, Namakkal, Tamil Nadu, India[2]

U.G. Student, Department of Information Technology, Gnanamani College of Technology, Pachal, Namakkal, Tamil Nadu, India[3456]

ABSTRACT: Digital identity verification has become an essential requirement in modern online ecosystems, where secure and reliable user authentication is critical for preventing fraud and maintaining trust. This paper presents an AI-based digital identity verification system that integrates intelligent document analysis and biometric validation to automate the authentication process. The proposed framework employs Optical Character Recognition (OCR) techniques to accurately extract personal information from government-issued identity documents. Simultaneously, facial recognition algorithms are used to compare the document image with a live user capture for effective identity matching.

To enhance security, the system incorporates anomaly detection mechanisms capable of identifying forged documents and detecting inconsistencies in extracted data. Machine learning models are utilized to adapt to diverse document formats and varying image qualities, thereby ensuring robustness and reliability in real-world environments. The proposed solution significantly reduces manual intervention and processing time while improving verification accuracy, scalability, and operational efficiency.

The framework is particularly suitable for applications in banking, e-commerce, healthcare, and digital service platforms, where secure onboarding and regulatory compliance are essential. Furthermore, the system supports real-time decision-making through optimized processing pipelines and secure data handling practices, ensuring user privacy and compliance with international data protection standards. The proposed approach also enables seamless integration with existing digital platforms through flexible APIs, improving adaptability and deployment efficiency across dynamic technological environments.

KEYWORDS: Artificial Intelligence, Digital Identity Verification, Optical Character Recognition, Facial Recognition, Fraud Detection, Authentication Systems.

I. INTRODUCTION

The rapid expansion of digital platforms and online services has significantly increased the demand for secure and reliable identity verification systems. As organizations continue to adopt digital transformation strategies, accurate user authentication has become essential for maintaining trust, preventing fraud, and ensuring secure access to online services. Traditional identity verification methods, which primarily depend on manual document inspection and physical verification procedures, are often time-consuming, error-prone, and vulnerable to fraudulent activities. These limitations create major challenges for sectors such as banking, e-commerce, healthcare, telecommunications, and digital governance, where security and user trust are critical.

Recent advancements in artificial intelligence (AI) have introduced new possibilities for improving the efficiency and reliability of digital identity verification systems. AI-based solutions enable the automated processing of identity documents and biometric information, reducing human intervention while improving consistency and accuracy in authentication. Technologies such as Optical Character Recognition (OCR) allow systems to extract textual information from identity documents and convert it into machine-readable data. This capability minimizes manual data entry errors and accelerates verification workflows.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

In addition to document analysis, biometric authentication has become a key component of modern identity verification systems. Facial recognition techniques powered by deep learning algorithms enable the comparison of a live user image with the photograph available on official identity documents. This process strengthens authentication by ensuring that the individual presenting the document is its legitimate owner. The integration of document analysis and biometric verification creates a multi-layered authentication framework that enhances security and reliability.

Another important challenge in digital identity verification is the growing sophistication of identity fraud. Fraudsters increasingly use forged documents, manipulated images, and stolen identities to gain unauthorized access to digital platforms. AI-driven fraud detection models can identify anomalies, detect inconsistencies, and recognize suspicious patterns in real time, thereby reducing the risk of identity theft and unauthorized transactions.

Furthermore, organizations require faster and more seamless onboarding processes to improve user experience without compromising security. Automated AI-based identity verification systems address this need by enabling rapid processing, scalability, and adaptability to different document types and formats. These systems support efficient onboarding while maintaining high verification accuracy.

Overall, the integration of artificial intelligence into digital identity verification represents a transformative approach to addressing modern authentication challenges. AI-based systems not only improve accuracy, efficiency, and scalability but also contribute to building a secure and trustworthy digital environment for users and organizations.

1.2 Importance of the Study

The importance of this study lies in addressing the increasing demand for secure, efficient, and reliable identity verification in modern digital environments. With the rapid growth of online services and digital transactions, traditional verification methods are no longer sufficient to handle large-scale authentication requirements. This study demonstrates how artificial intelligence can enhance digital identity verification by introducing automation, accuracy, scalability, and real-time decision-making capabilities.

One of the major contributions of this study is the improvement of security in digital platforms. Identity fraud, cyberattacks, and unauthorized access have become major concerns for organizations and users. By integrating intelligent document analysis and biometric authentication, the proposed system reduces the risk of identity theft and strengthens trust in online services.

The study also contributes to improving operational efficiency. Manual verification processes are often slow, labor-intensive, and prone to human error. The proposed AI-based framework automates data extraction and identity validation, thereby reducing processing time and minimizing the workload of human operators. This is especially beneficial for industries that handle large-scale customer onboarding.

Another important aspect is the enhancement of user experience. A fast and seamless verification process improves customer satisfaction and encourages the adoption of digital services. By reducing delays and simplifying authentication procedures, the proposed system supports efficient and user-friendly onboarding.

Furthermore, the study contributes to technological advancement by demonstrating the practical application of AI techniques in real-world identity verification systems. The findings of this research can support future developments in secure digital authentication technologies and intelligent fraud prevention systems.

1.3 Problem Statement

The rapid adoption of digital platforms has created a growing need for secure and efficient identity verification systems. However, many existing verification approaches still depend on manual processes and basic digital validation methods that are often slow, inconsistent, and vulnerable to human error. These traditional systems struggle to process large volumes of verification requests efficiently, leading to delays in user onboarding and reduced operational performance.

Another major challenge is the increasing sophistication of identity fraud and cyber threats. Fraudsters exploit weaknesses in conventional verification systems by using forged documents, manipulated images, and stolen identities to gain unauthorized access. Many current systems lack advanced capabilities to accurately detect such fraudulent activities, resulting in security breaches, financial losses, and compromised user data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

In addition, variations in identity document formats and image quality create difficulties in accurate information extraction and verification. Low-resolution images, poor lighting conditions, and damaged documents can negatively affect the performance of conventional verification methods. These issues often lead to incorrect authentication results and reduced user satisfaction.

Furthermore, many existing systems rely on single-layer authentication methods without integrating document verification and biometric validation. Such approaches are insufficient for ensuring strong security in sensitive sectors such as banking, healthcare, and digital financial services.

Therefore, there is a need for an intelligent, automated, and scalable digital identity verification system that can accurately extract information, perform biometric authentication, detect fraudulent activities, and provide secure real-time verification.

1.4 Aim and Objectives

The primary aim of this study is to develop an AI-based digital identity verification system that provides secure, accurate, and efficient user authentication for online platforms. The proposed system is designed to overcome the limitations of traditional verification methods through intelligent automation and advanced analytical techniques.

The objectives of the study are as follows:

- To develop an automated document verification system using Optical Character Recognition (OCR) for extracting personal information from government-issued identity documents.
- To implement facial recognition techniques for comparing identity document images with live user captures to ensure reliable biometric authentication.
- To integrate fraud detection mechanisms capable of identifying forged documents, manipulated images, and suspicious activities.
- To improve verification speed and operational efficiency through real-time processing and automated decision-making.
- To design a scalable and adaptable system capable of supporting multiple document formats and handling large-scale verification requests.
- To ensure secure handling of personal and biometric data while maintaining compliance with privacy and security standards.

Overall, the study aims to create a robust, intelligent, and user-friendly identity verification framework suitable for modern digital applications.

1.5 Scope and Limitations of the Study

The scope of this study focuses on the design and implementation of an AI-based digital identity verification system for secure online authentication. The proposed framework integrates Optical Character Recognition (OCR) for extracting textual information from identity documents and facial recognition techniques for biometric validation. The system is intended to support multiple identity documents, including national identity cards, passports, and driver's licenses, thereby providing flexibility for various real-world applications.

The study also includes the development of fraud detection mechanisms to identify forged or tampered documents, detect inconsistencies in user information, and prevent identity misuse. In addition, the framework emphasizes real-time processing capabilities to support faster user onboarding while maintaining security and accuracy. Scalability is another important aspect of the study, enabling the system to process large numbers of verification requests efficiently. The proposed system is also designed for integration with existing digital platforms through APIs and cloud-based deployment models.

Despite its broad scope, the study has certain limitations. One limitation is the dependency on the quality of input data. Poor image resolution, improper lighting conditions, and damaged documents can affect the accuracy of OCR and facial recognition processes. Variations in document formats, languages, and regional standards may also require additional model training and customization.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

Another limitation involves privacy and data security concerns. Since the system processes sensitive personal and biometric information, strict compliance with legal and regulatory requirements is necessary. Ensuring secure data storage, transmission, and processing increases implementation complexity.

In addition, the system may face challenges in detecting highly sophisticated fraud techniques such as deepfake images and advanced document forgeries, which continue to evolve over time. The deployment of AI models may also require significant computational resources and infrastructure, potentially increasing operational costs.

II. LITERATURE SURVEY

1. TrustNet: Decentralised Identity Verification & Management System

This study presents a decentralized identity verification framework designed to enhance user control over personal data and reduce dependency on centralized authorities. The proposed system leverages distributed ledger technology to create a secure and tamper-resistant identity management environment. It focuses on enabling users to store and manage their identity credentials independently while ensuring authenticity and integrity through cryptographic techniques. The system incorporates smart contracts to automate verification processes and enforce trust among participating entities. It also emphasizes privacy by allowing selective disclosure of identity attributes, ensuring that only necessary information is shared during verification. The architecture is designed to be scalable and adaptable, supporting multiple use cases across industries. Additionally, the study highlights improved transparency and reduced risk of data breaches due to decentralization. By eliminating single points of failure, the system enhances resilience against cyberattacks. The proposed approach demonstrates the potential of decentralized identity systems in transforming traditional verification models, offering a secure, user-centric, and efficient solution for digital identity management in modern applications.

2. IVBlock: A Blockchain-Based Digital Identity Verification System

This paper introduces a blockchain-based identity verification system that aims to provide secure and transparent authentication mechanisms. The system utilizes blockchain technology to store identity records in an immutable and distributed manner, ensuring data integrity and preventing unauthorized modifications. It incorporates cryptographic hashing and consensus mechanisms to validate identity transactions across the network. The framework is designed to reduce reliance on centralized verification authorities, thereby minimizing risks associated with data breaches and single points of failure. The study also explores the use of smart contracts to automate identity verification processes, enabling faster and more efficient operations. Privacy is maintained through controlled access to user data, ensuring that sensitive information is shared only with authorized entities. The system supports interoperability, allowing integration with various digital platforms and services. Additionally, the research highlights improved trust among users and service providers due to transparent verification procedures. Overall, the proposed model demonstrates how blockchain technology can enhance security, reliability, and efficiency in digital identity verification systems.

3. A Hybrid Blockchain Framework for Secure, Scalable, and Energy-Efficient Digital Identity Management with Token-based Selective Disclosure

This research proposes a hybrid blockchain-based framework aimed at achieving secure and scalable digital identity management while addressing energy efficiency concerns. The system combines public and private blockchain architectures to balance transparency and performance. It introduces a token-based selective disclosure mechanism that allows users to share only specific identity attributes, preserving privacy while ensuring verification accuracy. The framework integrates cryptographic techniques to secure identity data and prevent unauthorized access. It also focuses on reducing computational overhead by optimizing consensus mechanisms, making the system more energy-efficient compared to traditional blockchain models. The study emphasizes scalability, enabling the system to handle large volumes of identity transactions without compromising performance. Additionally, it supports interoperability across different platforms, enhancing its applicability in diverse domains. The proposed solution demonstrates improved data security, user privacy, and operational efficiency. By combining multiple blockchain approaches, the framework provides a balanced and effective solution for modern digital identity management challenges.

4. Secure Digital Identity using Non-Fungible Tokens

This study explores the use of non-fungible tokens (NFTs) for secure digital identity management. The proposed system leverages blockchain technology to create unique and verifiable identity tokens that represent individual user identities. Each NFT is associated with specific identity attributes, ensuring authenticity and preventing duplication.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

The system focuses on decentralization, allowing users to have full control over their identity data without relying on centralized authorities. It incorporates cryptographic techniques to secure identity information and ensure data integrity. The use of NFTs enables traceability and transparency, allowing verification processes to be conducted efficiently. The study also highlights the potential for integrating identity tokens with various digital platforms, enhancing interoperability and usability. Privacy is maintained by allowing selective sharing of identity attributes, ensuring that sensitive information is protected. The proposed approach demonstrates how emerging technologies like NFTs can be utilized to create secure and innovative identity management solutions, addressing challenges related to data security, ownership, and trust.

5. Decentralized Digital Identity Verification System Using Blockchain Technology

This paper presents a decentralized approach to digital identity verification using blockchain technology. The system aims to eliminate the need for centralized authorities by distributing identity data across a secure and transparent network. It utilizes cryptographic algorithms to ensure data integrity and prevent unauthorized access. The framework supports user-controlled identity management, allowing individuals to store and share their credentials securely. The study also incorporates smart contracts to automate verification processes, improving efficiency and reducing processing time. Privacy is a key focus, with mechanisms for controlled data sharing and protection against misuse. The system is designed to be scalable and adaptable, supporting various applications across industries. Additionally, it enhances trust among users and service providers by providing verifiable and tamper-proof identity records. The research highlights the potential of blockchain technology in transforming traditional identity verification systems into more secure, transparent, and user-centric solutions.

6. Securing Legal Identity for Third-Gender Individuals Using Distributed Ledger-Based Verification Systems

This study focuses on addressing identity verification challenges faced by third-gender individuals through a distributed ledger-based system. The proposed framework aims to provide secure and inclusive identity management by leveraging blockchain technology. It ensures that identity records are stored in a tamper-proof and transparent manner, reducing the risk of discrimination and data manipulation. The system emphasizes privacy and user control, allowing individuals to manage their identity information securely. It incorporates cryptographic techniques to protect sensitive data and ensure authenticity. The study also highlights the importance of inclusivity in digital identity systems, ensuring that marginalized communities have access to secure verification mechanisms. The framework supports interoperability, enabling integration with various digital services. By addressing social and technical challenges, the proposed system contributes to creating a more equitable and secure digital identity ecosystem, promoting trust and accessibility for all users.

7. Remote Identity Proofing System

This paper presents a remote identity proofing system designed to enable secure identity verification without physical presence. The system integrates document verification and biometric authentication to ensure reliable user identification. It utilizes advanced image processing techniques to extract and validate information from identity documents. Additionally, facial recognition is employed to compare user images with document photographs, enhancing verification accuracy. The system is designed to operate in real-time, providing quick and efficient authentication results. Security is ensured through encryption and secure data transmission protocols. The study also addresses challenges related to remote verification, such as image quality and fraud detection. It incorporates mechanisms to detect spoofing attempts and ensure the authenticity of user inputs. The proposed solution demonstrates the feasibility of remote identity verification, offering a convenient and secure alternative to traditional in-person methods, particularly in digital and online service environments.

8. Gryphon Digital Identity Management System with Hyperledger Fabric

This research introduces a digital identity management system built on Hyperledger Fabric, supporting decentralized identifiers and verifiable credentials. The system aims to provide a secure and scalable platform for managing digital identities in a decentralized environment. It leverages blockchain technology to ensure data integrity and transparency while maintaining user privacy. The framework supports the issuance and verification of digital credentials, enabling efficient and trustworthy identity validation. It incorporates cryptographic techniques to secure data and prevent unauthorized access. The system is designed to be interoperable, allowing integration with various applications and services. Additionally, it emphasizes scalability, ensuring that the platform can handle large volumes of identity transactions. The study highlights the advantages of using Hyperledger Fabric for enterprise-level identity management, providing a robust and flexible solution for modern digital ecosystems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

9. Enhancing Decentralized Identity Management with Zero-Knowledge Proofs for Selective Disclosure
This study explores the use of zero-knowledge proofs to enhance privacy in decentralized identity management systems. The proposed approach allows users to verify their identity without revealing sensitive information, ensuring confidentiality and data protection. It integrates cryptographic techniques to enable selective disclosure of identity attributes, allowing only necessary information to be shared. The system is built on a decentralized architecture, ensuring data integrity and resistance to tampering. The study highlights the importance of privacy-preserving technologies in modern identity systems, addressing concerns related to data misuse and unauthorized access. It also demonstrates the potential of zero-knowledge proofs in improving trust and security in digital interactions. The proposed solution offers a balance between transparency and privacy, making it suitable for various applications in digital identity verification.

10. Zero-Knowledge Proof Algorithm for Blockchain-Based Identity Verification Systems
This paper presents a zero-knowledge proof algorithm designed to enhance security and privacy in blockchain-based identity verification systems. The algorithm enables users to prove their identity without disclosing actual data, reducing the risk of information leakage. It integrates with blockchain technology to ensure data integrity and transparency while maintaining confidentiality. The system focuses on improving verification efficiency and reducing computational overhead. It also addresses challenges related to scalability and performance, ensuring that the system can handle large volumes of transactions. The study highlights the potential of combining cryptographic techniques with blockchain to create secure and privacy-preserving identity verification solutions. The proposed algorithm demonstrates improved security and user trust, making it a valuable contribution to the development of advanced digital identity systems

III. METHODOLOGY

A. Existing System

Existing digital identity verification systems mainly rely on manual inspection and basic automated techniques for user authentication. These systems commonly use Optical Character Recognition (OCR) to extract textual information from identity documents and simple image-matching methods for verification. However, their performance is often affected by poor image quality, document variations, and inconsistent lighting conditions. Most existing approaches also depend on rule-based fraud detection mechanisms, which are limited in identifying advanced fraudulent activities such as forged documents and manipulated images. Additionally, manual review processes increase verification time and reduce scalability, making these systems less effective for large-scale digital platforms. Therefore, there is a need for more intelligent, automated, and secure AI-driven identity verification solutions.

B. Proposed System

The proposed system introduces an AI-based digital identity verification framework designed to deliver secure, accurate, and efficient user authentication in modern digital environments. It integrates advanced technologies such as Optical Character Recognition and deep learning-based facial recognition to automate the verification process. The system begins by capturing identity document images and extracting relevant personal information using intelligent text recognition techniques. This extracted data is then structured and validated to ensure correctness and completeness.
Simultaneously, the system captures a live image or video of the user and performs biometric verification by comparing it with the photograph present on the identity document. This multi-layered approach enhances reliability by ensuring both document authenticity and user identity. The proposed model also incorporates machine learning algorithms for fraud detection, enabling it to identify anomalies such as forged documents, mismatched data, or suspicious patterns in real time.

To improve performance, the system is designed with optimized processing pipelines that support real-time verification and quick decision-making. It is scalable and adaptable, allowing it to handle large volumes of requests and support various document formats and regional variations. The architecture also ensures secure data handling through encryption and compliance with privacy standards, making it suitable for sensitive applications such as banking and digital services.

Overall, the proposed system provides a comprehensive and intelligent solution that minimizes manual effort, enhances accuracy, and strengthens security. It aims to create a seamless and trustworthy verification experience while addressing the limitations of traditional systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

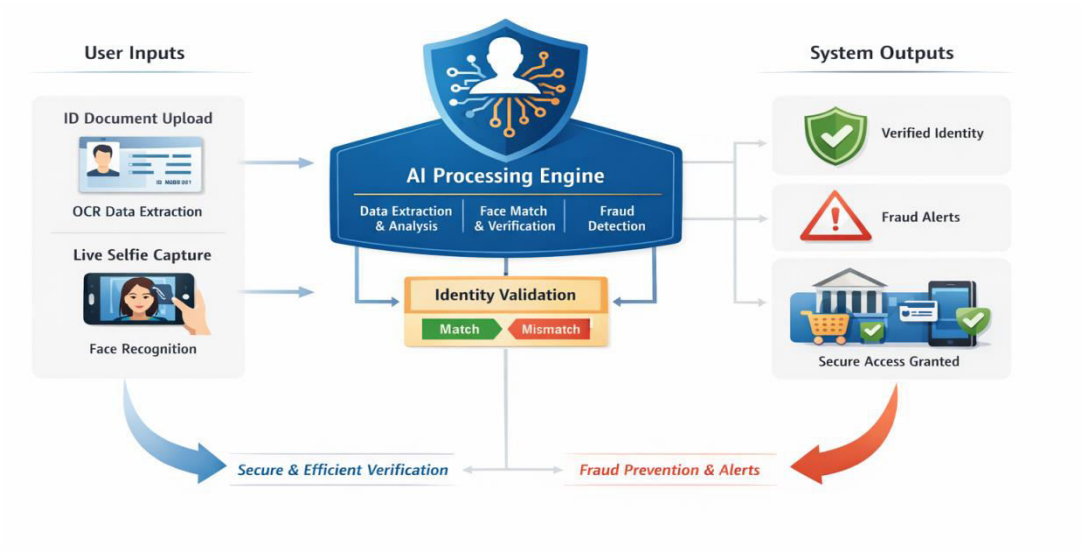
Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

C. SYSTEM ARCHITECTURE



IV. MODULE DESCRIPTION

1. User Registration Module
The User Registration Module collects essential user details and creates a secure profile for identity verification. It validates input data, supports email or mobile authentication, and ensures secure storage of user information using encryption techniques. The module provides a user-friendly interface and acts as the foundation for the verification process.

2. ID Document Upload Module
The ID Document Upload Module allows users to securely upload government-issued identity documents such as ID cards, passports, and driving licenses. It verifies file quality, format, and clarity to ensure accurate processing. The module also protects uploaded data through secure transmission and storage mechanisms.

3. OCR Data Extraction Module
The OCR Data Extraction Module automatically extracts textual information from uploaded documents using Optical Character Recognition techniques. It identifies important fields such as name, date of birth, and ID number while improving accuracy through image preprocessing and validation methods.

4. Live Selfie Capture Module
The Live Selfie Capture Module captures real-time facial images from users for biometric verification. It ensures proper image quality and may include liveness detection techniques to prevent spoofing attacks. The module supports secure handling of captured facial data.

5. Face Recognition Module
The Face Recognition Module compares the user's live facial image with the photo available on the uploaded identity document. Using deep learning algorithms, it performs accurate biometric matching while handling variations in lighting, pose, and facial expressions.

6. Fraud Detection Module
The Fraud Detection Module identifies suspicious activities, forged documents, and inconsistencies using machine learning techniques. It analyzes document authenticity, biometric mismatches, and unusual behavior patterns to prevent identity fraud and unauthorized access.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

7. Identity Verification Module

The Identity Verification Module integrates results from OCR, facial recognition, and fraud detection modules to validate the authenticity of a user's identity. It ensures consistency across all verification layers and generates reliable authentication outcomes.

8. Decision and Alert Module

The Decision and Alert Module produces the final verification result by categorizing users as verified, rejected, or requiring further review. It also generates alerts for suspicious activities and maintains logs for security monitoring and compliance purposes..

V. EXPERIMENTAL RESULTS

RESULT

The implementation of the AI-based digital identity verification system demonstrates significant improvements in accuracy, efficiency, and security compared to traditional verification approaches. The system successfully integrates document analysis, biometric authentication, and fraud detection into a unified framework, enabling automated and reliable identity validation. The Optical Character Recognition component effectively extracts relevant textual information from various types of identity documents, maintaining high precision even under moderate variations in image quality and format. This reduces dependency on manual data entry and minimizes associated errors.

The facial recognition module produces consistent and accurate matching results by analyzing facial features and generating similarity scores. It effectively handles variations in lighting, orientation, and expression, ensuring reliable biometric verification. The integration of liveness detection further strengthens the system by preventing spoofing attempts using static images or pre-recorded media. Additionally, the fraud detection component identifies inconsistencies and suspicious patterns, contributing to improved system security and reduced risk of identity misuse.
The system demonstrates efficient processing capabilities, enabling real-time or near real-time verification outcomes. This significantly enhances user onboarding experiences by reducing waiting time and simplifying the verification process. The modular architecture ensures scalability, allowing the system to handle increased workloads without performance degradation. Furthermore, secure data handling mechanisms protect sensitive user information, ensuring compliance with privacy standards.

Overall, the results indicate that the proposed system achieves a high level of reliability and effectiveness in digital identity verification. It successfully addresses the limitations of existing systems by providing a comprehensive, automated, and intelligent solution suitable for modern digital applications.

DISCUSSION

The findings of this study demonstrate the effectiveness of integrating artificial intelligence into digital identity verification systems. The combination of document analysis, facial recognition, and fraud detection provides a multi-layered verification approach that improves accuracy, reliability, and security. The results indicate that automation significantly reduces processing time and manual intervention, making the system suitable for large-scale applications.
The study also highlights the system's adaptability to different document formats and varying image qualities. Machine learning techniques enable continuous improvement and help the system respond to evolving fraud methods. In addition, the proposed framework achieves a balance between security and user convenience by offering a fast and user-friendly verification process without compromising authentication standards.

However, certain challenges remain, including dependence on input data quality, privacy concerns, and regulatory compliance requirements. Poor image resolution or incomplete information may affect verification accuracy. Despite these limitations, the proposed AI-based system provides a robust, scalable, and efficient solution for modern digital identity verification and represents a significant advancement in secure online authentication.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

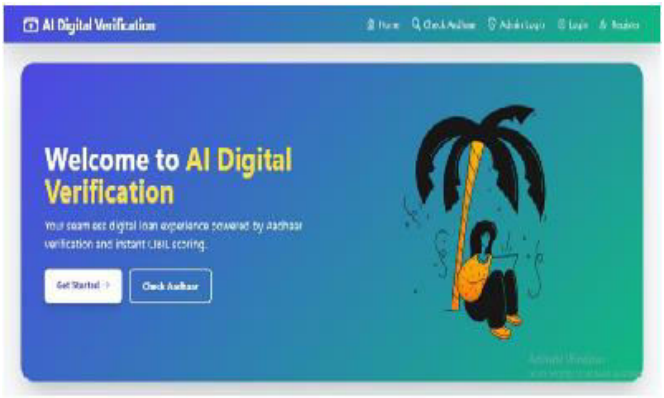
Impact Factor 9.935

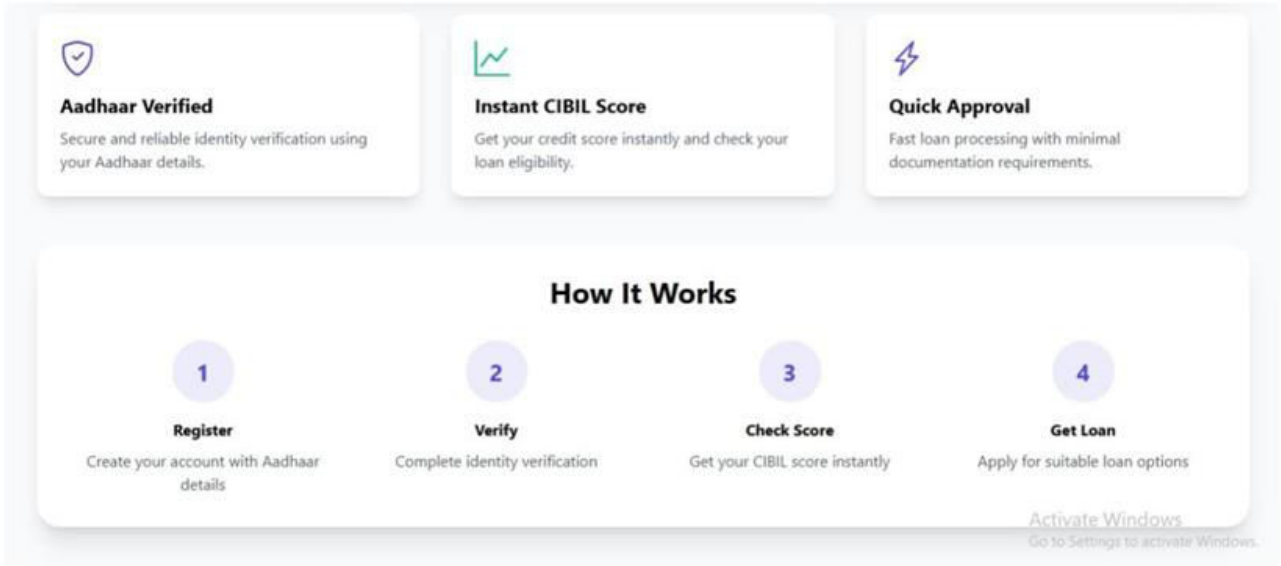
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

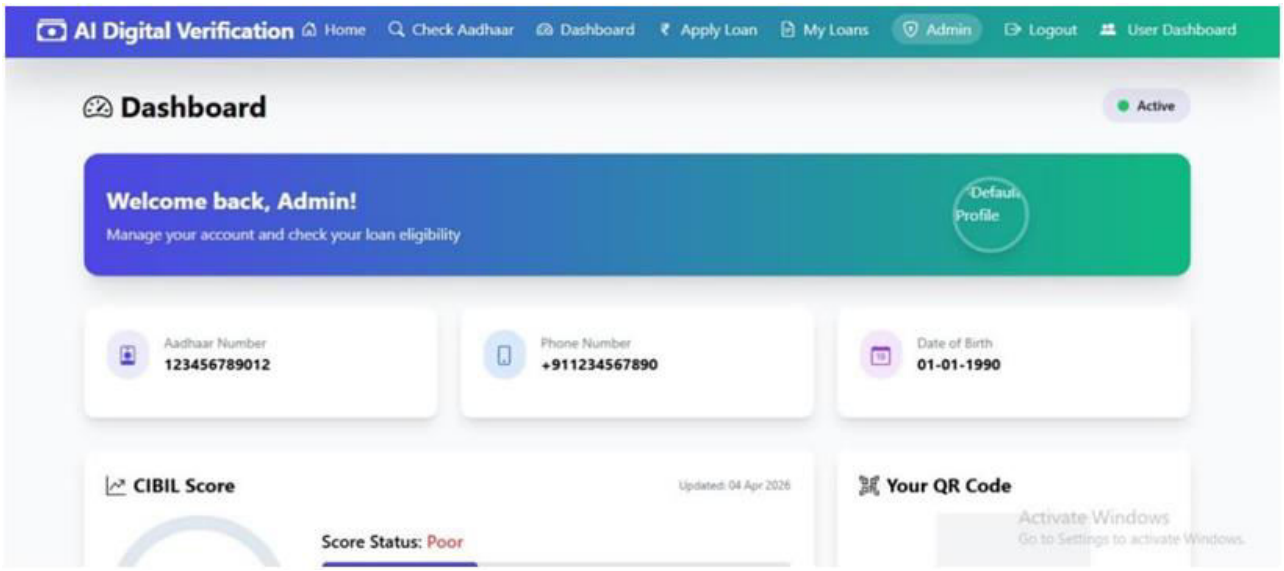
Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

OUTPUT







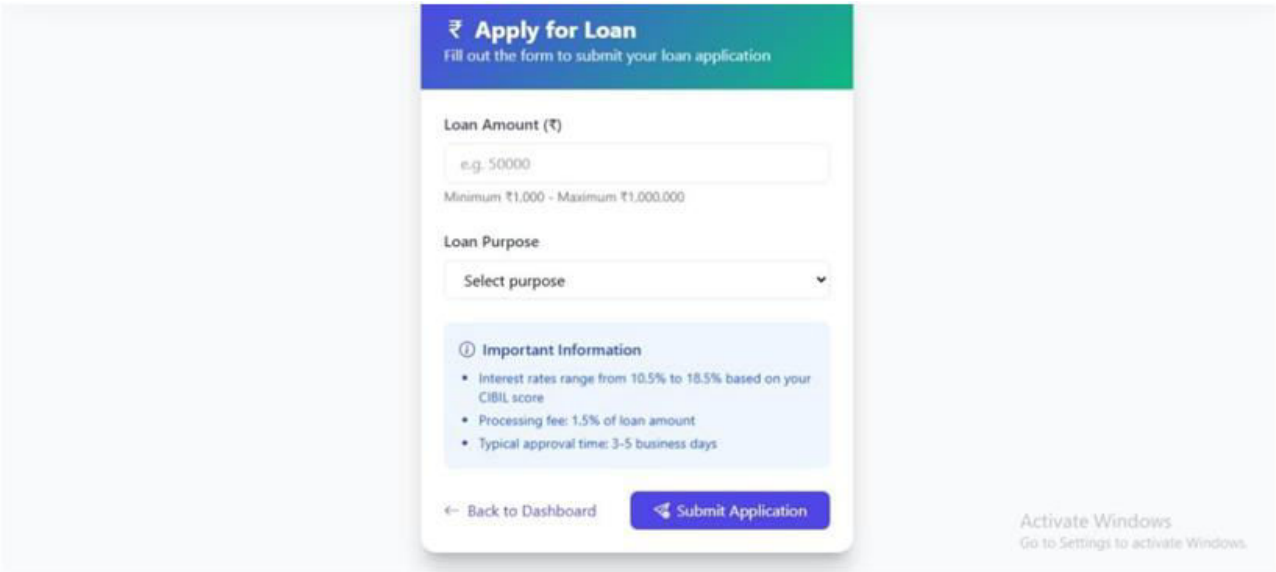
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

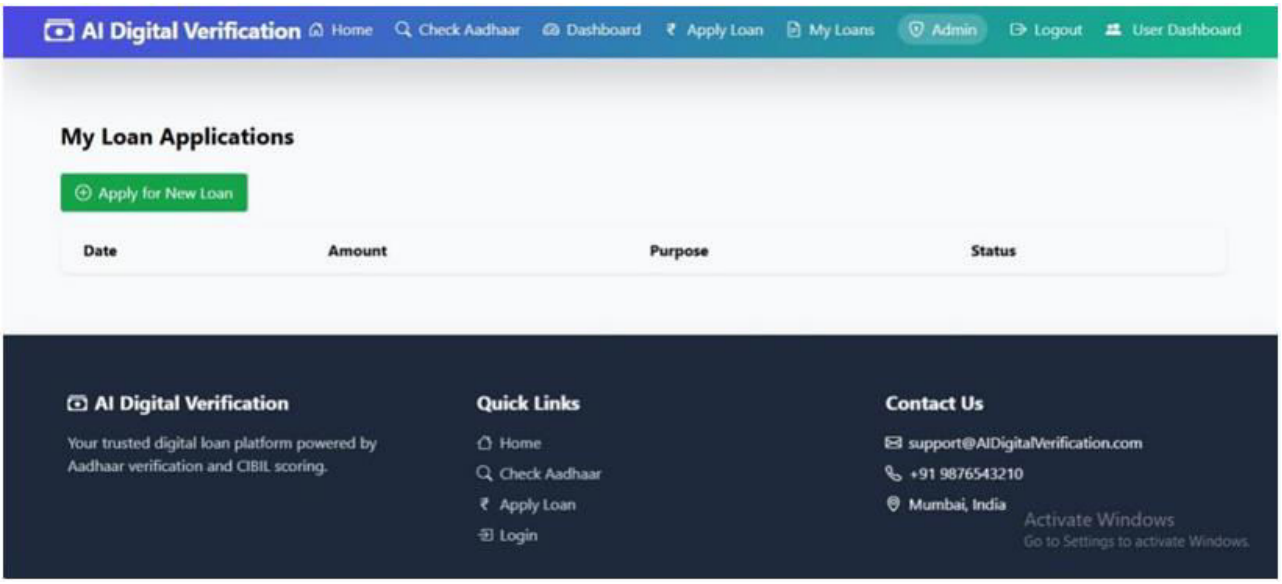
Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|





VI. CONCLUSION

The AI-based digital identity verification system proposed in this study provides a secure, reliable, and efficient solution for modern authentication challenges. By integrating Optical Character Recognition (OCR), facial recognition, and intelligent fraud detection techniques, the system enhances the accuracy and automation of identity verification processes. It effectively overcomes the limitations of traditional methods by reducing manual effort, minimizing processing delays, and improving decision-making consistency.

The multi-layered verification approach strengthens security by combining document validation, biometric authentication, and fraud detection mechanisms. Machine learning models further improve system adaptability by handling different document formats, image qualities, and evolving fraud patterns. In addition, the framework supports real-time processing and scalability, making it suitable for large-scale applications such as banking, e-commerce, healthcare, and digital services.

The study also emphasizes secure data handling and privacy protection to ensure responsible management of sensitive user information. Although challenges such as input data quality and regulatory compliance remain, the overall system

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 9.935

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 5, May 2026

|DOI: 10.15680/IJIRSET.2026.1505154|

demonstrates strong performance in providing accurate and trustworthy identity verification. Therefore, the proposed AI-based framework represents a significant advancement in digital authentication by offering a scalable, intelligent, and secure solution for modern digital ecosystems.

VII. FUTURE ENHANCEMENT

Future enhancements of the proposed AI-based digital identity verification system include integrating advanced deep learning models, multimodal biometric authentication, and improved liveness detection techniques to strengthen security and accuracy. Future work can also focus on faster real-time processing using cloud and edge computing technologies. Enhancing data privacy, regulatory compliance, and user experience through secure encryption and intuitive interfaces will further improve system reliability. Additionally, continuous updates to fraud detection models will help the system adapt to evolving cyber threats and emerging fraud techniques.

REFERENCES

[1] P. Diwan, T. Kashyap, A. K. Badhan, M. Sai Painkra, S. Maurya and P. Agrawal, "TrustNet: Decentralised Identity Verification & Management System," 2025 4th OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 5.0, Raigarh, India, 2025, pp. 1-5, doi: 10.1109/OTCON65728.2025.11071164.

[2] P. Budhathoki, G. Upreti, M. Giri, A. Yadav and S. Noor, "IVBlock: A Blockchain-Based Digital Identity Verification System," SoutheastCon 2025, Concord, NC, USA, 2025, pp. 631-636, doi: 10.1109/SoutheastCon56624.2025.10971644.

[3] V. M, S. C. K, G. Maya, R. Ramya, R. Kanimozhi and S. I. A. Lathif, "A Hybrid Blockchain Framework for Secure, Scalable, and Energy-Efficient Digital Identity Management with Token-based Selective Disclosure," 2025 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2025, pp. 930-937, doi: 10.1109/ICEARS64219.2025.10940179.

[4] J. Agarkhed, S. S. Patil, S. Y. Raza and V. Patil, "Secure Digital Identity using Non-Fungible Tokens," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 1196-1201, doi: 10.1109/ICIRCA57980.2023.10220854.

[5] V. Nehra, A. MJ, H. Khanna and N. Jindal, "Decentralized Digital Identity Verification System Using Blockchain Technology," 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM), Noida, India, 2024, pp. 1-6, doi: 10.1109/ICIPTM59628.2024.10563665.

[6] M. S. Srivastava, R. K. Pandey, R. Singh, D. B. Gautam and K. Fatima, "Securing Legal Identity for Third-Gender Individuals Using Distributed Ledger-Based Verification Systems," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 1048-1053, doi: 10.1109/IC3ET64989.2026.11467284.

[7] M. Waliyullah and R. K. Moloo, "Remote identity proofing system," 2025 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bengaluru, India, 2025, pp. 1-6, doi: 10.1109/CONECCT65861.2025.11306528.

[8] A. Neri, I. Onea, M. Pânzariu, M. Frânculescu, R. Kromes and Z. Erkin, "Demo: Gryphon Digital Identity Management System with Hyperledger Fabric, Compatible with Decentralized Identifiers and Verifiable Credentials*," 2025 7th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Zurich, Switzerland, 2025, pp. 1-3, doi: 10.1109/BRAINS67003.2025.11302904.

[9] M. Ramya, B. S. Anuvarshini, G. Kanika, A. Lohith and B. Barath, "Enhancing Decentralized Identity Management with Zero-Knowledge Proofs for Selective Disclosure," 2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2025, pp. 727-732, doi: 10.1109/ICESC65114.2025.11212333.

[10] A. Nayak et al., "Zero-Knowledge Proof Algorithm for Blockchain-Based Identity Verification Systems," 2025 3rd International Conference on Cyber Resilience (ICCR), Dubai, United Arab Emirates, 2025, pp. 1-8, doi: 10.1109/ICCR67387.2025.11291870.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details