iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** I **Month of publication:** January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77187

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue I Jan 2026- Available at www.ijraset.com

NeuroDocs: AI Powered Document Analysis System

M. Krithika[1], U. Dhanya[2] , F. Evanjalin Jenifer[3] , P. Ilakkya[4] , R. Vaishnavi[5] , S. Yoga[6]
[1] *Lecturer, Department of Computer Engineering, PSG Polytechnic College*
[2, 3, 4, 5, 6] *Student, Department of Computer Engineering, PSG Polytechnic College*

Abstract: ***The rapid digitization of documents in banking, governance, and commercial environments has significantly increased the demand for intelligent document management systems that ensure security, usability, and authenticity. In the Indian context, users routinely manage sensitive documents such as bank statements, identity proofs, certificates, and invoices, which require secure access, structured organization, multilingual understanding, and protection against fraudulent manipulation. Traditional document management systems largely focus on storage and retrieval while lacking intelligence-driven automation, regional language support, and fraud detection capabilities. This paper presents NeuroDocs, a comprehensive document analysis platform that integrates secure authentication, automated document organization, multilingual document highlighting and translation, and scam and fraud detection. The system employs OTP-based secure authentication for user access, OCR-based text extraction for document understanding, rule-based automated foldering, neural machine translation for English, Tamil, and Hindi languages, and computer vision–based seal verification for fraud detection. NeuroDocs is implemented using a React-based frontend, Node.js backend, MongoDB database, and Python-based AI services. Experimental evaluation on real-world Indian documents demonstrates improved document organization efficiency, enhanced accessibility for regional language users, and effective identification of potentially suspicious documents. The proposed system provides a practical, scalable, and secure solution for intelligent document management.***

Keywords: Document Analysis, Secure Authentication, OCR, Multilingual Translation, Fraud Detection.

I. INTRODUCTION

The increasing adoption of digital technologies has significantly transformed the manner in which documents are created, stored, shared, and accessed across multiple sectors including banking, government administration, education, and commerce. In the Indian context, citizens routinely interact with digital documents such as bank statements, Aadhaar cards, land records, educational certificates, and commercial invoices. While digitization enhances accessibility, portability, and operational efficiency, it simultaneously introduces a range of technical and security-related challenges that demand systematic solutions. One of the primary concerns associated with digital document usage is secure access control. Personal and financial documents contain highly sensitive information, and unauthorized access can lead to identity theft, financial fraud, and serious privacy violations. Conventional username-password authentication mechanisms are often insufficient to prevent such risks, particularly when credentials are compromised. In addition to security issues, efficient organization of digital documents remains a major challenge. Users are typically required to manually sort and label documents, a process that is time-consuming, error-prone, and inconsistent, especially when managing large volumes of files. Language diversity further affects the usability of digital documents in India. A significant portion of official and financial documents are issued primarily in English, which creates comprehension difficulties for users who are more comfortable with regional languages. This linguistic barrier limits effective understanding and utilization of important information, particularly among rural and non-English-speaking populations. Furthermore, the growing prevalence of document forgery and digital scams, including the use of fake seals, manipulated certificates, and altered records, has increased the need for automated document verification mechanisms. Manual verification processes are often slow and unreliable, making users vulnerable to fraudulent activities. Most existing document management systems focus on basic functionalities such as file storage and retrieval, offering limited automation and intelligence. These systems typically lack integrated security measures, automated organization, multilingual accessibility, intelligent user interaction, and fraud detection capabilities within a single framework. As a result, users are often required to rely on multiple fragmented tools, leading to inefficiency and reduced trust.

II. SYSTEM DESIGN

NeuroDocs is designed as a modular, extensible, and service-oriented system in which each functional component operates independently while seamlessly integrating with the overall platform. This modular design approach improves scalability, maintainability, fault isolation, and clarity of operation by clearly separating system responsibilities. Each module is assigned a specific functional role and communicates with other modules through secure, well-defined interfaces, ensuring reliable data exchange and controlled interaction between components.

©IJRASET: All Rights are Reserved

Such separation of concerns allows updates, enhancements, or bug fixes to be applied to individual modules without adversely affecting the operation of the entire system. The modular architecture also enables efficient handling of increasing document volumes and concurrent user interactions, which is essential for real-world deployment scenarios. As system usage grows, individual modules can be optimized, scaled, or deployed independently based on workload requirements and performance demands. By segregating key functionalities such as secure authentication, document processing, multilingual services, and fraud detection into distinct modules, NeuroDocs achieves improved performance optimization, simplified debugging, and easier long-term maintenance. This design philosophy enhances system robustness and flexibility while allowing future extensions and integration of additional features, making NeuroDocs adaptable to evolving user needs and deployment environments.

A. Secure Authentication and User Management Module

The Secure Authentication and User Management Module forms the foundational layer of the NeuroDocs platform by ensuring controlled, authenticated, and authorized access to user data and uploaded documents. This module manages user registration, secure login, session handling, access privileges, and monitoring of active user activity. During registration, users are required to provide a valid and active email address, which serves as a unique identifier within the system and enables secure communication. To enhance security beyond conventional username–password mechanisms, the system employs OTP-based email verification during the login process. Whenever a user initiates a login request, a dynamically generated One-Time Password is issued by the server and sent to the registered email address. The OTP is time-bound and valid only for a short duration, thereby minimizing the risk of replay attacks or unauthorized reuse. Access is granted only upon successful OTP verification, significantly reducing the risk of unauthorized entry even if credentials are compromised. Once authenticated, users are redirected to a personalized dashboard that acts as the central interface for all document-related operations. The dashboard provides access to document uploads, automatically categorized folders, multilingual translation features, and fraud detection results. Secure session tokens are generated and managed to ensure session integrity and prevent unauthorized access through session hijacking. Additionally, session activity is monitored to detect abnormal behavior and restrict access when necessary, thereby safeguarding user data. By integrating OTP verification, secure session management, and activity monitoring, this module establishes a strong foundation of trust, confidentiality, and data protection within the NeuroDocs platform.

B. Automated Document Organization Module

The Automated Document Organization Module constitutes the core document intelligence component of NeuroDocs and is responsible for categorizing uploaded documents in a structured and efficient manner. When a user uploads a document, the system initiates OCR-based text extraction to convert the document into machine-readable textual content. The extracted text is preprocessed to remove noise, normalize formatting, and eliminate irrelevant elements in order to improve analysis accuracy. Based on predefined keyword rules, structural patterns, and domain-specific indicators, the system analyzes the processed text to identify document characteristics. Keywords such as bank names, account numbers, transaction details, government identifiers, and invoice-related terms are used to classify documents. Using this rule-based approach, documents are automatically categorized into predefined folders such as Bank, Government, or Others. This strategy avoids reliance on complex machine learning models while ensuring transparency, interpretability, and consistent classification behavior. Automated document organization significantly reduces manual effort, minimizes human error, and enhances document retrieval efficiency for users.

C. Document Highlighting and Multilingual Translation Module

The Document Highlighting and Multilingual Assistance Module is designed to enhance document readability, comprehension, and accessibility for users with diverse linguistic backgrounds. The module analyzes the extracted document text to identify important elements such as names, dates, monetary values, document numbers, headings, and official terminology. These critical components are automatically highlighted in the user interface, enabling users to quickly locate key information without reading the entire document. Highlighting improves visual clarity and reduces cognitive effort, particularly when handling complex or lengthy official documents.To address linguistic diversity in India, the module provides multilingual assistance by supporting translation of selected content into Tamil, Malayalam, and Hindi. Translation is selectively applied to highlighted sections to preserve contextual accuracy and reduce the risk of misinterpretation of legal or technical terms. As part of multilingual assistance, the system also offers voice support by converting the translated content into speech, enabling users to listen to document information in their preferred language.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

This integrated text-to-speech functionality improves accessibility for users with reading difficulties and enhances inclusiveness. Users can access the original text, translated text, and corresponding voice output simultaneously, allowing effective cross-reference and improved understanding.

D. Scam and Fraud Detection Module

The Scam and Fraud Detection Module enhances document trustworthiness by identifying potential forgery, manipulation, or scam indicators. This module focuses primarily on verifying visual authenticity markers such as official seals and stamps, which are commonly present in government and financial documents. Uploaded document images are analyzed using AI-based image processing and computer vision techniques. The module detects seals and stamps and evaluates visual attributes including shape, size, position, clarity, alignment, and consistency with known authentic patterns. These features are examined to assess whether the seal appears genuine or suspicious. Documents that fail verification checks or exhibit irregularities are flagged as potentially fraudulent. Alerts and warnings are displayed prominently on the user dashboard, prompting users to exercise caution before relying on such documents. This module is particularly valuable for verifying government certificates, legal records, and financial documents where authenticity is critical.

III. SYSTEM ARCHITECTURE

The NeuroDocs system is designed using a three-tier architecture model to ensure scalability, security, and efficient processing of digital documents. The architecture separates the system into three distinct layers—presentation layer, application layer, and data layer—allowing each layer to perform specific responsibilities while interacting seamlessly with the others. This layered separation improves system maintainability, simplifies updates, enhances security, and enables future expansion without significant architectural changes

A. Presentation Layer

The presentation layer serves as the user-facing interface of the NeuroDocs platform and is responsible for all interactions between the user and the system. This layer is developed using React.js along with standard web technologies such as HTML, CSS, and JavaScript to provide a responsive, interactive, and user-friendly interface. The design ensures compatibility across desktop and mobile devices, enabling users to access the platform conveniently from different environments. Through the presentation layer, users can securely register and authenticate, upload documents, view automatically categorized folders, access highlighted document content, utilize multilingual translation and voice assistance features, and receive fraud detection alerts. Multilingual assistance allows users to view translated content in Tamil, English, and Hindi, while integrated voice support enables users to listen to translated document content, improving accessibility for users with limited reading proficiency. Input validation and secure communication mechanisms are implemented at the client side to prevent unauthorized actions and ensure safe interaction with backend services.

B. Application Layer

The application layer acts as the central control unit of the NeuroDocs system and serves as an intermediary between the presentation and data layers. This layer is implemented using Node.js and the Express framework, providing a scalable and efficient backend environment for handling system logic and API requests. It manages core functionalities such as OTP-based user authentication, session management, document upload handling, and access control.In addition, the application layer coordinates OCR processing, rule-based document classification, multilingual translation services, voice generation, and fraud detection workflows. Extracted document text is processed and analyzed within this layer to identify important information for highlighting and categorization. By separating business logic from the user interface, the application layer ensures that computationally intensive operations are handled efficiently without affecting system responsiveness. The modular design of this layer also allows future integration of advanced AI services or external verification systems with minimal changes.

C. Data Layer

The data layer is responsible for the storage, management, and security of all system data. MongoDB is used as the primary database for storing user profiles, authentication records, document metadata, access logs, and processing results due to its flexibility and scalability. Uploaded documents and extracted textual content are securely stored to support efficient retrieval and further analysis.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

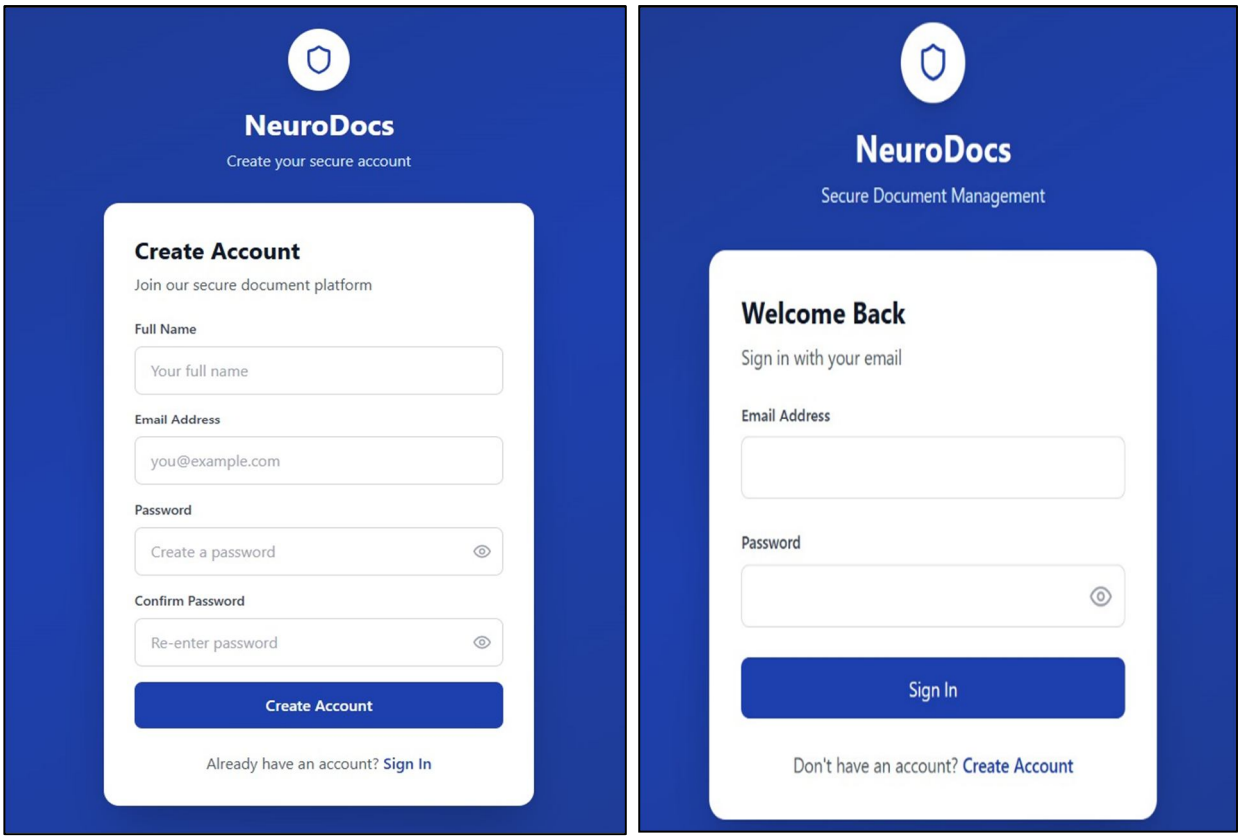
This layer ensures data integrity, secure access control, and reliable storage even as the number of users and documents increases. Proper indexing mechanisms are employed to improve data retrieval performance, while secure storage practices help protect sensitive user and document information. By providing a stable and scalable data foundation, the data layer supports the overall reliability and performance of the NeuroDocs platform.

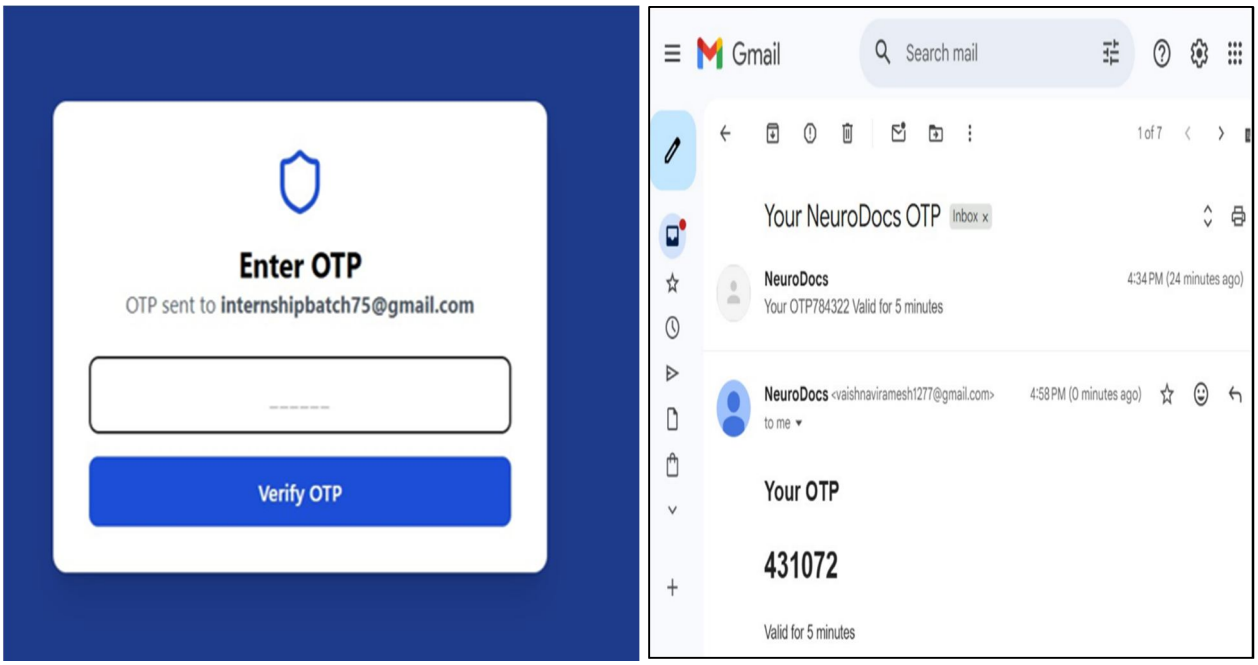
IV. IMPLEMENTATION

The implementation of NeuroDocs was carried out using a modular and incremental development approach to ensure clarity, scalability, and ease of integration. Each functional module was designed as an independent unit, allowing parallel development and simplified debugging. Modules were individually tested before integration to ensure reliable system behavior. The system combines modern web technologies with AI-based processing services to enable seamless document handling, analysis, and user interaction. The implementation phase focused on secure data flow, efficient processing, and user-friendly interaction. The following subsections describe the implementation details of each functional module.

A. Implementation of Secure Authentication and User Dashboard Module

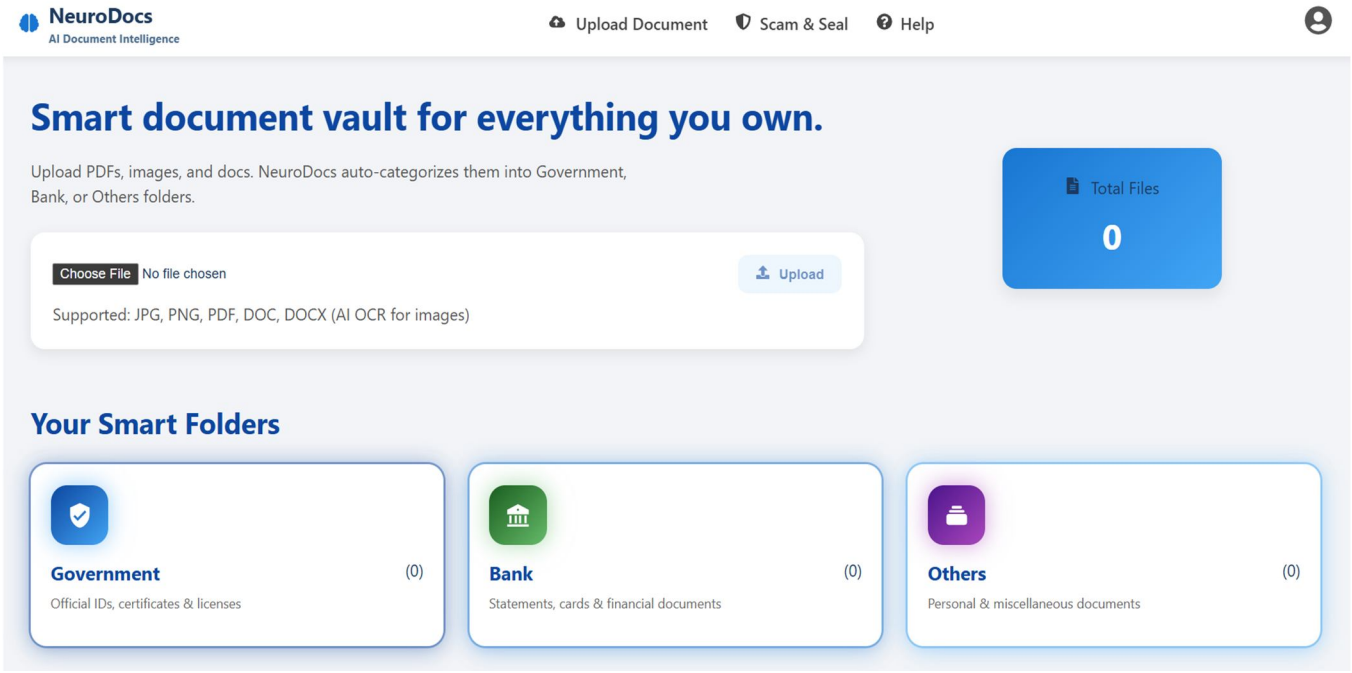
The Secure Authentication and User Dashboard Module was implemented to provide controlled, reliable, and secure access to the NeuroDocs platform. User registration requires a valid email address, which serves as a unique identifier within the system. During the login process, a One-Time Password (OTP) is dynamically generated on the server side and transmitted to the user's registered email address through a secure mailing service. Access to the system is granted only after successful OTP verification within a predefined time window, thereby reducing the risk of unauthorized access, brute-force attacks, and credential misuse. Upon successful authentication, a secure session token is generated to maintain session continuity and prevent session hijacking. Authenticated users are redirected to a personalized dashboard that acts as the central control interface of the system. The dashboard provides access to uploaded documents, automatically categorized folders, document processing status, multilingual assistance features, and fraud detection results. User activities are logged to support system monitoring and auditing.





B. Implementation of Automated Document Organization

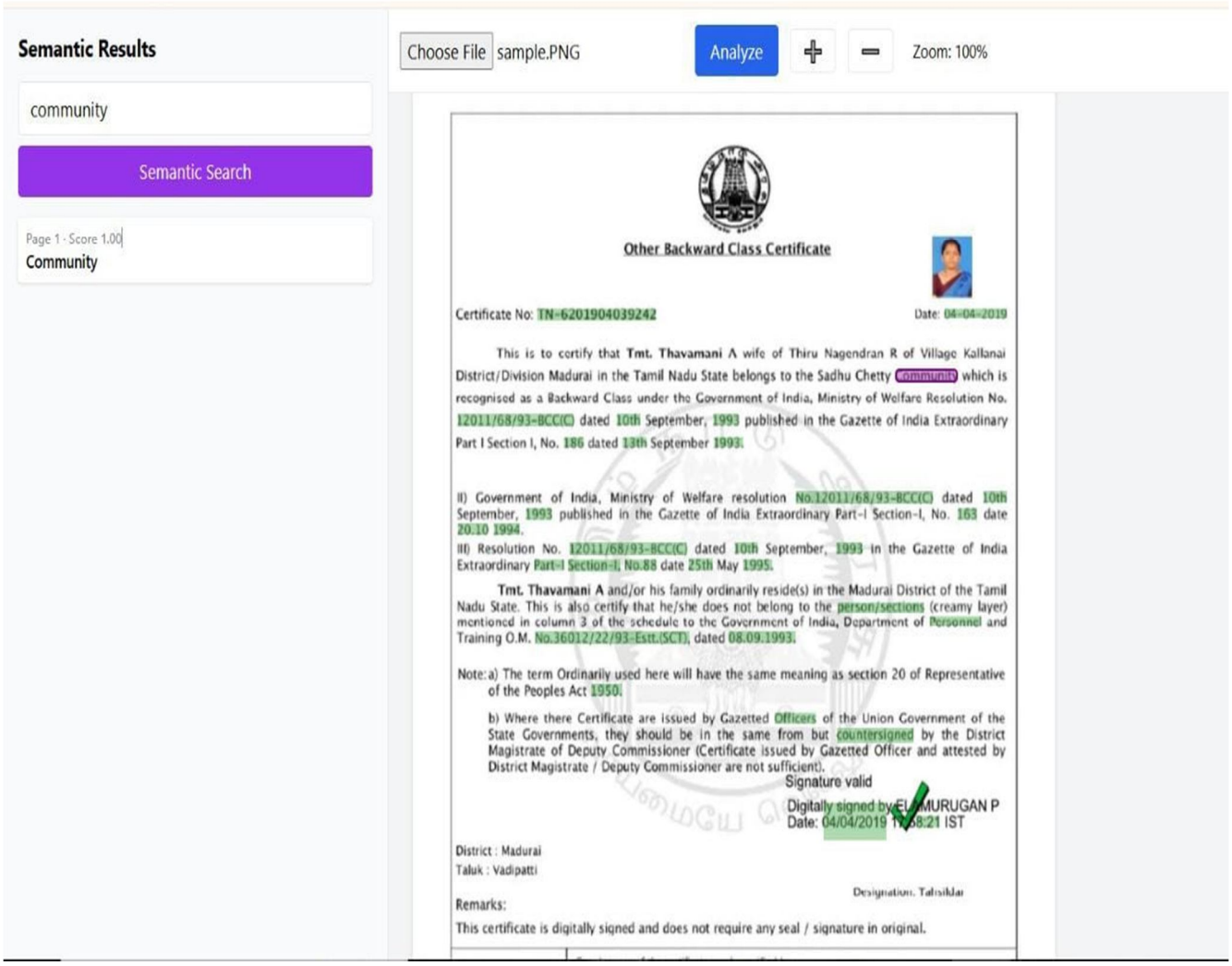
The Automated Document Organization Module is responsible for categorizing uploaded documents in a structured and efficient manner to improve document management and retrieval. Upon upload, documents are first validated to ensure supported file formats and safe size limits, after which they are securely stored before further processing. The validated documents are then processed through an OCR pipeline to extract machine-readable text from scanned images or PDF files. The extracted text undergoes preprocessing steps such as noise removal and text normalization to improve analysis accuracy. Using a rule-based keyword matching approach, domain-specific indicators including bank names, government identifiers, account-related details, and invoice-related terms are detected within the processed text. Based on the presence of these indicators, documents are automatically classified into predefined folders such as Bank, Government, or Others. This rule-based classification strategy ensures transparent and consistent document organization, significantly reduces manual effort, and enhances document retrieval efficiency for users.

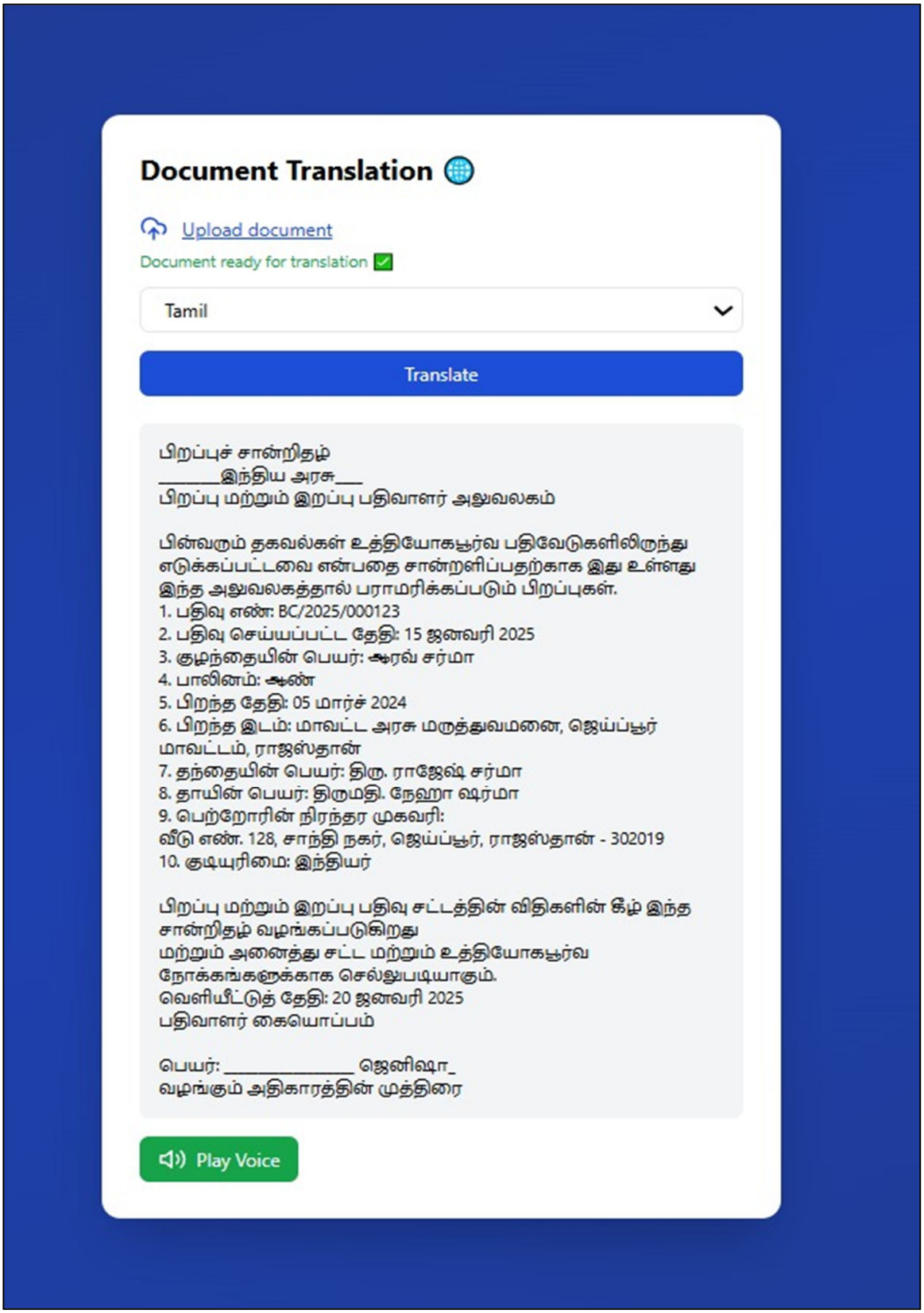


C. Implementation of Document Highlighting and Multilingual Translation Module

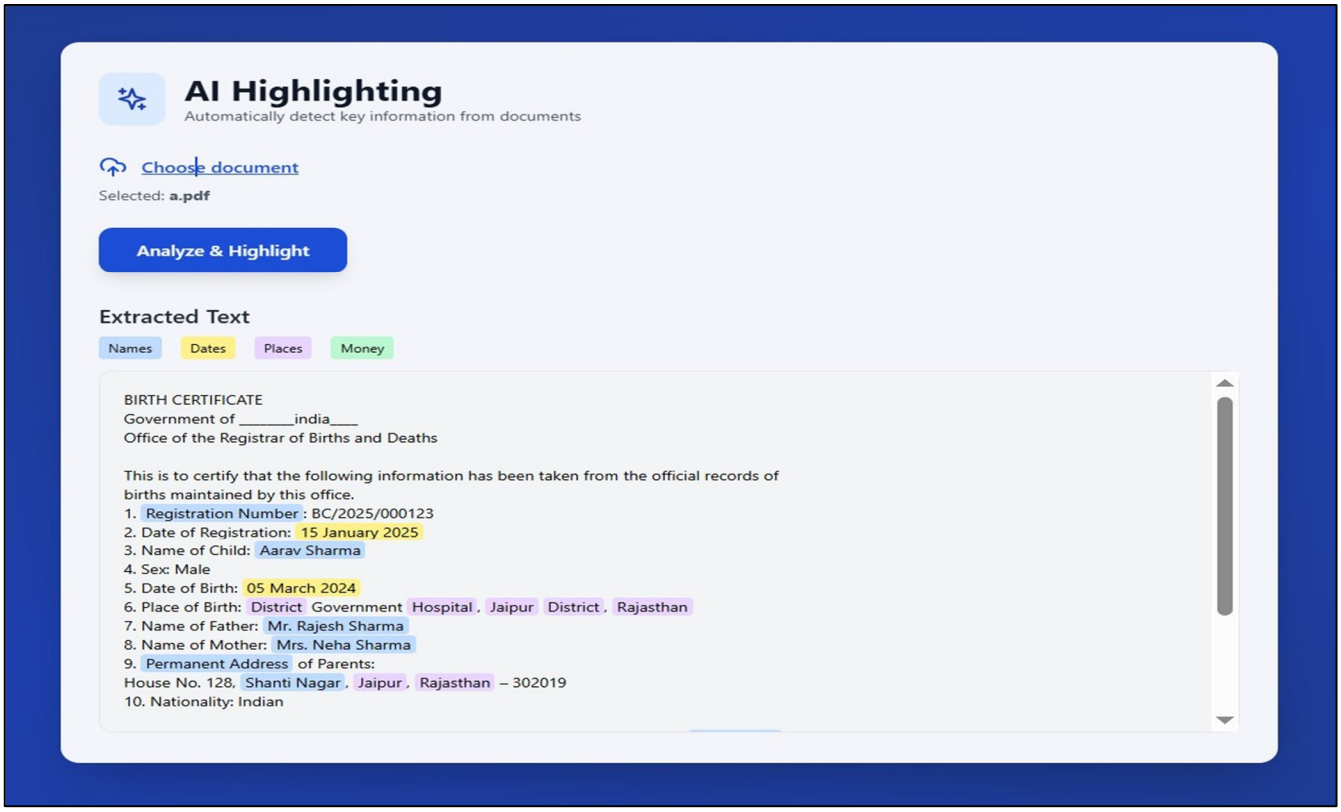
The Document Highlighting and Multilingual Translation Module was implemented to enhance document readability, comprehension, and accessibility for users with diverse linguistic backgrounds. Following OCR-based text extraction, the document content is systematically analyzed to identify important informational elements such as personal names, dates, monetary values, document reference numbers, section headings, and official or legally relevant terminology. These key elements are visually highlighted within the user interface, enabling users to quickly locate essential information without reading the entire document, which is particularly beneficial when handling lengthy, dense, or complex official documents. Visual highlighting improves clarity, reduces cognitive load, and supports faster information retrieval.

To address linguistic diversity and language barriers, the highlighted content is selectively forwarded to a multilingual translation service that supports Tamil, English, and Hindi languages. Translation is applied in a context-aware manner to preserve semantic accuracy and minimize the risk of misinterpreting technical, financial, or legal terminology. In addition to text-based translation, the system provides voice assistance as part of multilingual support by converting the translated content into speech, allowing users to listen to document information in their preferred language. Users can view the original text, translated text, and corresponding voice output simultaneously, enabling effective cross-referencing and improved understanding. By integrating intelligent highlighting, multilingual translation, and voice assistance, this module significantly improves document usability, reduces language-related challenges, and ensures inclusive access to digital documents, particularly for regional language users and individuals with limited English proficiency.



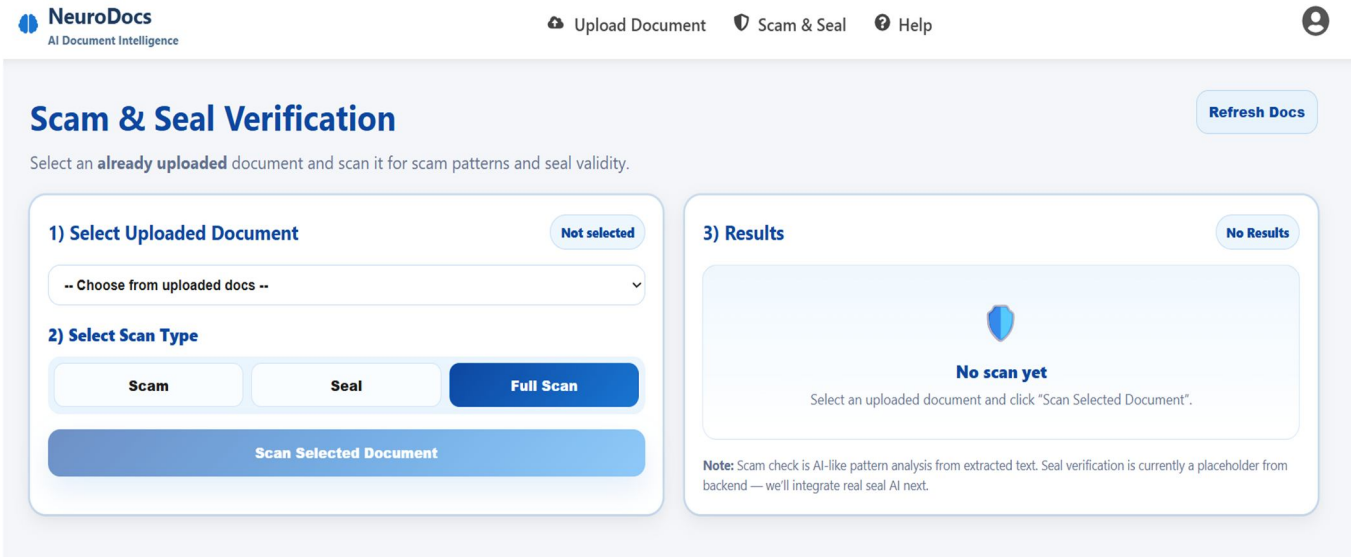


©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



D. Implementation of Scam and Fraud Detection Module

The Scam and Fraud Detection Module was implemented to enhance document reliability and user confidence by identifying potentially forged or manipulated documents. This module primarily focuses on the verification of seals and stamps commonly present on government and financial documents. Uploaded document images are analyzed using computer vision techniques to detect the presence of seals. Pre-trained object detection models are employed to locate seals within the document image. The detected seals are then examined for attributes such as shape, size, position, clarity, and consistency with known authentic patterns. Verification logic compares detected seal features against predefined authenticity criteria. Documents that do not meet verification standards or exhibit visual anomalies are flagged as suspicious. Alerts and visual indicators are displayed on the user dashboard to notify users of potential fraud risks.



V. FUTURE WORK

Future enhancements to NeuroDocs focus on improving robustness, scalability, and usability. Planned improvements include:

1) Development of a mobile application for wider accessibility
2) Advanced OCR preprocessing to handle low-quality and handwritten documents
3) Expansion of fraud detection datasets to improve accuracy
4) Support for additional Indian regional languages
5) Integration with cloud storage and government verification services
6) These enhancements will further strengthen the system's real-world applicability.

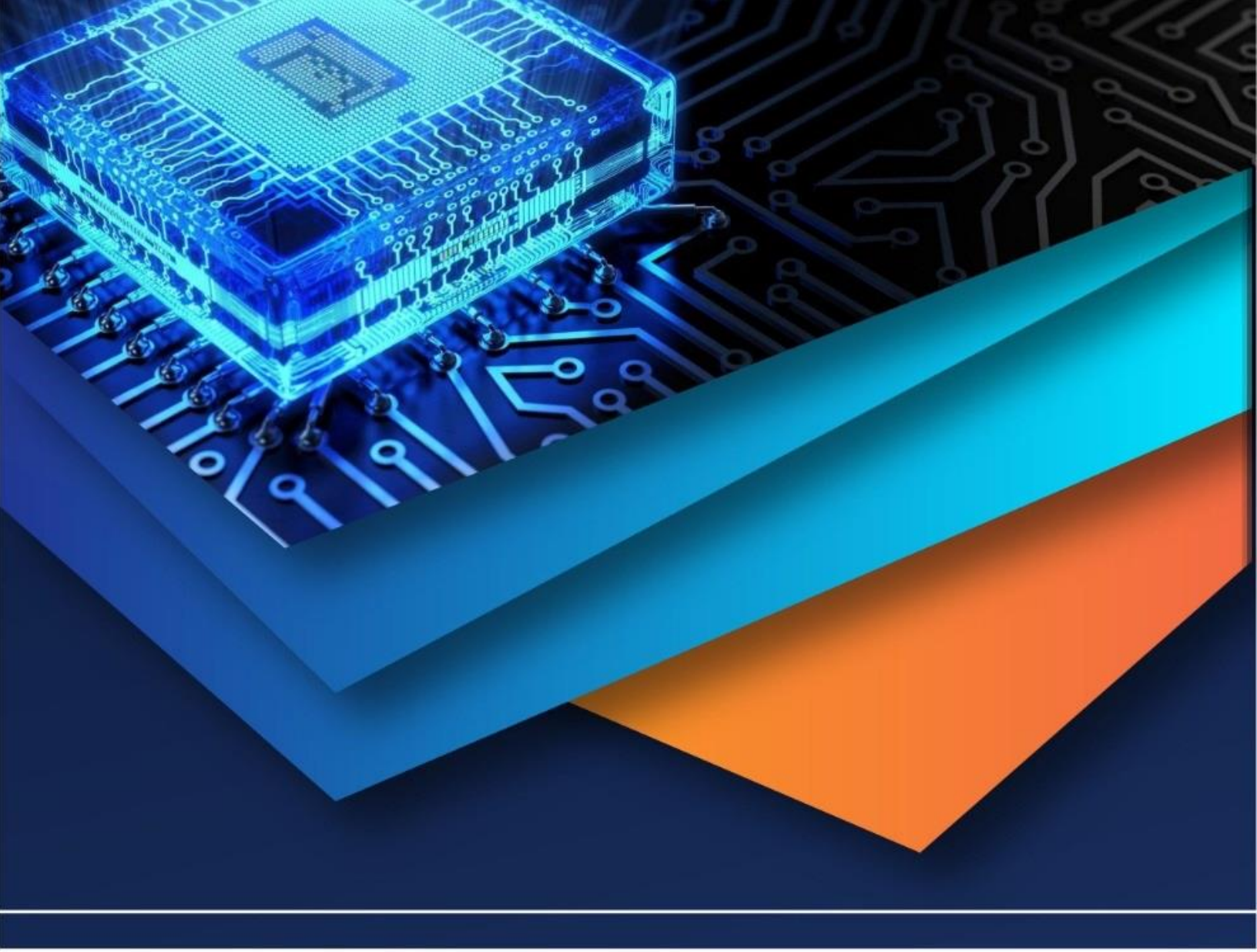
VI. CONCLUSION

This paper presented NeuroDocs, an intelligent document analysis system that integrates secure authentication, automated document organization, multilingual translation, and scam and fraud detection within a unified framework. The proposed system addresses critical challenges in digital document management by combining security, accessibility, automation, and trust in a single platform tailored to the Indian context. The rule-based document organization mechanism ensures reliable and transparent categorization, while AI-driven modules provide intelligent interaction and proactive fraud awareness. The modular and scalable system architecture allows individual components to be upgraded or extended without impacting overall system stability. As a result, NeuroDocs is well suited for deployment in real-world Indian digital environments such as banking, government services, and educational institutions, where secure, intelligent, and accessible document management is essential.

REFERENCES

[1] R. Smith, "An overview of the Tesseract OCR engine," in Proceedings of the International Conference on Document Analysis and Recognition (ICDAR), IEEE, 2007, pp. 629–633.
[2] J. Johnson, M. Douze, and H. Jégou, "Billion-scale similarity search with GPUs," IEEE Transactions on Big Data, vol. 7, no. 3, pp. 535–547, 2021.
[3] A. Bapna, N. Arivazhagan, et al., "IndicTrans: A multilingual neural machine translation system for Indic languages," Transactions of the Association for Computational Linguistics (TACL), vol. 10, pp. 1–16, 2022.
[4] G. Jocher, A. Chaurasia, and J. Qiu, "YOLOv8: Ultralytics real-time object detection," Ultralytics, 2023.
[5] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778
[6] S. Afzal, M. Liwicki, and T. Breuel, "Document image analysis—A review," *IEEE Access*, vol. 7, pp. 1–18, 2019.
[7] T. Brown et al., "Language models are few-shot learners," *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 33, pp. 1877–1901, 2020
[8] M. Schlichtkrull et al., "Graph-based fraud detection in real-world financial networks," *IEEE Transactions on Knowledge and Data Engineering*, vol. 33, no. 8, pp. 1–14, 2021
[9] N. Saharia et al., "Image-to-text generation for document understanding," *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, pp. 1–10
[10] N. Saharia, J. Li, D. Gutfreund, et al., "Image-to-text generation for document understanding," Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), 2021, pp. 1–10.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)