IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design And Implementation Of Restful Automated Document Verification System

[1]Sahil Sahay, [2]Divya Londhe, [3]Vinay Pawar, [4]Balasaheb B. Gite

[1]Student, [2]Student, [3]Student, [4]Professor Department of Comp. Engineering

[1]Department of Computer Engineering,

[1]ISB&M College of Engineering, Pune, India

Abstract: Government initiatives in India, designed for citizen welfare, often require extensive identity verification. Manual scrutiny of documents is time-consuming and susceptible to threats like counterfeiting. Our proposed solution employs digital signature verification and OCR technology for automated document verification, enhancing speed and security. This project aims to ensure user authentication, data integrity, and secrecy while adhering to the principles of Representational State Transfer (REST). By digitally signing and authenticating documents, it streamlines the verification process for government schemes, minimizing time and effort.

***Index Terms* - Rest API, OCR, Document Verification**

I. Introduction

In the contemporary landscape of administrative processes, the demand for swift and secure document verification is paramount. This research focuses on an Automated Document Verification System, integrating Optical Character Recognition (OCR) technology to expedite and fortify the verification of identity documents.

By automating the scrutiny process and addressing issues like counterfeiting, this system not only enhances efficiency but also upholds the integrity of sensitive information. This paper delves into the technical intricacies, exploring how this innovative approach can revolutionize identity verification processes within governmental frameworks.

The core objective of this project is to design and implement an Automated Document Verification System, leveraging OCR technology, to significantly reduce manual processing time, enhance document security, and ensure the authenticity of identity papers within government initiatives.

II. Rest Api

REST (Representational state transfer) is an architectural API (Application Programming Interface) that provides client-server communications for Web Applications over HTTP protocol, making it easily implemented since it is not bound to any transfer protocol. REST addresses acceptability by defining endpoints in a directory structure via different URIs for extracting the data.

The API works on the principle of CRUD (Create, Read, Update, Delete), which corresponds to the most popular functions INSERT, SELECT, UPDATE, and DELETE, in persistent data-storages such as SQL.

III. OCR TECHNOLOGY

Optical Character Recognition (OCR) stands as the linchpin of our Automated Document Verification System, offering a transformative approach to the processing of identity documents. This technology empowers the system to automatically extract and interpret textual information from images or scanned documents, mitigating the inefficiencies of manual scrutiny.

By converting physical documents into machine-readable text, OCR not only expedites the verification process but also plays a pivotal role in fortifying security measures against counterfeiting and tampering. This section delves into the technical nuances of OCR, elucidating its integration within the system and its pivotal role in revolutionizing document verification within governmental frameworks.

IV. DIGITAL SIGNATURE

In the ever-evolving landscape of digital technology, the integration of secure and efficient document verification systems has become paramount. As part of the ongoing efforts to enhance document verification processes, this survey focuses on the critical aspect of digital signature verification. In the context of an automated document verification system, understanding the challenges, preferences, and perceptions regarding digital signature verification is crucial. This survey aims to gather insights from users and stakeholders to inform the development and improvement of an automated document verification system, contributing to the broader discourse on secure and reliable digital transactions.

In the automated document verification workflow, when a user submits a document, the system extracts the digital signature and compares it with the associated cryptographic key. The verification process involves assessing the validity of the digital signature against established standards and protocols. Understanding the intricacies of this process is essential for refining the automated system to meet user expectations and industry standards. By engaging participants in this survey, we aim to obtain valuable feedback on their experiences, concerns, and suggestions related to digital signature verification, contributing to the continuous enhancement of automated document verification technologies.

The design of a secure digital signature uses the concept of hybridization of secure hash code, DNA encryption/decryption technique, and ElGamal encryption /decryption techniques. The use of the SHA algorithm generates a secure hash code and the hybridization of the encryption algorithm reduces the computational complexity this research method is then compared with the existing Play-Gamal algorithm with respect to encryption/decryption time complexity.

V. CHARACTERISTICS

1. **Efficiency and Speed:**

   The system excels in its ability to rapidly process a diverse array of identity documents, significantly reducing verification time compared to manual methods. The integration of OCR technology allows for swift extraction and interpretation of textual information, streamlining the entire verification process.

2. **Enhanced Security Measures:**

   Through robust encryption protocols and digital signature verification, the system ensures the integrity and authenticity of processed documents. By addressing threats like counterfeiting and tampering, it establishes a secure framework for handling sensitive information within government initiatives.

3. **User Authentication:**

   The system incorporates advanced user authentication mechanisms to verify the legitimacy of document submissions. This not only prevents unauthorized access but also adds an additional layer of security to the verification process

4. **Adaptability and Scalability:**

   Designed with scalability in mind, the system accommodates a growing volume of documents and users. Its adaptability to evolving technological landscapes ensures sustained relevance and effectiveness in handling the dynamic requirements of government schemes

5. **Comprehensive Data Integrity:**

   By leveraging OCR technology and digital signatures, the system ensures the accuracy and completeness of the extracted data. This comprehensive data integrity plays a crucial role in upholding the reliability of information and safeguarding against errors that might arise in manual processing.

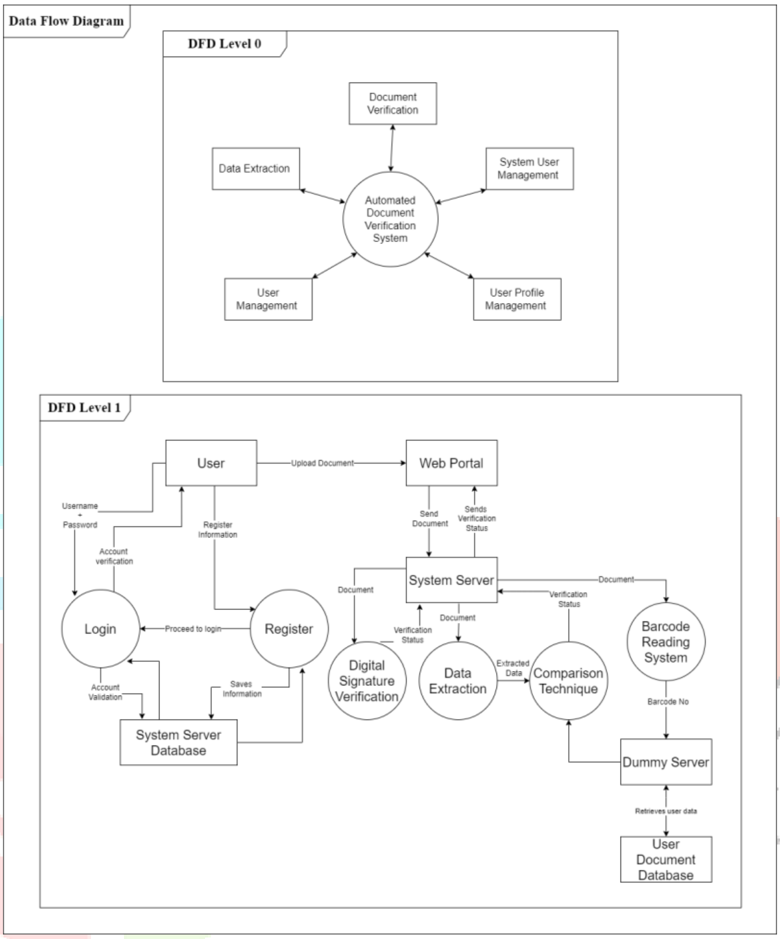

Fig 1. Data Flow Diagram

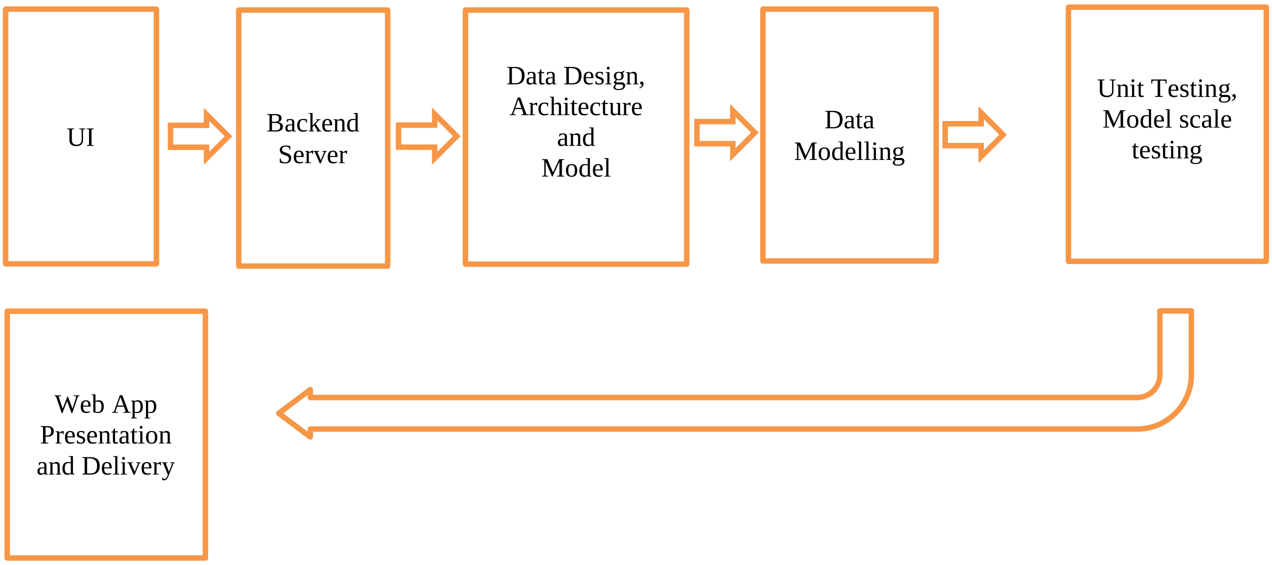
UI
Backend Server
Data Design, Architecture and Model
Data Modelling
Unit Testing, Model scale testing
Web App Presentation and Delivery

Fig 2. Pre-Development Anallysis

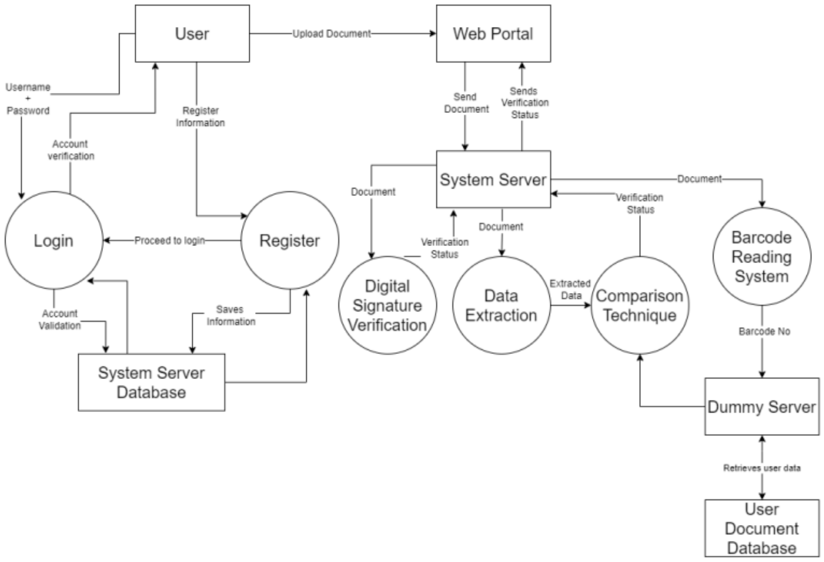

Fig 3. System Architecture

VI. CHALLENGES OFREST API

1. Data Retrieval Challenges: REST APIs frequently provide fixed data structures, leading to the potential problems of over-fetching (retrieving excessive data) or under-fetching (insufficient data retrieval). This can result in inefficient network resource utilization and hinder performance.

2. Absence of Consistent Standards: REST APIs lack strict standardization, offering guidelines but allowing for varied implementation details across different APIs. This lack of uniformity can create interoperability issues and pose a challenge for developers working with diverse APIs.

3. Security Vulnerabilities: REST APIs are susceptible to common web security threats such as Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and SQL Injection. Ensuring the security of RESTful APIs requires robust authentication and authorization mechanisms.

4. Real-time Data Limitations: Due to their request-response nature, REST APIs may not be optimal for real-time applications requiring low-latency updates, like online gaming or live chat. Implementing real-time features often demands additional technologies or creative solutions.

5. Versioning Complexities: As APIs undergo evolution, maintaining backward compatibility becomes a crucial concern. Modifications to the API can potentially break existing client applications, emphasizing the need for effective versioning strategies to facilitate both evolution and improvement.

VII. CONCLUSION

In closing, the Automated Document Verification System, driven by OCR technology, marks a transformative leap in identity verification. With its swift processing, enhanced security, and adaptability, the system not only addresses current challenges but lays a foundation for efficient, secure identity verification. This research contributes to the evolving landscape of administrative processes, offering a glimpse into the future of streamlined and reliable document verification.

VIII. REFERENCES

- https://www.researchgate.net/publication/343164544_Design_and_Implementation_of_REST_API_for_Academic_Information_System
- OCR.space Blog: https://ocr.space/blog/
- Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21(2), 120–126.