Software Requirements Specification

for

Real-Time Title Document Verification & Risk Assessment Platform

Prepared by

-Bhuvan J

-Harsha M

-Shreyas G

-Shwetha S

-Vinoda R

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) outlines the functional and non-functional requirements of the Real-Time Title Document Verification and Risk Assessment Desktop Application. It serves as a reference for developers, testers, stakeholders, and end-users. The application is designed to automate the verification of property title documents, integrate geo-location intelligence, and generate data-driven risk assessments. Its primary goals are to reduce manual effort, enhance compliance, and build trust in property-related transactions.

1.2 Scope

The desktop application facilitates property title verification through document parsing, location-based intelligence, and a risk scoring engine.
Key Objectives:

Automate document upload and metadata extraction
Evaluate property risk using predefined rules and historical data
Provide dashboards with real-time insights for underwriters and managers
Ensure secure data storage and role-based access control

Business Goals:

Minimize fraudulent claims and disputes
Improve operational efficiency in title verification workflows
Promote transparency through audit trails and analytics

1.3 Project Challenges

1. Technical Challenges

File Format Limitations: Some systems accept only PDFs or specific image formats, leading to rejection of scanned or low-quality files.
Large File Sizes: High-resolution scans often exceed upload limits.
OCR/Parsing Accuracy Issues: Automated tools may struggle with handwritten text, regional languages, or unclear stamps.
System Downtime: Government portals frequently experience high traffic, causing delays in uploads.

2. User-Related Challenges

Low Digital Literacy: Many users, especially senior citizens or rural residents, face difficulties in scanning, uploading, or validating documents.
Incomplete Submissions: Missing annexures such as identity proofs or encumbrance certificates result in repeated rejections.
Multiple Document Versions: Users often confuse documents like the Mother Deed and Sale Deed. The application simplifies this by consolidating historical records for easy access.

3. Verification Challenges

Data Mismatch: Discrepancies in owner names or addresses across Aadhaar, sale deeds, and other records.

Forgery Risks: Tampered or fake documents may be uploaded, necessitating robust verification mechanisms.
Inheritance Cases: Uploading legal heirship or partition documents can be complex and error-prone.

4. Process & Governance Issues

Lack of Standardization: Document requirements vary across municipal zones.
Manual Intervention: Despite digital submissions, physical verification by staff is often required, causing delays.
Transparency & Tracking: Applicants frequently lack visibility into the status of their submissions.

5. Connectivity & Infrastructure

Limited Internet Access: Rural and semi-urban users may struggle to upload large files.
Non-Mobile-Friendly Interfaces: Many portals are optimized for desktops, reducing accessibility for mobile users.

2. Overall Description

2.1 Product Overview

The desktop application offers a unified system for verifying property documents and assessing associated risks. It aims to:

Provide a single-window access for document verification
Ensure accuracy, transparency, and accountability in title validation
Minimize manual errors, fraud, and delays in property-related services
Enable stakeholders to make informed decisions based on risk insights

2.2 Product Perspective

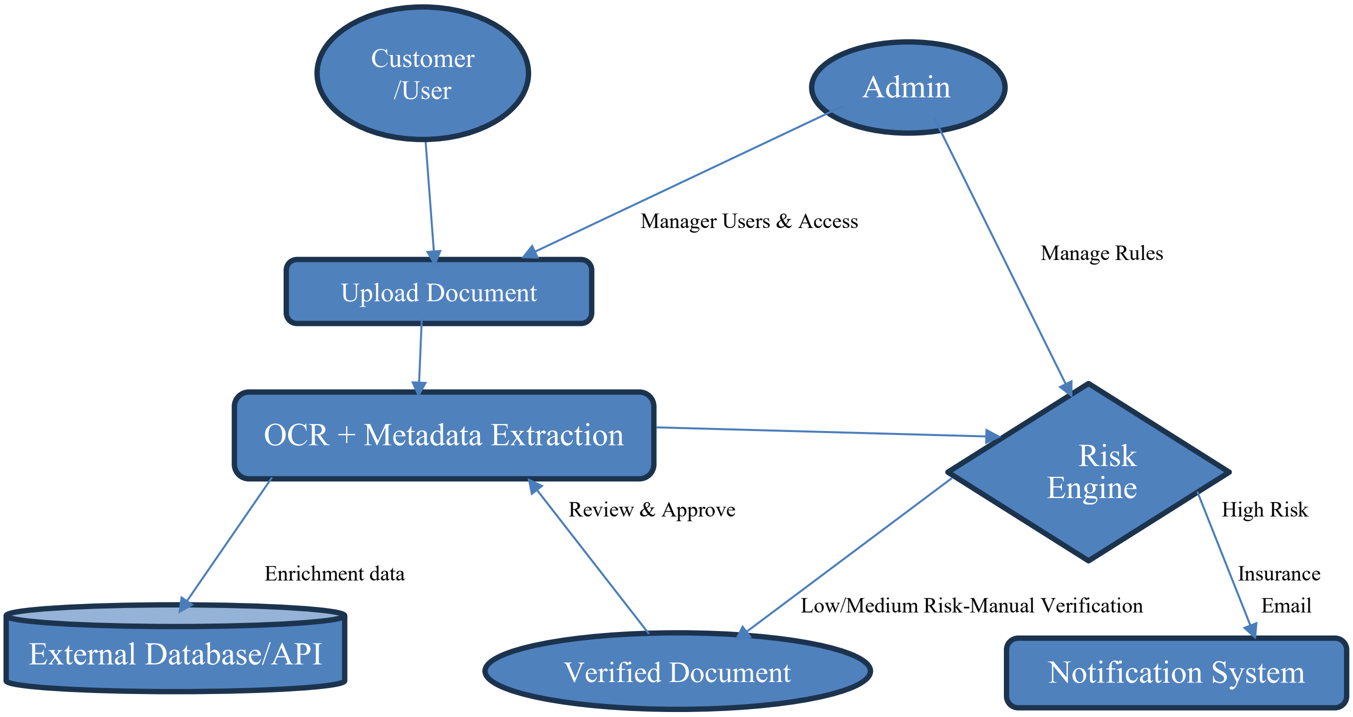
This is a newly developed desktop solution, designed after a thorough analysis of existing challenges faced during property registration and verification. While similar products exist, this application offers superior efficiency, automation, and intelligence.
2.3 User Classes and Characteristics

Master Database Access
OTP-Based Authentication
Sensitive Information Restrictions
Fraud Detection Mechanisms
Admin and User Login Portals

2.4 Operating Environment

Frontend Technologies: HTML, CSS, JavaScript, Angular/React, Bootstrap
Operating System: Windows
Backend Technologies: ASP.NET (C#), Node.js
Database: SQL Server
Security: SSL/TLS encryption, Role-Based Authentication

1.1 Design and Implementation Constraints



2. System Features

1. User Management
Role-based access (Admin, Customer/User, Verification Officer).
Secure login with authentication (e.g., OTP, biometrics, 2FA).
Profile management for customers and officers.

2. Document Upload & Capture
Upload documents in multiple formats (PDF, JPG, PNG, DOC).
Mobile camera integration for real-time capture.
Drag-and-drop web upload feature.

3. OCR & Metadata Extraction
Automatic extraction of text from scanned documents.
Metadata recognition (Name, Date of Birth, ID number, etc.).
AI-based anomaly detection (e.g., forged signatures, mismatched fonts).

4. External Data Integration
Connect with government databases (Aadhaar, PAN, Driving License, Passport, etc.).
Integration with APIs for real-time verification (KYC, financial databases, blacklists).

Cross-check against historical records.

5. Risk Engine
Configurable rules (set by Admin) to classify risk: Low, Medium, High.
Fraud detection (duplicate IDs, tampered documents, expired proofs).

6. Manual Verification Support
Workflow for Verification Officers to review flagged cases.
Side-by-side document comparison (uploaded vs official record).
Approve/reject functionality with audit trail.

7. Notification & Alerts
Email/SMS alerts for high-risk documents.
Real-time status updates to users.
Admin dashboard alerts for fraudulent activity.

8. Audit & Compliance
Complete logging of every action (upload, review, approval).
Data encryption (at rest & in transit).
GDPR/ISO/Local regulatory compliance for sensitive data.

9. Reporting & Analytics
Risk assessment reports for individual documents.
Statistical dashboard (fraud trends, verification success rate).
Downloadable reports (PDF/Excel).

3. Data Requirements

4.1 Logical Data Model

The system will process property title documents, ownership records, and risk metadata. The logical model includes the following entities:
- User (UserID, Name, Role, Email, PasswordHash, JWT Token, LastLogin)
- Property (PropertyID, Address, Coordinates, OwnerID, DocumentID, CreatedDate)
- Document (DocumentID, FilePath / BlobURL, UploadDate, FileType, HashSignature, Status)
- RiskAssessment (RiskID, PropertyID, RiskScore, RiskFactors, AssessmentDate, AnalystID)
- GeoLocation (GeoID, PropertyID, Latitude, Longitude, GeoSource)
- AuditTrail (AuditID, UserID, ActionType, Timestamp, Metadata)

Relationships:
- One User → Many Properties
- One Property → Many Documents
- One Property → One RiskAssessment
- One Property → One GeoLocation
- One User → Many AuditTrail

4.2 Data Dictionary

Field	Description	Type	Length	Format/Allowed Values
UserID	Unique user identifier	INT / UUID	36	Auto-generated UUID

Email	User login email	VARCHAR	100	Valid email format
PasswordHash	Encrypted password	VARCHAR	255	SHA-256 / bcrypt hash
PropertyID	Unique property identifier	INT / UUID	36	Auto-generated UUID
Address	Property location	VARCHAR	255	Free text, validated
Coordinates	Latitude/Longitude	FLOAT	N/A	WGS84 format (decimal degrees)
DocumentID	Unique document reference	INT / UUID	36	Auto-generated UUID
FilePath/BlobURL	File storage reference	VARCHAR	255	Azure Blob URI / Local Path
RiskScore	Calculated risk score (0–100)	INT	3	Range: 0 (Low Risk) – 100 (High)
RiskFactors	JSON representation of contributing data	JSON	N/A	Parsed key-value pairs
AuditTrail.Timestamp	Record of actions	DATETIME	N/A	ISO 8601 format

4. 4.3 Reports

Report Name	Description	Sort/Filter Options	Output
Title Verification Report	Verifies uploaded title document and authenticity	By DocumentID, PropertyID	Verification status, hash check, authenticity result
Risk Assessment Report	Generates property risk score with contributing factors	By Risk Level (High→Low)	Risk Score, contributing factors, trends
Audit Trail Report	Shows chronological log of all user/system actions	By Date/Time	UserID, ActionType, Timestamp, Metadata
Geolocation Risk Report	Displays location-based property risks	By Region/Coordinates	Heatmap visualization, disputed property markers

5. 4.4 Data Acquisition, Integrity, Retention, and Disposal

- Acquisition: Title documents uploaded by users; property metadata from databases; geo-coordinates from APIs
- Integrity: File hash signatures (SHA-256), validation checks, transaction logging
- Retention: Documents retained 7 years; metadata retained indefinitely
- Disposal: Secure deletion of expired docs; cached data cleared during cleanup

6. External Interface Requirements

7.1 User Interfaces

- Web Portal: Login, Upload, Property Entry, Dashboard, Audit Trail viewer
- GUI Standards: Navigation bar, Upload/View/Download buttons, inline + toast error messages

7.2 Software Interfaces

- Backend: ASP.NET Core Web API
- Database: SQL Server / PostgreSQL
- File Storage: Azure Blob / Local FS
- Authentication: JWT
- External APIs: Google Maps/HERE Maps, public registry datasets
- Tools: Swagger UI, Postman

7.3 Hardware Interfaces

- Client: Browser-based access
- Server: Cloud-hosted (2vCPU+, 8GB RAM, 50GB+ storage)
- Storage: Azure Blob Storage
- Connectivity: 2 Mbps minimum

7.4 Communications Interfaces

- HTTPS REST APIs (TLS 1.2/1.3)
- JSON data exchange
- JWT tokens in headers
- WebSocket (future scope)
- Email notifications (SMTP)
- API Rate limits: 1000 req/min/tenant

7. Quality Attributes

7.1 Usability

- 3-click process: Upload → Verify → Report
- Color-coded dashboard
- WCAG 2.1 AA compliance

7.2 Performance

- Verification: <5 sec/file
- Risk scoring: <3 sec/property
- 10,000 concurrent users

7.3 Security

- JWT + role-based access
- AES-256 + TLS encryption
- Immutable audit logs
- GDPR & IT Act compliance

7.4 Safety

- Prevent accidental deletion
- DB failover and backup
- Daily recovery checkpoints

7.5 Other Attributes

- Scalability: Auto-scaling
- Portability: Azure/AWS
- Reliability: 99.9% uptime
- Interoperability: Open API standard

8. Internationalization and Localization Requirements

- Date formats by region
- Currency per region
- Time zones supported
- Multi-language (English, Hindi, Spanish future)

9. Other Requirements

- ISO/IEC 27001 compliance
- Full logging of transactions
- Dockerized startup/shutdown
- CI/CD with GitHub Actions

10. Appendix A: Glossary

- JWT	JSON Web Token
- Blob Storage	Cloud file storage
- Risk Score	Property/document risk metric
- ERD	Entity Relationship Diagram
- CI/CD	Continuous Integration/Deployment

11. Appendix B: Analysis Models

- ERD showing entities and relationships
- DFD showing data flow from user to reports
- Architecture diagram of 3-tier des