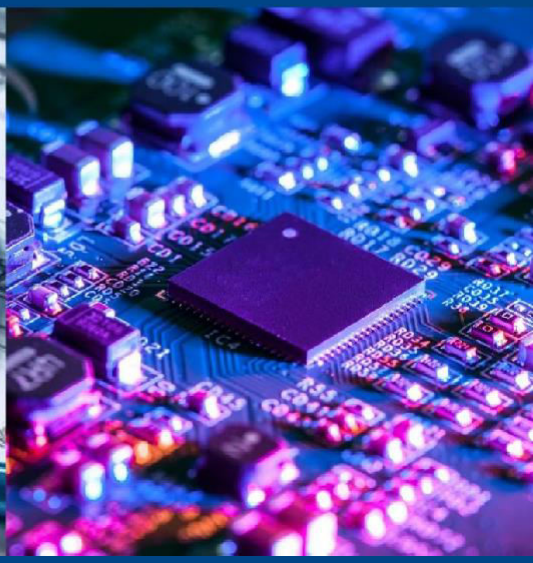
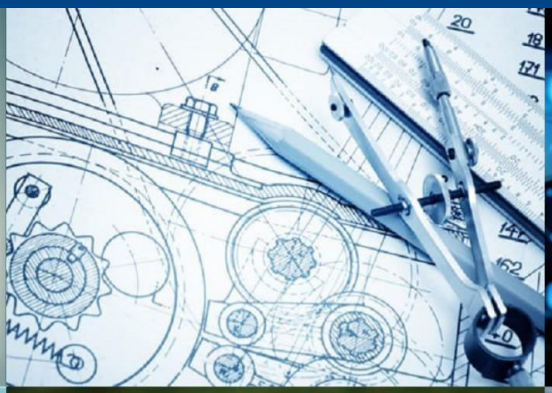
ISSN: 2582-7219

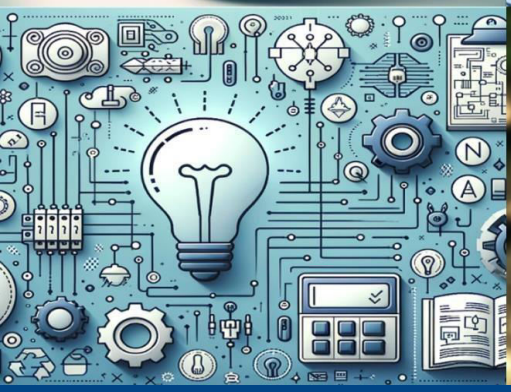




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206

Volume 8, Issue 12, December 2025

© 2025 IJMRSET | Volume 8, Issue 12, December 2025| DOI:10.15680/IJMRSET.2025.0812018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

IntelliCloud+: Automated Cloud System for Smart and Secure Document Management

Nithin H V[1], Chandana G V[2], Poorvika K M[3], S. Tejashree[4], Sudhir Reddy[5]

Assistant Professor, Department of Computer Science and Engineering (Data Science), PESITM, Shivamogga, Karnataka, India[1]

U.G. Students, Department of Computer Science and Engineering (Data Science), PESITM, Shivamogga, Karnataka, India[2, 3, 4, 5]

ABSTRACT: The exponential rise of unstructured digital documents demands secure, intelligent, and scalable management solutions. This work introduces IntelliCloud+, an AI-powered cloud system integrating OCR, classical machine learning, deep learning, and LLM-based reasoning for document classification and secure retrieval. The platform enables multi format ingestion, real-time classification, PIN-protected access, SHA-256-based deduplication, Google OAuth authentication, analytics dashboards, and cloud synchronization. Evaluations demonstrate high accuracy, reduced latency, and improved usability, positioning IntelliCloud+ as an effective solution across personal, academic, and enterprise domains.

KEYWORDS: Intelligent Cloud Systems, Document Classification, Secure Retrieval, OCR, LLM Reasoning

I. INTRODUCTION

In the contemporary knowledge-driven economy, documents constitute the foundational elements of personal, academic, and organizational workflows. Individuals routinely manage certificates, identification documents, medical records, and financial statements, whereas teams process proposals, invoices, contracts, reports, and electronic correspondence. The proliferation of scanning devices, smartphone cameras, and cloud storage solutions has precipitated an exponential increase in the volume, velocity, and diversity of documents.

However, despite this growth, the majority of users continue to rely on manual folder hierarchies, inconsistent naming conventions, and improvised sharing protocols. Such practices introduce inefficiencies, including file duplication, version mismatches, privacy vulnerabilities, and substantial time spent searching for documents that should ideally be instantly accessible. IntelliCloud+ is an artificial intelligence–enabled document management system engineered to address these challenges comprehensively.

It integrates ingestion capabilities (supporting multi-format uploads and drag-and-drop functionality), comprehension mechanisms (optical character recognition and automated classification), organizational features (automatic categorization and metadata tagging), security protocols (PIN-secured access for sensitive materials), and retrieval functionalities (full-text and faceted search) within a responsive web-based interface. The overarching objective is to achieve seamless document organization underpinned by privacy-centric design principles. Users may upload documents in PDF, image (JPG/PNG).

II. LITERATURE REVIEW

Existing research on intelligent document management systems highlights significant progress in automated classification, secure storage, and retrieval mechanisms, yet substantial gaps remain in achieving high accuracy, low-latency inference, and seamless scalability. Traditional systems rely heavily on rule-based or folder-driven organization, which studies have shown to be prone to redundancy, version inconsistencies, and limited search capabilities. Recent advancements in OCR technologies and deep learning–based classifiers demonstrate improved performance in processing heterogeneous document formats, while works integrating cloud computing emphasize enhanced accessibility and fault tolerance. Moreover, literature on security frameworks underscores the need for robust

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

encryption standards such as SHA-256 and user-centric access mechanisms including PIN-based or multi-factor authentication. Despite these developments, existing solutions often lack unified platforms that combine multi-format OCR, AI classification, secure access control, cloud backup, and analytics into a single responsive system—highlighting the necessity for platforms like IntelliCloud+ to bridge these gaps and deliver a comprehensive, intelligent document management architecture.

A. Machine Learning for Cloud Computing — ACM Computing Surveys

This survey provides an extensive overview of how machine learning is integrated into cloud computing environments to enhance automation, orchestration, and intelligent decision-making. The authors outline the application of supervised learning, reinforcement learning, and deep learning across major cloud platforms such as AWS, Microsoft Azure, and Google Cloud Platform. The review emphasizes how ML-driven resource prediction, load balancing, anomaly detection, and dynamic auto-scaling significantly improve operational efficiency in distributed cloud systems. The paper also highlights the importance of ML in optimizing compute, storage, and networking components, and in enabling predictive analytics for fault tolerance. While comprehensive, the work notes limitations in cross-platform model portability, high computational overhead for deep learning–based orchestration, and the lack of unified ML governance across cloud vendors.

B. Data Encryption in Cloud Storage

The author analyzes symmetric and asymmetric cryptographic mechanisms used to safeguard user data and evaluates how client-side and server-side encryption models differ in terms of access control and threat exposure. The paper emphasizes that encryption mitigates unauthorized access, insider threats, and data breaches by ensuring that only entities possessing valid decryption keys can read stored content. It also discusses key-management challenges, including key rotation, secure distribution, and protection against replay attacks. Despite offering strong confidentiality guarantees, the study acknowledges that encryption alone cannot prevent metadata leakage or access-pattern inference in cloud environments

C. Attention Over Pretrained Sentence Embeddings (AoSE)

This work proposes an attention mechanism layered on top of pretrained embedding mod els such as BERT and SBERT to improve sentence-level representation for downstream NLP tasks. The authors argue that standard embedding models often treat all tokens equally, missing contextual nuances. AoSE reweights sentence components through an attention mask, resulting in better semantic capture and relevance scoring. The approach improves performance in classification, clustering, and retrieval tasks. However, the model sacrifices token-level granularity and relies heavily on accurate sentence segmentation. The study concludes that while attention-enhanced embeddings improve representation quality, they introduce additional computational overhead and require careful tuning for domain-specific text.

D. ShieldDB: An Encrypted Document Database

ShieldDB introduces a fully encrypted document database designed to eliminate access pattern leakage through padding-based countermeasures. Traditional encrypted databases often leak structural information during query execution, enabling adversaries to infer patterns based on query frequency and response size. ShieldDB addresses this by employing padding, encrypted indexing, and secure data retrieval workflows that preserve confidentiality even during active querying. The system integrates end-to-end encryption, integrity verification, and secure update propagation. While highly secure, ShieldDB incurs additional storage and computational overhead due to padding expansion and encrypted query transformation. This research informs cloud-security design by demonstrating how encrypted databases can support privacy-preserving document search.

E. VisFormers: Multimodal Document Classification

This study presents a multimodal transformer-based architecture that combines visual document layout features with OCR-extracted textual embeddings. By integrating Vision Transformers (ViTs) and language models, the system captures both structural cues (such as font, spacing, and layout) and semantic meaning, significantly improving classification accuracy for unstructured documents. The authors demonstrate that multimodal fusion outperforms text-only or image-only baselines. Despite its strength, the model is computationally expensive, requiring high GPU memory and long training times. Additionally, it faces challenges in handling noisy scans and multi-language documents.

© 2025 IJMRSET | Volume 8, Issue 12, December 2025| DOI:10.15680/IJMRSET.2025.0812018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

F. Deep Learning for Document Image Analysis

This comprehensive review details the use of deep learning models such as CNNs, RNNs, autoencoders, and attention mechanisms in tasks like document layout analysis, text detection, handwriting recognition, and OCR enhancement. The study explores end-to end pipelines for converting raw scanned documents into structured digital formats. It also discusses challenges related to dataset scarcity, domain variability, multilingual text, and computational complexity. The work demonstrates that deep learning significantly improves accuracy and automation in document processing, forming the foundation of modern cloud-based document-management systems such as IntelliCloud.

G. Deep Learning for Text Classification

This large-scale survey reviews deep learning architectures used for text classification, in cluding CNN-based encoders, RNN/LLSTM models, hybrid architectures, and transformer based models such as BERT, RoBERTa, XLNet, and ALBERT. The paper evaluates benchmark performance across numerous datasets, highlighting each model's strengths and weaknesses. It explains that while transformer models deliver state-of-the-art ac curacy, they require large datasets, substantial computational resources, and lead to reduced interpretability. The findings provide critical insights for designing classification components in systems like IntelliCloud that rely on NLP-driven categorization.

H. Secure File Storage and Sharing Using Cryptography

This research proposes a cryptographic cloud-storage framework where files are encrypted locally before upload, ensuring strict confidentiality. Secure file sharing is supported through controlled key distribution and hashing for integrity verification. While effective in preserving privacy, the approach relies heavily on strong key-management practices and does not address metadata or access-pattern leakage, directly supporting IntelliCloud's secure storage module.

III. SYSTEM ARCHITECTURE

The IntelliCloud platform is designed using a layered architectural model to ensure modularity, scalability, and secure processing of uploaded documents. At a conceptual level, the system operates through four major layers: the Client Layer, the Application Layer, the AI/ML and Document Processing Layer, and the Data and Integration Layer. These layers work together to deliver seamless document classification, secure storage, and efficient retrieval. The interaction among system components follows a structured forward-and-return flow: User → UI (Web/Mobile) → Flask Application → Document Processing Pipeline → MongoDB and Storage → Back to UI. This workflow abstracts computational complexity behind backend services while ensuring a smooth and intuitive user experience.

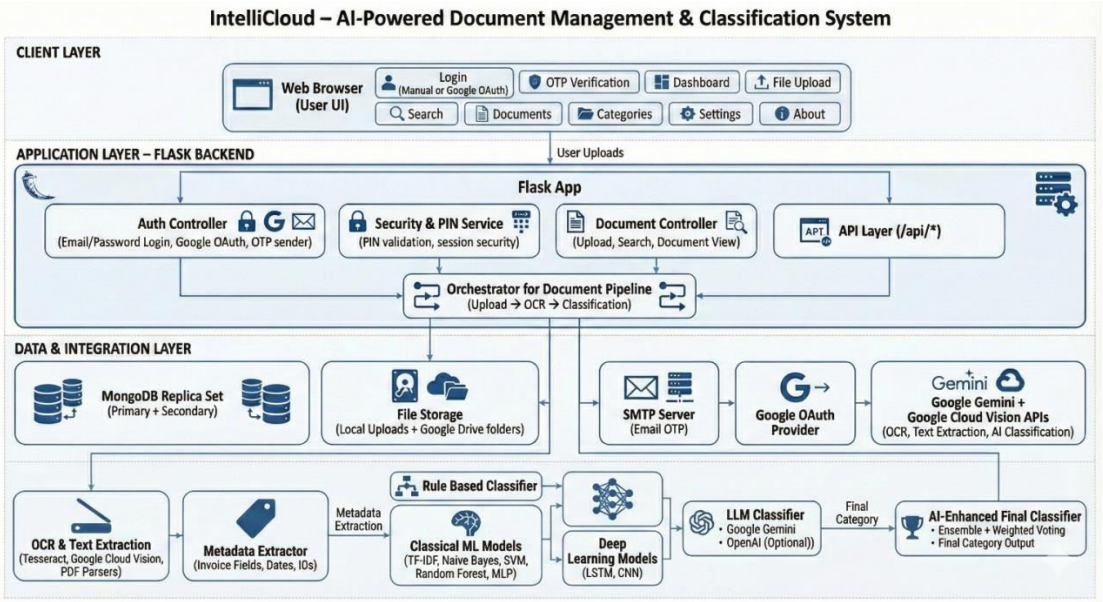


Figure 1: Intellicloud+ System Architecture

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Client Layer (Frontend and UI)

The Client Layer serves as the primary interaction point for users accessing the IntelliCloud system. Developed using HTML5, Bootstrap 5, and JavaScript, the web-based interface facilitates user registration, login, document upload, browsing, filtering, and permission management. With its focus on simplicity and responsiveness, the interface provides seamless usability across desktops, tablets, and mobile devices. Additionally, an optional Android application interacts with the Flask backend via HTTPS-secured REST APIs, enabling mobile-friendly access. Authentication is handled using secure session cookies for browser clients and token-based methods for mobile applications. By design, the client layer remains lightweight, delegating intensive processing tasks to the backend while ensuring a clean and responsive user experience.

Application Layer (Flask Backend and APIs)

The Application Layer, powered by the Flask backend, acts as the operational core of IntelliCloud. It manages routing, session handling, authentication workflows, document uploads, metadata assignment, and communication with both OCR and AI modules. The backend supports multiple authentication mechanisms, including password-based login, email-based OTP verification, and Google OAuth. Sensitive operations—such as PIN validation for protected documents—are processed securely on the server side. All critical data, including passwords and PINs, is hashed using robust cryptographic methods before storage. For every uploaded document, the backend oversees integrity checks, content validation, secure storage operations, and interaction with external AI services to maintain a complete and secure processing flow.

AI/ML and Document Processing Layer

This layer provides the analytical intelligence that powers IntelliCloud's document understanding capabilities. It handles OCR, text preprocessing, feature extraction, and hybrid classification. OCR is performed using both Tesseract for on-device extraction and Google Vision for cloud-based processing, ensuring accuracy across high- and low-quality scanned documents. The classification pipeline uses a hybrid ensemble model that combines rule-based methods, classical machine learning algorithms (Naive Bayes, Random Forest, SVM, MLP), deep learning architectures such as LSTM-CNN, and reasoning-enhanced predictions from LLMs like Gemini. Ensemble weighting allows the system to adapt to different document types—rule-based logic for identity documents and ML/DL models for business, academic, or financial documents. The final output includes the predicted category, confidence score, extracted metadata, and processed text, which are returned to the backend for indexing and secure storage.

Security and Protection

IntelliCloud employs a multi-layered, enterprise-grade security architecture that spans the application, network, and data layers. All sensitive credentials—such as API keys, encryption keys, authentication tokens, and database URIs—are stored exclusively as secured environment variables and injected at runtime to prevent accidental leakage through source code or version control platforms. Strong session management ensures that only authenticated and validated users can access backend resources, supported by encrypted tokens, strict expiration rules, and automatic invalidation of suspicious sessions. Robust input-validation pipelines scan all incoming data to safeguard against injection attacks and script-based exploits, significantly reducing the attack surface.

Network-Level Security (Nginx + ModSecurity)

At the network layer, Nginx functions as a secure reverse proxy providing TLS 1.2/1.3 encryption, HTTPS enforcement, IP-based rate limiting, and essential response headers such as HSTS, X-Frame-Options, and X-Content-Type-Options. ModSecurity acts as a Web Application Firewall (WAF), inspecting incoming requests using the OWASP Core Rule Set (CRS 3.3.5) to detect SQL injection, cross-site scripting, remote/local file inclusion, command injection, and other anomalies. Running in DetectionOnly mode, the WAF logs potential threats without interrupting user activity, allowing rule fine-tuning and minimizing false positives.

Application-Level and Data-Layer Security

At the application level, IntelliCloud secures sensitive document access with PIN-based authentication, using SHA-256 hashing for both PINs and user credentials. Secure session management incorporates HTTPS-only cookies, IP and user-agent tracking, and enforced authentication for all protected routes. File uploads undergo rigorous validation and filtering to prevent malicious file exploitation. In the data layer, MongoDB enforces hashed credentials, granular access control, and TTL-based expiration for OTPs and active sessions. Stored files are isolated in protected directories and cannot be accessed directly through URLs, mitigating the risk of path traversal and unauthorized file retrieval.

© 2025 IJMRSET | Volume 8, Issue 12, December 2025| DOI:10.15680/IJMRSET.2025.0812018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Attack Surface Protection

The combined security stack—Nginx, ModSecurity, and Flask—provides strong protection against common cyber threats, including SQL injection, cross-site scripting, path traversal, malicious file uploads, brute-force attempts, bot-based traffic, and small-scale DDoS spikes. By integrating layered defenses at every stage of the workflow, IntelliCloud ensures robust protection for user data, operational stability, and secure document management in real-world environments.

IV. METHODOLOGY

The development of IntelliCloud follows a comprehensive and research-driven methodology designed to ensure accuracy, scalability, and security in automated document classification. The project adopts an Agile development framework, enabling iterative improvements, rapid prototyping, continuous feedback integration, and user-centric refinement. Initial stages involved an extensive review of existing document processing systems and classifica tion approaches, which informed the selection of appropriate technologies, preprocessing techniques, and AI model architectures.

A. Requirement Analysis:

The requirement analysis for IntelliCloud focuses on identifying the essential capabilities, constraints, and performance expectations necessary for an effective AI-driven document management and classification system. The analysis considers system-level objectives, user needs, security requirements, and operational constraints to ensure that the platform is robust, scalable, and user-friendly. The requirements were gathered through literature review, analysis of similar document management systems, and evaluation of real-world workflows where automated classification can significantly reduce manual effort. IntelliCloud aims to streamline document organization by enabling users to upload heterogeneous document formats, extract textual content, classify them using multiple AI models, and securely store them with searchable metadata.

B. *System Design:*

The system design of IntelliCloud+ follows a modular, layered architecture that ensures scalability, security, and efficient document processing. At the core, the platform separates responsibilities across the Client Layer, Application Layer, AI/ML Processing Layer, and Security Layer, enabling smooth communication and easy maintainability. The frontend provides a responsive and intuitive interface for users to register, log in, upload documents, and perform file operations, while the backend—built using Flask—manages routing, authentication, session handling, and integration with OCR and classification modules. The document processing pipeline is designed to automatically validate inputs, extract text, classify documents, generate metadata, and encrypt content before storing it in secure cloud-backed directories. A multi-layered security framework, consisting of environment-level secret management, encrypted communication, hashed credential storage, and firewalls, protects the platform against unauthorized access and cyber threats. This structured design allows IntelliCloud+ to deliver fast, reliable, and intelligent document management while remaining flexible for future enhancements such as advanced summarization, multilingual OCR, and cross-platform synchronization.

C. *Development:*

The development of IntelliCloud+ followed an iterative and modular approach to ensure reliability, scalability, and smooth integration of all system components. The project began with setting up the core Flask backend, defining API routes, configuring secure session management, and establishing communication between the client and server through REST APIs. Frontend development involved creating responsive pages using HTML5, CSS, Bootstrap 5, and Python, ensuring a seamless user experience across devices. Parallel to this, the OCR and AI/ML modules were implemented and tested independently, using both local Tesseract processing and cloud-based recognition for better accuracy. The classification engine was built using a hybrid ensemble model, combining rule-based logic, machine learning, deep learning, and LLM-assisted predictions. Security mechanisms such as hashing, input validation, secure file handling, and environment-based secret management were added during the mid-development phase to strengthen the system against vulnerabilities.

D. Testing:

The system testing phase of IntelliCloud+ followed a comprehensive and multi-layered strategy to ensure reliability, accuracy, and security across all components. A combination of unit, integration, functional, non-functional, and end-

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

to-end testing was conducted to validate both core features and system performance. End-to-end tests evaluated the complete user workflow, classification accuracy, and OCR efficiency using a dataset of over 500 documents across twelve categories, measured through precision, recall, and F1-score. Functional tests covered authentication, OTP and PIN validation, document upload handling, OCR quality, classification correctness, metadata generation, and API reliability. Non-functional testing involved load and stress tests with up to 100 concurrent users, security scans against common vulnerabilities, and usability evaluations for interface responsiveness and accessibility.

Model	Accuracy	Precision	Recall	F1-Score
Naive Bayes	87.3%	85.1%	84.7%	84.9%
Deep Learning Model	91.8%	90.2%	89.9%	90.0%
Gemini AI	95.1%	94.3%	93.8%	94.0%
Ensemble (Final)	94.2%	92.8%	91.9%	92.3%

The above table shows that the ensemble model achieves a balanced trade-off between accuracy and latency. Gemini AI attains the highest accuracy and F1-score but requires a significantly longer inference time, making it less suitable as the sole decision engine in real-time applications. The ensemble model, by combining signals from multiple models, delivers near-Gemini performance while keeping the average inference time within 180ms. This makes the ensemble particularly appropriate for high-throughput scenarios and interactive classification workflows where responsiveness is important.

V. RESULTS

During the testing phase, all major modules, including campaign creation, admin verification, and donor transactions, operated as expected.

1. *Website Features*:
The IntelliCloud+ Home Dashboard serves as the central hub for all major system operations, providing users with easy navigation through sections such as Upload, Documents, Search, Categories, and About. A welcome banner with a brief introduction and a prominent “Upload Documents” button guides users toward quick interaction with the platform. The top navigation bar and profile menu enhance accessibility, while real-time statistics panels display recent uploads and classification activity, offering users an immediate snapshot of system usage and performance.

The Upload Documents interface in IntelliCloud+ provides a clean and user-friendly layout with both drag-and-drop and manual file selection options, ensuring a smooth upload experience. The page includes a clear header, intuitive icons, and responsive design for easy interaction. The Documents Dashboard further enhances usability by offering a filter panel for search, category, and file-type selection, along with a main section displaying documents as neatly arranged cards containing thumbnails, metadata, and quick-action buttons. Soft color themes, spacious layout, and well-designed icons make navigation simple and efficient for users managing large sets of documents.

The Categories Dashboard in IntelliCloud+ provides a well-organized view of documents by grouping them into visually distinct category cards, each displaying key details such as document count, description, and average classification confidence. The layout allows users to quickly understand category-wise activity through progress bars and clear indicators, while the “View Documents” button enables easy navigation to specific groups. Consistent color themes, clean formatting, and an analytical design make it simple for users to identify where most documents are stored and access files efficiently without extensive searching.

The SecureDocs folder structure in IntelliCloud+ automatically organizes uploaded files into category-based directories, ensuring a clean and scalable storage system without requiring manual sorting. When a document is uploaded, the system identifies its type and places it into predefined folders such as Academic, Business, Financial, Legal, or Medical, creating new folders when needed. The interface resembles modern cloud storage platforms, offering easy navigation through sortable folders and a sidebar with quick-access options. Consistent design elements, clear icons, and a structured grid layout make browsing simple and efficient for users managing large collections of documents.

© 2025 IJMRSET | Volume 8, Issue 12, December 2025| DOI:10.15680/IJMRSET.2025.0812018

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

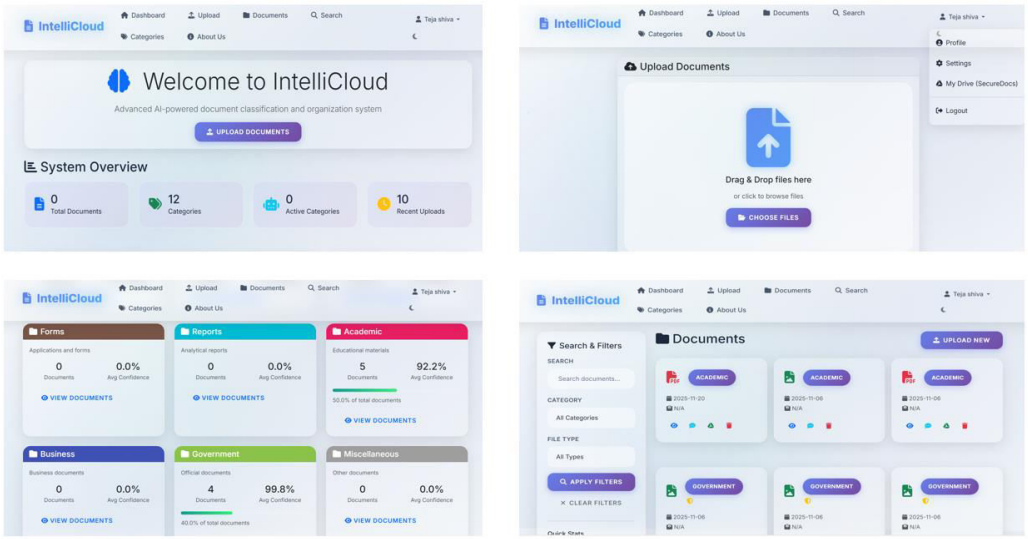


Figure 2: Intellicloud+ Website Snapshots

2. Email-Based Authentication with Encrypted Cloud Storage:

Email-based verification ensures that only legitimate users gain access to the IntelliCloud+ platform. When a user registers or attempts sensitive actions, a unique verification link or OTP is sent to their email. The system grants access only after successful confirmation, preventing unauthorized entry, fake accounts, and misuse. This adds a strong first layer of security and builds user trust by validating identity before allowing access to cloud services.

Cloud secure storage protects all uploaded documents through encrypted storage, controlled access, and continuous monitoring. Files are stored in isolated, category-based folders and secured with industry-standard encryption, ensuring data remains confidential and tamper-proof. Role-based permissions, authentication checks, and automated backups further enhance reliability. This feature ensures that users can safely store, organize, and retrieve their documents anytime without worrying about data loss or unauthorized access.

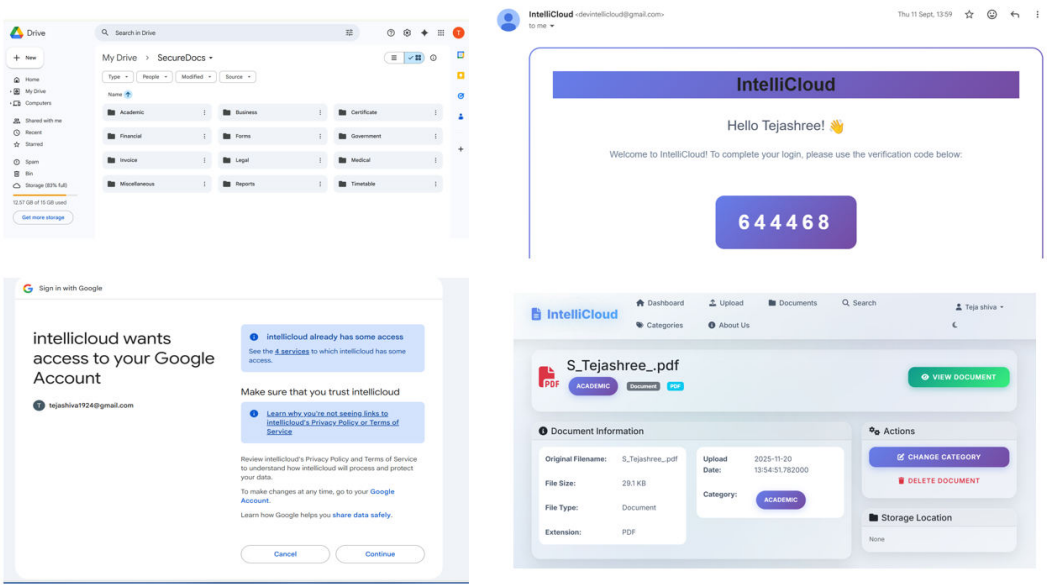


Figure 3: Email-Based Authentication with Encrypted Cloud Storage

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

VI. CONCLUSION

This research shows that blockchain can effectively tackle major challenges in traditional crowdfunding, especially the lack of transparency and trust in fund management. By using smart contracts, the system eliminates intermediaries and ensures that funds are released only when the campaign conditions are met. Donors can check every transaction on the blockchain, which cuts down on fraud and boosts trust in the fundraising process. The results indicate that the de centralized approach improves data security, accountability, and fairness. Campaign creation, donation, verification, and fund withdrawal processes were successfully managed without manual oversight. Overall, the system offers a more depend able and transparent crowdfunding model and demonstrates how blockchain can support trustworthy and efficient financial collaboration in real-world situations.

REFERENCES

[1] ACM Computing Surveys, “Machine Learning for Cloud Computing,” 2024.
[2] S. R. Gudimetla, “Data Encryption in Cloud Storage,” IRJMETS, 2024.
[3] A. Abdaoui and S. Dutta, “Attention Over Pretrained Sentence Embeddings (AoSE),” 2023.
[4] V. Vo et al., “ShieldDB: An Encrypted Document Database with Padding Countermeasures,” 2020.
[5] MDPI Authors, “VisFormers: Multimodal Document Classification,” 2022.
[6] A. B. Hamida et al., “Deep Learning for Document Image Analysis,” Applied Sciences, 2021.
[7] S. Minaee et al., “Deep Learning for Text Classification: A Survey,” ACM Computing Surveys, 2021/2022.
[8] M. R. B. Madhumala and H. Jain, “Secure File Storage and Sharing on Cloud Using Cryptography,” 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com