International Journal of Engineering and Techniques - Volume 12 Issue 2, March-April - 2026

RESEARCH ARTICLE OPEN ACCESS

Cloud Native Centralised Document Lifecycle & Approval System

Harsh Deo[1], Ashish Kumar Dass[2] Badri Narayan Hotta[3] Maruti Kar[4] Saurav Kumar[5]

1(Computer Science and Engineering, NIST University, Berhampur Odisha
Email: harshdeo5142@gmail.com)
2(Computer Science and Engineering, NIST University, Berhampur Odisha
Email: ashishkumardass@nist.edu
3(Computer Science and Engineering, NIST University, Berhampur Odisha
Email: narayanbadri97@gmail.com)
4(Computer Science and Engineering, NIST University, Berhampur Odisha
Email: marutikar1234@gmail.com)
5(Computer Science and Engineering, NIST University, Berhampur Odisha
Email: sauravsinghon2002@gmail.com)

Abstract:

Modern businesses require efficient document processing systems to meet regulatory requirements and support essential operations. The use of traditional email-based tracking systems causes operational delays because it restricts monitoring capabilities and creates security vulnerabilities. This research proposes an AWS-based document management solution that enables end-to-end handling of documents from creation to approval workflows. The system uses Amazon S3 for secure file storage and DynamoDB for document workflow tracking and EC2 to provide scalable computing resources and Redis to enhance system performance. The system uses role-based access control and token-based authentication together with SHA-256 hashing for cryptographic verification to protect its security. The system offers real-time monitoring alerts together with complete user activity tracking to maintain organizational transparency and accountability. Performance evaluation shows that Redis optimization improves response times by approximately 4–6 times compared to traditional systems. The proposed solution consolidates document operations into a unified platform which enables modern enterprises to achieve better regulatory compliance and stronger security measures while gaining complete operational visibility.

Keywords — **Document Management System, Workflow Automation, Document Approval, Microservices, Data Security, Performance Caching, Amazon Web Services, Cloud Computing**

I. INTRODUCTION

Enterprise operations require document authorization to complete their essential functions which include procurement and compliance together with administrative tasks. Modern organizations depend on documents as essential resources which enable them to make decisions and communicate with others while meeting their legal obligations. The traditional methods of handling documents which depend on email threads and shared network drives create operational problems through their tendency to produce duplicate files and leave documents without assigned responsibility which results in decreased document tracking capabilities.

A document workflow is defined as the structured process through which documents are created, reviewed, approved, and stored within an organization, ensuring proper access and control over information. The traditional approaches fail to deliver this structured flow which results in disorganized data management together with higher operational difficulties.

The research proposes a cloud-native centralized document lifecycle and approval system to solve

these problems. The system uses modern cloud technology to create secure document storage and efficient operational processes together with immediate document tracking features. The proposed solution improves operational efficiency through its unified platform which combines multiple functions, while reducing processing time and increasing document management transparency [1].

II. PROBLEM STATEMENT

Document handling processes of today show three main operational problems that need to be solved. The organization lacks complete process tracking because it does not have tools to monitor all workflow activities from start to finish. The organization cannot establish accountability through auditing because its system lacks essential proof of past events. Organizations also face significant risks related to data breaches and data loss due to inadequate security mechanisms. The organization experiences operational problems because its personnel must manually track tasks, which creates delays and prevents work from proceeding.

The combination of these problems results in lower output while increasing the probability that organizations will break regulations, which leads to monetary penalties and damage to their public image.

The proposed system uses cloud technology through Amazon Web Services (AWS) to solve existing problems. The system uses core AWS services to deliver high availability and scalability and reliability, which creates a powerful document management solution that meets modern business needs [2].

III. SYSTEM ARCHITECTURE

The system has been designed with a cloud-native architecture which delivers both scalable and reliable high-performance capabilities. The architecture uses Amazon Web Services (AWS) to build its system because all components can operate independently while maintaining their connections to each other. Cloud architecture enables efficient workload management which keeps systems operational while protecting against faults with data protection and monitoring systems [3].

The system consists of four primary components. Amazon S3 serves as the secure document storage solution which provides both durability and permanent data access with high availability. The real-time database in DynamoDB stores workflow states together with metadata and audit logs. EC2 instances deliver the computational resources needed to run backend services while they process user requests. The system integrates Redis as its caching layer to boost performance through decreased database demands and quicker response times.

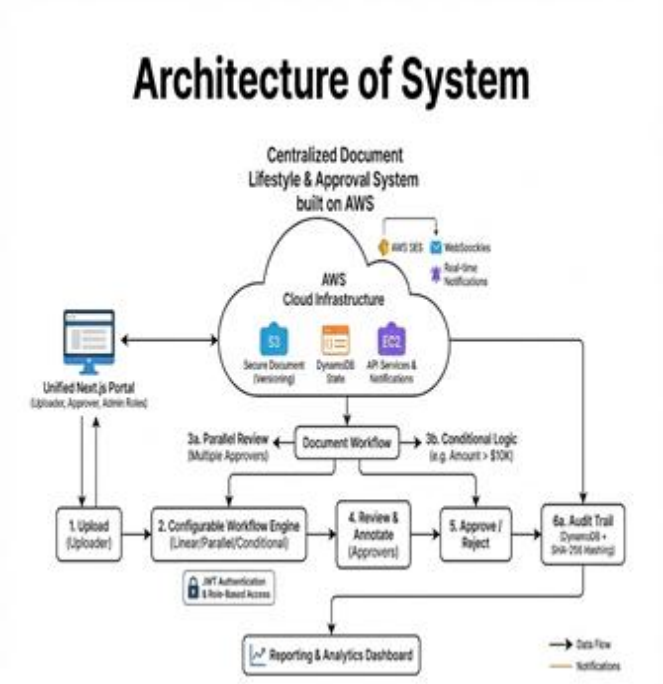

Fig. 1 Architecture of the system

The modular architecture enables separate scaling of all system components which results in better system performance and shorter response times and increased system reliability.

IV. SECURITY

The proposed system needs security measures because it processes confidential documents and personal information of users. Security architecture describes the established framework which

organizations use to secure their systems and data and applications from unauthorized access and various security threats.

The system establishes multiple security layers which protect the three fundamental elements of confidentiality and integrity and availability. The system uses JSON Web Tokens (JWT) for authentication because they offer secure management of user sessions. Role-Based Access Control (RBAC) restricts user access to resources which their roles permit them to access.

SHA-256 hashing creates distinct fingerprints for every document to establish data integrity which allows for detection of unauthorized changes. The system uses encryption protocols to secure all data transfers which protects information during its movement. The system uses cloud security practices which include access control policies and monitoring mechanisms to protect its resources.

A secure and dependable system needs a cloud security architecture which links identity management with data protection and monitoring systems [4].

V. METHODLOGY

The system development process follows an Agile iterative approach which creates modular components that function as separate system functions. The system provides key features which include real-time notifications that use WebSocket technology and operational dashboards that depend on user roles and audit logs that maintain permanent records for compliance purposes and document version control which eliminates conflicting versions. The orchestration layer controls system execution through its sequence validation gates and escalation procedures.

The workflow establishes a multi-officer approval system which operates in a dynamic manner. The user submits a document which the Junior Reviewer reviews at the beginning of the process. The reviewer selects Compliance Officers (COs) and establishes their sequence to create the workflow. The document progresses through all COs who execute their designated reviews according to the established sequence of operations. The system produces a digitally signed document after all review stages reach completion. The Junior Reviewer completes the process by sending the download link to others through email.

The system enables users to create customized workflows through its adaptable workflow management system. The Junior Reviewer has the authority to change workflow operations by choosing to add or delete or change the sequence of Compliance Officers. The COs follow their designated execution times because each CO only performs tasks at their scheduled time. The system allows users to use a rollback feature which enables them to return an approved document to the review process when they provide a legitimate justification. The system resets all workflow progress when an approved document requires review and it informs all involved parties through email about this change.

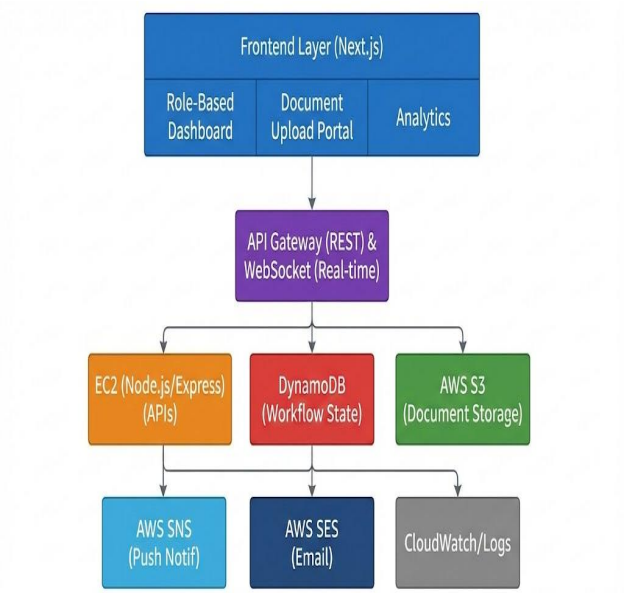

Fig. 2 Workflow of the system

The system uses version control to protect document authenticity while enabling document tracking. The system automatically stores all document versions which users can access through the version history feature. The system requires that all previously signed documents and their

associated verification codes must be invalidated during rollback to maintain system consistency.

The system provides a substitution mechanism which enables Compliance Officers to delegate their duties to other officers. The officer who requests a substitution must present a legitimate reason which allows the designated replacement officer to decide whether to approve or reject the request. The workflow permits substitution rights only during active stages when the replacement officer must not already be assigned to the workflow. The system sends notifications to all involved parties after the workflow receives approval. The system keeps an entire record of substitution requests to support transparency and auditing procedures [5].

VI. WORKFLOW

The system implementation follows a defined framework that guarantees secure and effective document handling through its established sequential process. The workflow describes the complete document journey which starts with document creation and ends with document approval.

Users start the upload process by uploading their documents together with accompanying metadata information. The system routes the document to Junior Reviewer who initiates the approval process by designating Compliance Officers (COs) for review. The document moves through the review process where each reviewer evaluates it before making their decision to approve or reject it. The system executes its operations through fixed sequences which guarantee all steps are completed and every activity receives official documentation.

The system produces a validated document after all approval processes have been finished which contains a distinct verification code that gets protected in a secure location. Stakeholders receive updates about the project through real-time notifications and email alerts which activate at every project milestone. The document gets stored in its permanent archive together with complete version history and audit logs which provide the ability to trace document changes and meet compliance requirements while maintaining permanent access.

VII. IMPLEMENTATION AND RESULT

The experimental evaluation shows that the proposed architectural design delivers better performance results than traditional methods. The performance testing results show that system response time decreased from 2.2–6.3 seconds to 0.6–0.8 seconds which demonstrates major efficiency improvements. Redis caching integration leads to a throughput increase of approximately 4.7 times which results in speedier data access and shorter wait times. The system shows average content access times that reach 45 milliseconds which provides users with a fast content access experience.

The system demonstrates scalable performance because it can handle 100 users simultaneously without experiencing any performance drops. The system achieves a total transaction success rate of 98% which proves its ability to perform reliably during high load periods. The results show that the proposed solution can scale up while delivering high performance which makes it appropriate for use in actual environments [6].

Status		Request	Total Time	Render Time
With Redis Cache HIT	/api/applications	633ms	633ms	369ms
With Redis Cache HIT	/api/applications	751ms	751ms	381ms
With Redis Cache HIT	/api/applications	862ms	862ms	501ms
With Redis Cache HIT	/api/applications	696ms	696ms	390ms
Without Cache	/api/applications	6.3s	6.3s	5.8s
Without Cache	/api/applications	3.3s	4.2s	894ms
Without Cache	/api/applications	4.2s	2.2s	1756ms

Metric	With Cache	Without Cache	Improvement
Average Time	~750ms	~3.5s	4.7x faster
Render Time	~400ms	~2.5s	6x faster

Fig. 3 The above image shows Caching boosts system throughput by 98%

The system shows excellent performance when it processes document workflows because it can

manage different document volumes. The system uses a cloud-native architecture which enables it to dynamically allocate resources for handling increasing workloads while maintaining its operational capacity. The system achieves fault tolerance through its distributed services which also decrease the probability of system outages.

The use of caching mechanisms in the system leads to a substantial decrease in database demands which helps to achieve better query performance and more consistent response times. The system delivers dependable performance throughout its busiest times which allows users to continue their work without interruptions. The architectural features demonstrate their ability to handle actual deployment situations.

The system assessment shows that it successfully maintains its operational performance while using minimal system resources. The system achieves continuous operation and effective task management through its use of scalable cloud resources and its backend processing optimization. The proposed solution meets enterprise requirements because it delivers dependable performance, fast operation, and expanding capacity needs.

VIII. CONCLUSION

The AWS-native framework which is demonstrated establishes a complete document management system which provides customers with expandable security features and operational capabilities that meet their high-performance needs. Modern business operations benefit from cloud-based systems which enable organizations to use resources more effectively while achieving better system availability and faster operational processes. The system achieves regulatory compliance through its established governance framework which enables ongoing monitoring activities together with audit functions and restricted access to confidential information. The structured system enables better understanding of processes which leads to better responsibility distribution while ensuring data protection throughout the entire document management process. The system aims to develop advanced technological solutions through its upcoming development work which includes integrating machine learning systems for workflow management and predicting future developments. The system provides two main benefits through its functionality because it helps organizations improve decision-making workflows while boosting their overall operational performance in response to changing workplace demands.

ACKNOWLEDGEMENT

The authors express their deep appreciation to Professor Ashish Kumar Dass who provided essential research guidance, ongoing assistance, and valuable recommendations throughout the research process. The project reached its successful conclusion because of his specialized knowledge and supportive presence.

The faculty members of the Department of Computer Science and Engineering at NIST University have our gratitude for their educational assistance. We appreciate our peers and colleagues who provided assistance and valuable feedback throughout our research activities.

Our research project received essential support from our families who provided us with continuous motivation.

REFERENCES

1. *S. Deng, H. Zhao, B. Huang, C. Zhang, F. Chen, and A. Y. Zomaya, "Cloud-Native Computing: A Survey from the Perspective of Services,"Proceedings of the IEEE, 2024.*
2. *Y. Mao, Y. Fu, S. Gu, S. Vhaduri, L. Cheng, and Q. Liu, "Resource Management Schemes for Cloud-Native Platforms with Docker and Kubernetes," IEEE/ACM Transactions, 2020.*
3. *A. Bani Ahmad et al., "Framework for Cloud-Based Document Management System," International Journal of Intelligent Systems and Applications in Engineering, 2024.*
4. *B. R. Kandukuri, V. R. Paturi, and A. Rakshit, "Cloud Security Issues," IEEE International Conference on Services Computing, 2009.*

5. *P. Tyrvainen, T. Paivarinta, A. Salminen, and J. Iivari, "Characterizing the Evolving Research on Enterprise Content Management," European Journal of Information Systems, 2006.*

6. *Dass, A. K., Nayak, M., Pattanaik, S. R., & Panigrahi, A. (2023). Cloud Computing in Industrial Automation Systems and its Future. Research and Applications: Embedded System, 6(3), 8-18.*