

LEVERAGING LOCAL LLM's TO BENEFIT PC USERS AND FINE-TUNE PCs FOR PROFFESIONAL WORKERS

Dilip Kumar G

B.Tech Information Technology
Panimalar Engineering College, Chennai City Campus
Chennai, India
gsmdilip1812@gmail.com

Mohan M

B.Tech Information Technology
Panimalar Engineering College, Chennai City Campus
Chennai, India
mohanmadhavan7805@gmail.com

Kishore B

B.Tech Information Technology
Panimalar Engineering College, Chennai City Campus
Chennai, India
kishorekish1802@gmail.com

Muthu Karthickeyan D

B.Tech Information Technology
Panimalar Engineering College, Chennai City Campus
Chennai, India
muthu1044.com@gmail.com

Abstract—Modern organizations require secure and efficient project management systems that support structured access control and intelligent assistance. This project presents a role-based project management system integrated with an AI assistant to improve organizational productivity and workflow efficiency. The system defines four hierarchical roles—CEO, Manager, Project Lead, and Employee—with clearly enforced Role-Based Access Control (RBAC). The CEO manages departments and users, Managers handle departments, users, and projects, Project Leads assign tasks and upload documents, and Employees update task status and access documents. All roles are provided controlled access to AI features for intelligent query handling, task support, and information assistance. The AI component functions as a productivity aid without violating access restrictions or organizational policies. The system is designed using a modular architecture to ensure scalability, security, and maintainability. The proposed approach demonstrates how integrating RBAC with AI-driven assistance enhances collaboration, accountability, and operational efficiency in enterprise environments.

Index Terms—Local LLMs, Offline AI, Professional Security, RBAC.

I. INTRODUCTION

With the increasing complexity of organizational workflows, effective project and task management has become essential for maintaining productivity, accountability, and operational efficiency. Traditional project management systems often rely on manual coordination and lack structured access control, leading to security risks and inefficient resource utilization. Additionally, most existing systems provide limited intelligent assistance to users during task execution and decision-making.

The advancement of Artificial Intelligence (AI) has enabled the development of intelligent systems that can assist users by providing contextual information, summaries, and productivity support. However, integrating AI into enterprise applications requires careful control to ensure security, privacy, and role-based access compliance. Role-Based Access Control (RBAC)

is widely adopted in modern software systems to restrict access based on user responsibilities and organizational hierarchy.

This project focuses on the design and implementation of a role-based project management system integrated with AI assistance, suitable for organizational environments. The system supports four hierarchical roles—CEO, Manager, Project Lead, and Employee—each with predefined permissions. By combining RBAC with AI-enabled support, the system aims to improve workflow efficiency, enhance collaboration, and provide a secure and scalable solution for modern enterprises.

II. RELATED WORK

Discuss prior research and cite appropriately [1].

III. METHODOLOGY

In the existing system, project and task management is often handled using manual methods or basic digital tools such as spreadsheets, emails, or standalone applications. These approaches lack centralized control, leading to data inconsistency, limited collaboration, and difficulty in tracking task progress.

Existing systems also provide minimal access control, where users may have excessive or unclear permissions. Additionally, there is little to no integration of intelligent assistance, resulting in increased manual effort for decision-making and reporting.

The proposed system introduces a centralized, role-based project management platform integrated with AI assistance. The system defines four roles—CEO, Manager, Project Lead, and Employee—each with clearly defined permissions.

The CEO manages departments and users, ensuring organizational governance. Managers manage departments, users, and projects. Project Leads assign tasks and upload documents, while Employees update task statuses and view assigned

documents. All users have access to AI features that assist with information retrieval, summaries, and productivity support.

The system enforces Role-Based Access Control at every level, ensuring security, accountability, and efficient workflow management.

IV. RESULTS AND DISCUSSION

The implementation results demonstrate that the Role-Based Project Management System operates reliably within a structured enterprise environment. Functional validation confirms that hierarchical Role-Based Access Control (RBAC) is consistently enforced across all user roles, including CEO, Department Head, Team Lead, and Employee. Both frontend route protection and backend middleware validation mechanisms worked cohesively to prevent unauthorized access, privilege escalation, and improper resource exposure. This dual-layer enforcement significantly strengthens system security and ensures strict adherence to organizational boundaries.

Integration testing further verified seamless interaction between authentication services, role validation middleware, and protected API endpoints. All modules—including departments, projects, tasks, meetings, and document management—performed as expected under normal and concurrent usage conditions. Performance evaluation showed stable response times and consistent data integrity during multi-user operations, indicating that the system architecture can support real-world enterprise workloads without degradation.

Security validation confirmed resilience against token manipulation, unauthorized API calls, and role tampering attempts. The AI module successfully delivered contextual assistance while operating within predefined role constraints, ensuring that no direct database access or unrestricted data exposure occurred. Collectively, these results indicate that the system achieves its primary objectives of secure access governance, modular scalability, and intelligent support within a unified and controlled enterprise framework.

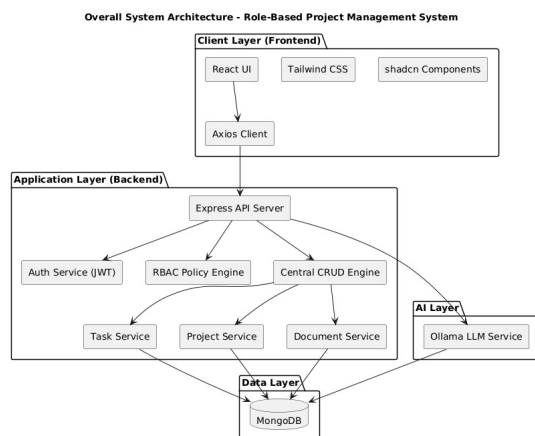


Fig. 1. System Architecture.

Strictly derived from your rules.				
Feature / Action	CEO	Dept Head	Project Lead	Employee
Manage Users	Yes	Yes (dept only)	No	No
Manage Departments	Yes	No	No	No
Create/Manage Projects	Yes	Yes	No	No
Assign Tasks	No	No	Yes	No
Upload Documents	No	No	Yes	No
Update Task Status	No	No	No	Yes
View Documents	Yes	Yes	Yes	Yes
Query AI Assistant	Yes	Yes	Yes	Yes (role-filtered)
View Reports	Yes	Yes	No	No

Fig. 2. RBAC.

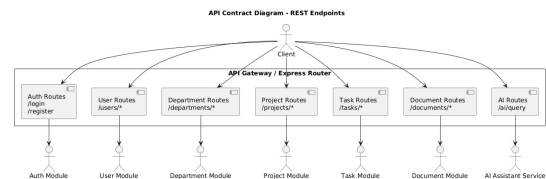


Fig. 3. API Contract.

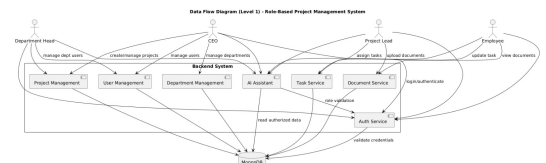


Fig. 4. Data Flow Diagram.

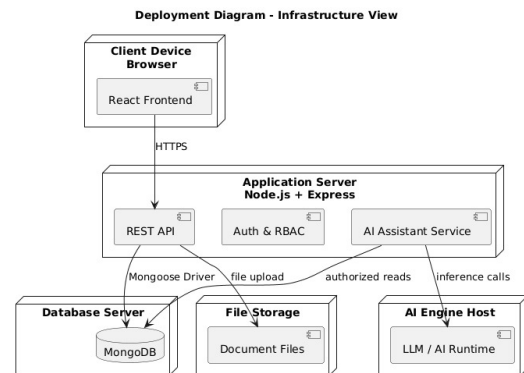


Fig. 5. Deployment Diagram.

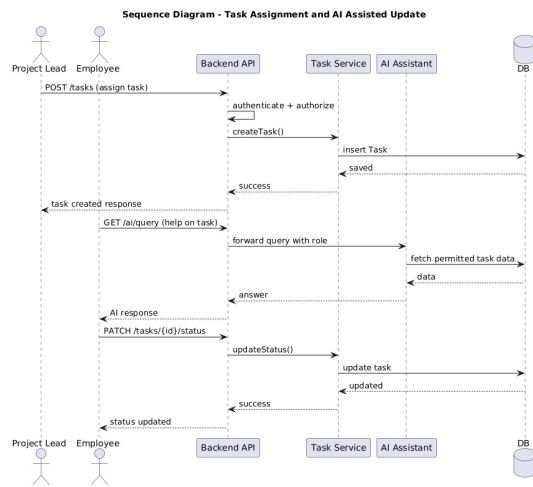


Fig. 6. Sequence Diagram.

Activity Diagram - Project Lead Assigns Task

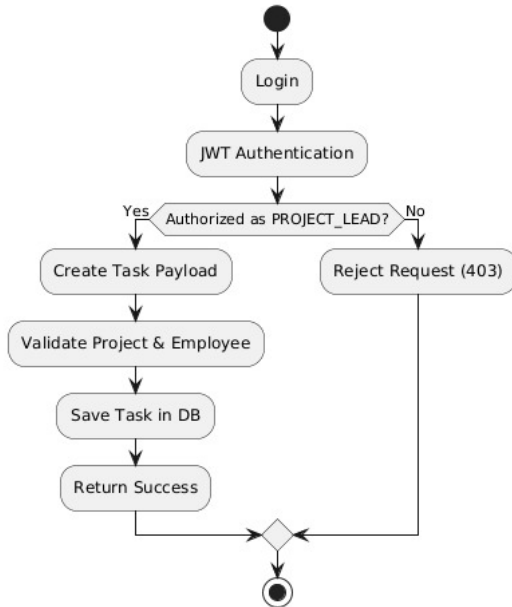


Fig. 7. Activity Diagram.

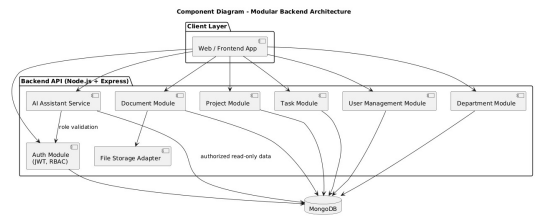


Fig. 8. Component Diagram.

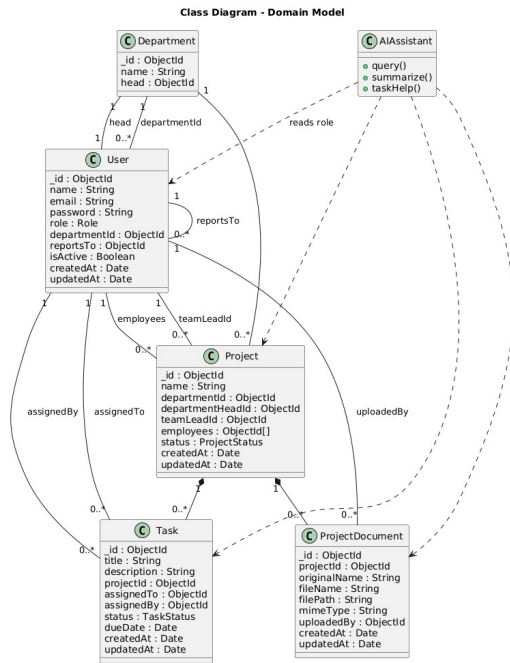


Fig. 9. Class diagram.

Entity Relationship Diagram - MongoDB Schema

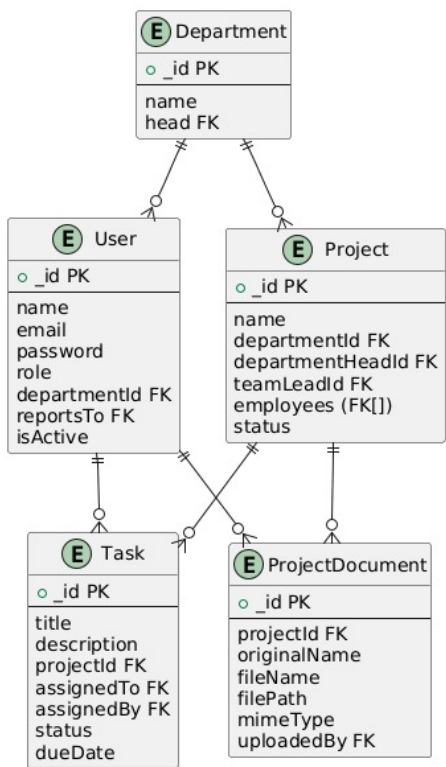


Fig. 10. Entity Relationship Diagram.

Use Case Diagram - RBAC Permissions

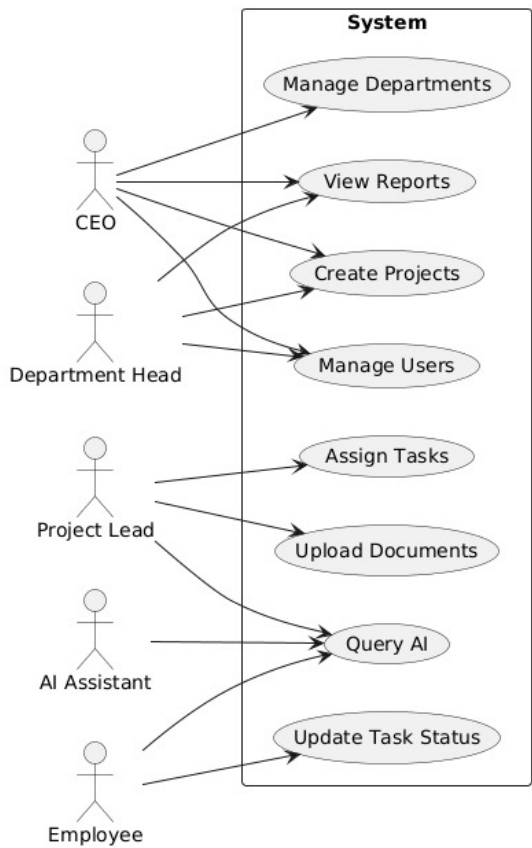


Fig. 11. Use Case Diagram.

V. CONCLUSION

The Role-Based Project Management System with Integrated AI Assistance demonstrates the successful development of a secure and scalable enterprise-grade application built using modern full-stack technologies. The system effectively addresses limitations commonly found in conventional project management platforms by implementing structured access control, centralized coordination, and intelligent assistance within a unified framework. The adoption of a layered architecture ensures maintainability, modular expansion, and long-term adaptability to evolving organizational needs.

A key achievement of this project is the rigorous implementation of hierarchical Role-Based Access Control (RBAC). Authorization is enforced at both the client and server levels, ensuring that permissions are validated through protected routes and backend middleware mechanisms. This multi-layered validation model minimizes risks such as unauthorized access, privilege escalation, and data exposure. The backend's modular separation of controllers, services, and middleware further strengthens code organization, while structured database relationships preserve referential integrity across users, departments, projects, and tasks.

The controlled integration of AI assistance within this secure environment represents an important contribution of the system. Rather than granting unrestricted data access, the AI component operates within predefined role boundaries and processes contextual inputs securely. This design ensures that intelligent support enhances productivity without compromising organizational hierarchy or data security. Comprehensive testing—including unit, integration, system, security, performance, and regression testing—confirms that the application operates reliably under diverse operational scenarios.

Overall, the project validates that enterprise applications can successfully combine strict access governance, scalable architectural design, and intelligent automation within a secure ecosystem. The system provides a robust foundation for future enhancements and demonstrates practical feasibility for real-world organizational deployment.

ACKNOWLEDGMENT

We would like to express our deep gratitude to our respected Secretary and Correspondent Dr.P.CHINNADURAI, M.A., Ph.D. for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our Directors Tmt.C.VIJAYARAJESWARI, Dr.C.SAKTHI KUMAR,M.E.,Ph.D and Dr.SARANYASREE SAKTHIKUMAR B.E.,M.B.A.,Ph.D., for providing us with the necessary facilities to undertake this project.

We also express our gratitude to our Principal Dr.S.MURUGAVALLI, M.E., Ph.D. who facilitated us in completing the project.

We thank the Head of the IT Department, Dr.S.KANIMOZHI, M.E.,Ph.D.,for the support extended throughout the project.

We would like to thank my Project Guide Dr.S.KANIMOZHI, M.E.,Ph.D., and all the faculty members of the Department of CSE for their advice and encouragement for the successful completion of the project.

Lastly, we would like to express our sincere gratitude to MANIKANDAN. R Software principal engineer, DELL International Services Pvt Ltd, Bengaluru for providing continuous guidance and valuable insights throughout the course of this project. His mentorship, periodic feedback, and technical support played a crucial role in shaping the successful completion of this work.

REFERENCES

- [1] A. A. Nikolakopoulos et al., “Exploring the Potential of Offline LLMs in Data Science” *IEEE Access*, vol. 1, 2025.
- [2] B. C. Ebert and P. Louridas, *Generative AI for Software Practitioners*. IEEE Software, 2023.
- [3] C. A. Fan et al., *Large Language Models for Software Engineering*. IEEE/ACM ICSE, 2023.
- [4] D.M.-F. Wong et al., *AI-Assisted Programming Using Large Language Models*, Entropy, 2023.
- [5] E. P. Sahoo et al., *Survey on Prompt Engineering in Large Language Models*. arXiv, 2024.
- [6] F. S. I. Ross et al., *Conversational AI Assistants for Software Development*. ACM IUI, 2023.
- [7] G. NIST, *Role-Based Access Control (RBAC) Standard*,USA.