IS Semester Project

ERP Security PenTest & Access Control Analysis

(Semester 4, 2023)

Submitted By

Rabia Nadeem 2023-CS-705

Abdul Rahman 2023-CS-725

Zain Shafique 2023-CS-738

Submitted To

Prof. Zoha Sohail

Submission Date

04/16/2025

Department of Computer Science

University of Engineering and Technology Lahore, New Campus

Abstract

This project audits role-based access control in the university's Odoo ERP system by extracting permissions with JSON-RPC APIs and presenting a structured analysis of what actions each role can perform on database models. The system provides a user-friendly interface for users to look up their column-level permissions and integrates AI/GenAI APIs for security analysis and recommendations. Advanced encryption and cipher implementations secure the authentication process and protect sensitive permission data.

Technology Stack

- **Backend:** Node.js with Express
- **Frontend:** Next.js/React with Context API
- **ERP Platform:** Odoo via JSON-RPC
- **AI:** OpenAI and Azure AI APIs
- **Cryptography:** AES-256, RSA, and custom cipher implementations
- **APIs Used:** res.groups, ir.model, ir.model.access, ir.model.fields, ir.model.fields.access

Key Features

1. Permission Mapping

- Auto-discovery of roles and permissions
- Visual matrix of role-to-resource access
- Field-level permission analysis

2. User Lookup Interface

- Name-based permission lookup for faculty/students
- Table and column-level access visualization
- Color-coded editability indicators

3. AI-Powered Analysis

- Anomaly detection for unusual permissions
- Risk scoring for access configurations
- GenAI-generated security recommendations

4. Advanced Authentication Security

- Multi-layered encryption for login credentials
- AES-256 encryption for session data
- Feistel cipher implementation for token generation
- Hill cipher for secure message exchange

5. GenAI Integration

- Natural language permission queries
- Automated security documentation
- Risk impact assessment for changes

Permission Flow