Project Report: Important and Securing Data in ServiceNow

1. Project Title

Securing Critical Data in ServiceNow Platform

2. Objective

To understand and implement best practices for protecting sensitive data in ServiceNow through access control, encryption, role-based access, and secure coding standards.

3. Introduction

ServiceNow is a leading cloud-based ITSM platform that manages digital workflows. As enterprises handle sensitive HR, financial, and personal data in ServiceNow, data security becomes a top priority. This report highlights data protection mechanisms built into the platform and how they can be applied effectively.

4. Importance of Data Security

- Prevent data breaches and unauthorized access
- Ensure compliance with regulations (e.g., GDPR, HIPAA)
- Protect PII, financial, and confidential information
- Maintain trust with users and stakeholders

5. Core Security Features in ServiceNow

5.1 Access Control Rules (ACLs)

- Fine-grained controls at table, field, and record levels.
- Based on roles, conditions, and scripts.

5.2 Role-Based Access Control (RBAC)

- Assign roles like admin, itil, or custom roles (e.g., hr_admin) to users.
- Only authorized users can perform specific operations.

5.3 Field-Level Encryption

- Protects sensitive fields such as Social Security Numbers (SSNs), passwords.
- Requires encryption plugins and key management.

5.4 UI & Data Policies

- Enforce rules to hide or restrict data entry/display on forms.