



IJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI:

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Research Paper on Salesforce Security Management

Alfred Desa

Abstract: *In today's digital world, businesses depend heavily on cloud platforms to store and manage data. Salesforce is one of the most popular cloud-based CRM systems used globally. However, as data moves to the cloud, security becomes a major concern.*

Salesforce Security Management provides multiple layers of protection such as authentication, authorization, encryption, and monitoring to ensure data safety. This research paper explains each security mechanism in detail with simple examples, making it easy to understand how Salesforce protects sensitive data from cyber threats.

Keywords: *Salesforce, Cloud Security, CRM, Authentication, Authorization, Encryption, Data Protection, Cybersecurity*

I. INTRODUCTION

Cloud computing allows companies to store data online instead of on local computers. Salesforce helps businesses manage customer data like:

Customer names
Phone numbers
Purchase history

□ Example:

A company stores customer details in Salesforce. If security is weak, a hacker could steal this data and misuse it. That's why Salesforce Security Management is important. It protects data using multiple security layers.

Shared Responsibility Model

Salesforce → protects servers, infrastructure

Company (User) → manages users, passwords, access

□ Example:

Salesforce locks the building, but you must lock your office room.

II. LITERATURE REVIEW

Research shows that:

Most data breaches happen due to human mistakes

Weak passwords and wrong permissions are common issues

Organizations like:

Cloud Security Alliance

NIST

recommend:

Strong authentication

Data encryption

Regular monitoring

□ Example:

If an employee shares their password, even the best system can be hacked.

III. SALES FORCE SECURITY ARCHITECTURE

Salesforce uses Defense-in-Depth, meaning multiple layers of protection.

A. *Physical Security*

This is the security of data centers.



Biometric locks

CCTV cameras

Security guards

Example:

Like a bank locker room where only authorized people can enter.

B. Infrastructure Security

Data is stored in multi-tenant environment

Each company's data is separated logically

Example:

Like different flats in one building — same building but separate homes.

C. Network Security

HTTPS (secure connection)

Firewalls

IP restrictions

Example:

Only devices from office IP can access Salesforce.

D. Application Security

Protects against:

SQL Injection → hacker tries to access database

XSS → malicious scripts

CSRF → fake requests

Example:

A hacker tries to enter “admin login” using code — Salesforce blocks it.

IV. IDENTITY AND ACCESS MANAGEMENT (IAM)

A. Authentication (Who are you?)

Verifies identity.

Types:

1. Username + Password Example: Gmail login

2. Two-Factor Authentication (2FA)

Example: OTP sent to mobile

3. Single Sign-On (SSO) Example: Login with Google

4. Biometric Example: Fingerprint login

B. Authorization (What can you do?)

After login, controls access.

Components:

Profiles Defines basic permissions

Example: Salesperson can view customers

Roles Hierarchy-based access

Example: Manager can see employee data

Permission Sets Extra permissions

Example: Temporary admin access

Sharing Rules Share data manually

Example: Share client record with another team



C. Multi-Factor Authentication (MFA)

Adds extra security layer.

Example:

Password + OTP

Password + fingerprint

Even if password is stolen, account stays safe.

V. DATA SECURITY MECHANISMS.

A. Data Encryption

Encryption = converting data into secret code.

Types:

Data at Rest Stored data encrypted

Example: Database encryption

Data in Transit Data moving over internet

Example: HTTPS lock icon

B. Field-Level Security

Controls specific fields.

Example:

Employee can see name

But NOT salary

C. Object-Level Security

Controls objects like:

Accounts

Contacts

Example: Intern cannot access "Finance" object

D. Record-Level Security

Controls individual records.

Example: Salesperson sees only their customers

E. Data Masking

Hides sensitive data.

Example: Real: 9876543210

Masked: 98XXXXXX10

Used in testing.

VI. MONITORING AND AUDITING (DETAILED)

A. Audit Trail

Tracks changes.

Example: Admin changed password policy → recorded

B. Login History

Tracks:

Login time

IP address

Example: Login from unknown country → suspicious



C. Event Monitoring

Tracks user behavior.

- Example: User downloads 1000 records → alert

D. Real-Time Alerts

Instant notifications.

- Example: Multiple failed logins → admin alerted

VII. COMPLIANCE AND GOVERNANCE

Salesforce follows:

GDPR → protects user privacy

ISO 27001 → security standards

HIPAA → healthcare data protection

- Example:

A hospital using Salesforce must follow HIPAA rules to protect patient data.

VIII. THREATS AND VULNERABILITIES (DETAILED)

Common Threats

1. Phishing Fake email asking password
2. Weak Password Easy password like 123456
3. Insider Threat Employee misuses data
4. Misconfiguration Wrong permissions

Risks

Data theft

Unauthorized access

API attacks

IX. SECURITY BEST PRACTICES (DETAILED)

Enable MFA

Use strong passwords

Limit access (least privilege)

Monitor activity regularly

Restrict IP access

Encrypt sensitive data

- Example:

Give employee only required access — not full admin rights.

X. CASE STUDY

A company had:

Weak passwords

No MFA

- Result: Unauthorized access happened

Solution:

Enabled MFA

Restricted access

Monitored login

- Result: Security incidents reduced by 70%



XI. ADVANTAGES

Strong multi-layer security
Easy scalability
Trusted globally
Advanced monitoring

XII. LIMITATIONS

Complex setup
Requires skilled admin
Costly advanced features
Human errors possible

XIII. FUTURE TRENDS (DETAILED)

AI-based security detection
Zero Trust Model (verify every access)
Blockchain security
Automated compliance
 Example:
AI detects unusual login automatically and blocks it.

XIV. CONCLUSION

Salesforce Security Management is essential for protecting cloud data. It uses multiple layers like authentication, encryption, and monitoring to ensure safety.

However, security is not automatic — organizations must properly configure and monitor their systems.

REFERENCES

- [1] Salesforce Documentation
- [2] Cloud Security Alliance
- [3] NIST Framework
- [4] IEEE Papers
- [5] GDPR Guidelines



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)