International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-13, Issue-3 (June 2023)
https://ijemr.vandanapublications.com https://doi.org/10.31033/ijemr.13.3.32

Protecting Sensitive Data in Salesforce – A Multi-Layered Security Approach

Sadaf Jahan[1], Faiyaz Ahmad[2] and Mohd Haroon[3]
[1]PG Student, Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, INDIA
[2]Associate Professor, Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, INDIA
[3]Professor, Computer Science & Engineering, Integral University, Lucknow, Uttar Pradesh, INDIA

[1]Corresponding Author: sadafjahan1210@gmail.com

Received: 29-05-2023 Revised: 16-06-2023 Accepted: 30-06-2023

ABSTRACT

Data security is a paramount concern for organizations across various industries, particularly when it comes to customer relationship management (CRM) platforms like Salesforce. As businesses increasingly rely on Salesforce for managing critical customer data, it is crucial to understand the security measures and best practices necessary to protect sensitive information from unauthorized access, breaches, and data leaks.

This research paper provides a comprehensive review of data security measures and best practices specifically tailored for Salesforce implementations. The objective is to equip organizations and Salesforce administrators with the knowledge and tools needed to establish robust security protocols and mitigate potential risks.

The paper examines the fundamental security features provided by Salesforce, including user authentication, access controls, and data encryption. It explores advanced security capabilities such as identity management, single sign-on (SSO), and multi-factor authentication (MFA), highlighting their role in enhancing data security and user access management.

Additionally, the research delves into the significance of data governance and data classification in maintaining data integrity and privacy. It discusses the implementation of role-based access control (RBAC), data sharing rules, and object-level permissions to ensure that data is accessible only to authorized individuals.

Furthermore, the paper explores best practices for securing data during transit and at rest, covering topics such as Secure Sockets Layer (SSL) encryption, data encryption at rest, and data backup strategies. It also addresses the importance of regularly monitoring and auditing user activity, employing security monitoring tools, and conducting vulnerability assessments and penetration testing.

By comprehensively reviewing the security measures and best practices in Salesforce, this research paper aims to serve as a valuable resource for organizations seeking to fortify their data security posture, protect customer information, and maintain compliance with data protection regulations.

Keywords-- Salesforce Data Security, Customer Relationship Management, Security Measures, Best Practices

I. INTRODUCTION

In today's digital landscape, data security is of utmost importance for organizations across industries. With the increasing reliance on customer relationship management (CRM) platforms like Salesforce, ensuring the protection of sensitive data becomes crucial. As businesses entrust their critical customer information to Salesforce, it is imperative to understand the security measures and best practices required to safeguard data from unauthorized access, breaches, and data leaks[1,2,3].

This research paper aims to provide a comprehensive review of the security measures and best practices specifically tailored for Salesforce implementations. By delving into the intricacies of Salesforce's security capabilities and exploring advanced features, this paper intends to equip organizations and Salesforce administrators with the knowledge and tools necessary to establish robust security protocols and mitigate potential risks[4,5,6].

The research paper will delve into the fundamental security features offered by Salesforce, such as user authentication, access controls, and data encryption. It will examine how these features contribute to the overall data security framework and their role in preventing unauthorized access to sensitive information. Additionally, the paper will explore advanced security capabilities like identity management, single sign-on (SSO), and multi-factor authentication (MFA), emphasizing their significance in enhancing data security and managing user access effectively[7,8].

Furthermore, the research will address the importance of data governance and data classification in maintaining data integrity and privacy. It will discuss the implementation of role-based access control (RBAC), data sharing rules, and object-level permissions, illustrating how these measures ensure that data is accessible only to authorized individuals. The paper will highlight the significance of maintaining a well-defined data access hierarchy and monitoring data access patterns to prevent potential breaches[9].

The research will also cover best practices for securing data during transit and at rest. Topics such as

Secure Sockets Layer (SSL) encryption, data encryption at rest, and data backup strategies will be explored to emphasize the importance of protecting data at every stage of its lifecycle. Additionally, the paper will discuss the significance of regularly monitoring and auditing user activity, employing security monitoring tools, and conducting vulnerability assessments and penetration testing to proactively identify and address security gaps[10,11].

Real-world case studies will be incorporated to provide practical insights into how organizations have successfully implemented Salesforce security measures. These case studies will illustrate the challenges faced, the security measures employed, and the outcomes achieved. Furthermore, the research will touch upon emerging trends in Salesforce security, such as the use of artificial intelligence (AI)-powered threat detection and the impact of evolving privacy regulations on data security practices[12].

By comprehensively reviewing the security measures and best practices in Salesforce, this research paper aims to serve as a valuable resource for organizations seeking to fortify their data security posture, protect customer information, and maintain compliance with data protection regulations. It is essential to establish a robust security framework on Salesforce to instill trust in customers and safeguard sensitive data from ever-evolving cyber threats[13].

II. BACKGOUND

In the era of digital transformation, organizations have witnessed a significant shift towards cloud-based platforms for managing their customer data. Salesforce, as one of the leading customer relationship management (CRM) platforms, has gained widespread adoption due to its robust features and scalability. However, this digital transformation has brought forth new challenges, particularly in the realm of data security.

Data security breaches, unauthorized access, and data leaks have become prevalent concerns, emphasizing the need for organizations to implement stringent security measures to protect their valuable data assets. Salesforce, as a custodian of vast amounts of customer information, must ensure the highest standards of data security to maintain the trust of its customers.

The importance of data security on Salesforce cannot be overstated. A breach or compromise of sensitive customer data can lead to severe consequences, including financial loss, reputational damage, and potential legal implications. Therefore, organizations must understand the security measures and best practices necessary to safeguard data stored and processed within the Salesforce environment[14].

Salesforce provides a robust security framework designed to address various aspects of data security. It offers features such as user authentication, access controls, and data encryption to protect data from unauthorized access. Additionally, advanced security capabilities like identity management, single sign-on (SSO), and multi-factor authentication (MFA) enhance the security posture by adding an extra layer of protection to user access[15,16].

Data governance and data classification also play a crucial role in maintaining data integrity and privacy within Salesforce. By implementing role-based access control (RBAC), data sharing rules, and object-level permissions, organizations can ensure that data is accessible only to authorized individuals based on their roles and responsibilities. This helps in preventing data breaches and limiting access to sensitive information[17].

Securing data during transit and at rest is another critical aspect of data security on Salesforce. Encryption protocols such as Secure Sockets Layer (SSL) ensure that data transmitted between users and the Salesforce platform remains encrypted and protected. Data encryption at rest provides an additional layer of security by encrypting data stored in databases or on physical devices[18].

Regular monitoring and auditing of user activity are essential to detect and prevent security breaches. By employing security monitoring tools and conducting vulnerability assessments and penetration testing, organizations can identify and address potential security vulnerabilities in their Salesforce implementation[19].

Understanding the best practices and emerging trends in Salesforce security is vital for organizations to stay ahead of evolving threats. Incorporating artificial intelligence (AI)-powered threat detection can enhance the ability to detect and mitigate security risks in real-time. Additionally, organizations must keep abreast of privacy regulations and compliance requirements to ensure their data security practices align with legal frameworks[20].

This research paper aims to provide a comprehensive review of the security measures and best practices specific to Salesforce, equipping organizations and Salesforce administrators with the necessary knowledge to establish a robust data security framework. By exploring the fundamental security features, advanced capabilities, and best practices, this paper intends to assist organizations in fortifying their data security posture, protecting customer information, and maintaining compliance with data protection regulations in the context of Salesforce[21,22].

III. PRILIMINARIES

Here, in the preliminaries section, the focus is on analyzing the existing security measures provided by Salesforce. This analysis serves as a foundation for proposing an enhanced security framework. The section evaluates the built-in security features of Salesforce,

highlighting their strengths and limitations. Here are some key aspects covered in the preliminaries section[23]:

a. User Authentication

Salesforce offers various authentication mechanisms to ensure that only authorized users can access the system. This includes username-password authentication, multi-factor authentication (MFA), and integration with external identity providers. The section examines the effectiveness of these authentication methods in protecting user accounts from unauthorized access[24].

b. Data Encryption

Salesforce employs encryption techniques to protect data at rest and in transit. This includes field-level encryption, where sensitive data fields are encrypted in the database, as well as transport encryption using SSL/TLS protocols. The preliminaries section assesses the encryption mechanisms used by Salesforce and discusses their role in securing sensitive data. The Hamming solution method primarily involves calculating the differences between corresponding numbers in two binary sequences. Additionally, there are four methods for determining similarity: cosine, overlap, dice, and Jaccard. The calculation formulas for these methods are as follows[27]:

$$\text{Overlap sim}(x,y)=\frac{\sum_{i=1}^{n} x_i y_i}{min \sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i^2}$$

$$\text{Dice –sim}(x,y)= \frac{2\sum_{i=1}^{n} x_i y_i}{min \sum_{i=1}^{n} x_i^2+\sum_{i=1}^{n} y_i^2}$$

$$\text{Jaccordsim }(x,y)= \frac{\sum_{i=1}^{n} x_i y_i}{\sum_{i=1}^{n} x_i^2+\sum_{i=1}^{n} y_i^2-\sum_{i=1}^{n} x_i y_i}$$

Plaintext Encryption after Preprocessing

During the actual calculation process, the key length can be 128, 192, or 256 bits, while the packet length remains fixed at 128 bits. The calculation process proceeds as follows:

1. Numerical Initialization

The 128-bit message packet is divided into 16 bytes and labeled accordingly[25,26].

2. Key Grouping Formula

The input key, based on the specified key length, is divided into appropriate groupings.

- For a 128-bit key: Divided into 16 bytes.
- For a 192-bit key: Divided into 24 bytes.
- For a 256-bit key: Divided into 32 bytes.

3. Internal Function (State) Solution

The internal function involves applying a specific solution to each byte in the state. It typically includes non-linear byte replacements, where a randomly selected non-zero byte, denoted as 'x,' may be replaced by another byte, denoted as 'y.'

Numerical initialization

Here, the 128 bit message packet is divided into 16 bytes and marked as

$$\text{input block } = m_0, m_1, m_2 \cdots m_{15}$$

According to the calculation result of the above formula, the key grouping formula is expressed as

$$\text{input keys } = m_0, m_1, m_2 \cdots m_{15}$$

where input block represents the input module, input key represents the input key, represents the input byte, and the internal data structure is

$$\text{input block} = \begin{pmatrix} m_0 & m_4 & m8 & m_{12} \\ m_1 & m5 & m9 & m13 \\ m_2 & mb & m10 & m14 \\ m_3 & m7 & m11 & m15 \end{pmatrix}$$

$$\text{input key } = \begin{pmatrix} k_0 & k_4 & k_8 & k_{12} \\ k_1 & k_5 & k_9 & k_{13} \\ k_2 & k_6 & k_{10} & k_{14} \\ k_3 & k_7 & k_{11} & k_{15} \end{pmatrix}$$

Internal function (state) solution

In general, the internal function is described as any byte in state. Generally x gives a nonlinear replacement byte, in which random non-0 byte x$\in f28$ may be replaced by y

$$y = \frac{A}{x} + b$$

c. Phishing Detection

The problem definition of phishing attack is a typical case ofbinary classification problem as an online communication (e.g.

website or email or e-chat) is either Phish or benign. More formally,let w be a request that needs classification i.e.

$\omega \xrightarrow{T}$ { phishing; benign}……..(1)

Then X is the anti-phishing system that takes features fi∈ w such that

$w = \sum_2^n F_i n \geqslant 0$w is non-empty set……..(2)

Thus, a request contains at least one feature (e.g. links, HTML tags, scripts, SSL certificate etc.) on which prediction of its status can be queried or classified. Because these features can range from simple to complex, the proposed model uses feature frequency assessment for feature vector composition depicted by X={x1,x2,x3,……..}which assign label y to each f ∈w, such that the label y is a binary class represented as:

$$y = \begin{cases} 1 & \text{Phishing} \\ 0 & \text{Genuine} \end{cases}$$ ……. ….(3)

Represented as

xi : f(w)→ y …….(4)

Equation 1 depicts the classification problem where, given a training data D, which contains (w1,w2,w3,w4,…….. ;wn) and each wi containsa set of features of (f1,f2,f3,…….) Also, the training data is a set of classes (C1,C2) which represents phishing and legitimate sites such that:

$C_1 = w_{ifi} \mid wi \in Dy = \text{benign}, i = 1,2, \cdots \cdot m$…….(5)

$C_2 = \omega_i F_i \mid w_i \in dy = \text{phishing}$ $i = m+1, \ldots p$ ……..(6)

Thus, each case wi∈D may be given a class ci ∈ C and is represented as a pair (wi(ci)) where ci is a class from C associated with the case Wi in the training data. Let H denote the set of classifiers for D →C; where each case ci ∈ C is given a class and the goal is to find a classifierhi ∈ H that maximizes the probability that h(ci) =c for each test case. In the proposed system, two most common machine learning classifiers for phishing classification namely, Naïve Bayes and Support Vector Machine are chosen to investigate the performance of the feature set/vector and to maximize the accuracy of our proposed approach[28,29].

d. Access Controls

Access controls are crucial for restricting data access to authorized individuals or roles within an organization. Salesforce offers granular access control mechanisms, such as role-based access control (RBAC) and permission sets, to manage user privileges and permissions. The section examines the effectiveness of these access controls in preventing unauthorized data access[30].

e. Audit Trails

Salesforce provides audit trail functionality that logs and tracks user activities and changes made to data within the system. This includes login history, setup changes, and record access logs. The preliminaries section discusses the importance of audit trails in detecting and investigating potential security incidents or data breaches[31].

f. Limitations and Considerations

While Salesforce offers robust security measures, it is important to be aware of their limitations. For example, organizations must ensure that appropriate password policies and MFA configurations are in place to mitigate the risk of weak user credentials. The section highlights these limitations and provides considerations for organizations to address potential security gaps[32,33,34].

IV. PROPOSED FRAMEWORK

The proposed framework for enhancing data security on Salesforce aims to provide organizations with a comprehensive approach to protect their valuable data. The framework encompasses multiple layers of security measures and best practices. Here are the key components of the proposed framework:

a. User Access Management

Effective user access management is crucial for ensuring data security. The framework recommends implementing strong password policies, enforcing multi-factor authentication (MFA), and regularly reviewing and revoking user access privileges. Role-based access control (RBAC) and permission sets should be utilized to grant appropriate levels of access based on user roles and responsibilities.

b. Data Encryption

To protect sensitive data stored within Salesforce, the framework emphasizes the use of data encryption techniques. It suggests implementing field-level encryption for sensitive data fields, ensuring that data is encrypted both at rest and in transit. Encryption keys should be securely managed, and encryption algorithms should adhere to industry best practices.

c. Network Security

Network security measures play a vital role in safeguarding data during transmission. The framework recommends implementing secure network protocols, such as SSL/TLS, for encrypting data in transit. Additionally, organizations should implement firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and secure network traffic.

d. Data Loss Prevention (DLP)

DLP measures help prevent the accidental or intentional loss of sensitive data. The framework suggests implementing data loss prevention tools that can monitor and control data flows, detect sensitive data patterns, and enforce data protection policies. This can include features such as data masking, redaction, and activity monitoring to ensure data integrity and prevent unauthorized data exfiltration[15,16].

To solve the DLP Data Inspection Problem, we introduce the concept of fingerprints:

To identify unique and robust features from a string;

Given a string T, we denote its fingerprints as: – SFP(T) = {FP1 , FP2 ,…, FPm(T) }

Indexing: • For each string T ∈ S that is assigned a unique string ID as SID, we generate fingerprints SFP(T), then we index SID with all fingerprints in SFP(T). • The whole indices is contained in FP-DB.

Searching + Matching: • For given T, we have SFP(T). We search SFP(T) against FP-DB to identify possible candidates (i.e., suspects) of similar strings, say, {t1 , t2 ,…, tk } •

Calculate EvalSim(T, tj) where j = 1, 2, 3,…..k

Pick those with EvalSim (T,*) ≥ X% as result

1. Fingerprints are generated from features of a given string.

2. Robust: we expect SFP(T1) ∩SFp(T2) ≠ NIL if they are similar; 3. Unique: SFP(T1 ∩ SFPT2) = NIL if they are irrelevant.

We use a score function F to describe the requirements :

$$F(b) = \sqrt{n} * (p_n - P_1) / \sqrt{\sum_{1 \le 2 \le n} (P_{i+1} - P_i)^2}$$

where b ϵ A , n is the number of occurrences of character b, and {P1 , P2…, Pn } represent all offsets of b in string.

$\sqrt{n}$measures the frequency of character b … intuitively !

The 2nd term $\frac{(p_n - P_1)}{\sqrt{\sum_{1 \le 2 \le n} (P_{i+1} - P_i)^2}}$measures its distribution.

e. Incident Response

Having a well-defined incident response plan is essential for effectively addressing security incidents. The framework recommends establishing an incident response team, defining incident response procedures, and conducting regular incident response drills. This ensures that in the event of a security incident, organizations can quickly detect, respond to, and mitigate the impact of the incident on data security.

f. Security Monitoring and Auditing

Continuous security monitoring and auditing are critical for maintaining data security on Salesforce. The framework suggests implementing security monitoring tools that can detect and alert on suspicious activities, unauthorized access attempts, and potential security breaches. Regular security audits should be conducted to assess the effectiveness of security controls and identify any vulnerabilities.

V. ALGORITHM

Step 1: Identify sensitive data: Determine the types of data that need to be secured, such as personally identifiable information (PII), financial information, or proprietary data.

Step 2: Access controls: Implement role-based access controls (RBAC) to ensure that users have the appropriate level of access to data based on their roles and responsibilities. This includes defining user profiles, permission sets, and sharing rules.

Step 3: Encryption: Implement encryption mechanisms to protect data at rest and in transit. Use industry-standard encryption algorithms to encrypt sensitive data stored in the Salesforce database and when transmitting data over networks.

Step 4: Two-factor authentication (2FA): Enable 2FA for user logins to add an extra layer of security. This requires users to provide an additional verification factor, such as a code sent to their mobile device, along with their username and password.

Step 5: Data backup and recovery: Regularly backup data and test the recovery process to ensure data can be restored in case of any data loss or system failures. Store backups securely and separate from the production environment.

Step 6: Monitor and log activities: Implement monitoring and logging mechanisms to track user activities, system events, and access attempts. This helps in detecting and investigating any suspicious activities or unauthorized access attempts.

Step 7: Security assessments and audits: Conduct regular security assessments and audits to identify vulnerabilities and ensure compliance with security standards and regulations. Address any identified issues promptly.

Step 8: Employee education and awareness: Train employees on data security best practices, such as creating strong passwords, avoiding phishing attacks, and reporting any security incidents. Regularly communicate security policies and updates to employees.

VI. MATHEMATICAL MODEL

Let:

- D = Set of sensitive data
- U = Set of users
- R = Set of roles
- P = Set of permission sets
- S = Set of sharing rules
- E = Set of encryption algorithms
- A = Set of authentication mechanisms

Variables

- **access_control(u, d, r):** Binary variable indicating whether user u has access to sensitive data d based on role r.

- **encryption(d, e):** Binary variable indicating whether sensitive data d is encrypted using encryption algorithm e.
- **two_factor_auth(u, a):** Binary variable indicating whether user u has two-factor authentication enabled using mechanism a .

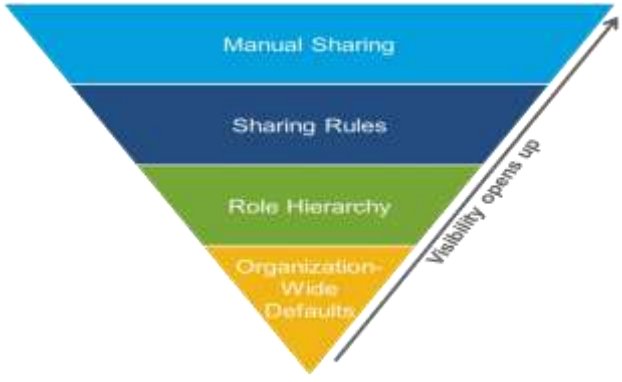
Objective Function: Maximize the overall data security on Salesforce.

Constraints:

1. **Role-based access control**
   - For each sensitive data d, the sum of access_control(u, d, r) over all users u and roles r should be equal to 1, indicating that each data is accessible by exactly one role or user.
2. **Encryption**
   - For each sensitive data d, the sum of encryption(d, e) over all encryption algorithms e should be equal to 1, indicating that each data is encrypted using exactly one algorithm.
3. **Two-factor authentication**
   - For each user u, the sum of two_factor_auth(u, a) over all authentication mechanisms a should be less than or equal to 1, indicating that each user has at most one two-factor authentication mechanism enabled.
4. **Other constraints**
   - Additional constraints can be defined based on specific security requirements, such as data backup frequency, logging thresholds, and compliance regulations.

VII. SALESFOCE DATA SECURITY MODEL — EXPLAINED VISUALLY

Salesforce offers a comprehensive and adaptable data security model to meet the diverse security requirements of real-world businesses. This model ensures the protection of data at various levels while also providing sharing tools for controlled and secure data access based on specific business needs. In this research paper, I will illustrate how Salesforce's security features synergistically function through textual explanations, as visual elements like images and GIFs cannot be directly incorporated[1,3,5].



Salesforce's data security model encompasses both powerful security features and flexible sharing tools to facilitate secure data access based on individual business needs. In this research paper, I will explore the seamless integration of these security measures by utilizing a real-world scenario. Although the use of visual aids such as images and GIFs is not possible in this context, this paper serves as an informative introduction to the Salesforce Data Security Model, providing a comprehensive understanding of its key components and their interplay.

The basics

Salesforce revolves around three fundamental components pertaining to data: objects, fields, and records. Objects function akin to tables in traditional databases, while fields resemble the columns within those tables. On the other hand, records parallel the individual rows of data within those tables. Salesforce employs object-level, field-level, and record-level security mechanisms to ensure controlled access to objects, fields, and individual records. These security measures collectively contribute to safeguarding data within the Salesforce ecosystem.

The scenario

In the given scenario, Maria, an experienced leader with a marketing background, has recently joined ABC Corp as a sales executive. As a direct report to the CEO, Maria requires access to various objects and apps within Salesforce.

Layer 1: Object-level-security

Salesforce employs object-level security to ensure that users have the necessary permissions to view objects of a specific type. Access to object-level security can be managed through two configurations: profiles and permission sets.

1.1 Profiles

Traditionally, profiles have been used in Salesforce to control object-level and field-level access. However, with the introduction of permission sets, it is now recommended to use them as the primary means of configuring object and field permissions, alongside permission set groups. While assigning each user a

profile remains mandatory for configuring other settings like page layouts and login IP restrictions, profiles should be configured with minimum access. Permission sets and permission set groups should then be utilized to grant additional permissions.

1.2 Permission sets and Permission Set Groups

In the case of Maria, being a new employee, it is necessary for an administrator to assign her to appropriate permission sets that grant access to the sales apps and related objects. Permission sets are highly recommended as the primary method for assigning object and field permissions, and here's why:

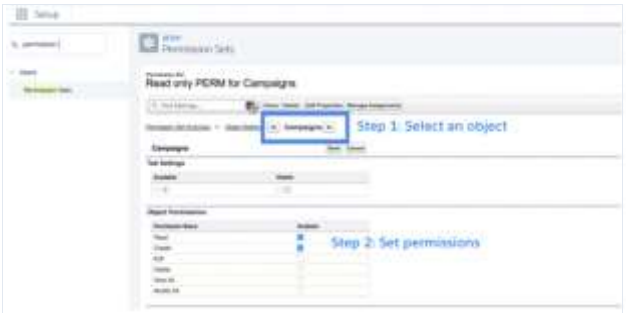
1. Flexibility: Permission sets offer greater flexibility compared to profiles. Unlike profiles, multiple permission sets can be assigned to a user. This flexibility allows for a more granular design of the security model, where functionalities can be grouped in more specific ways. Instead of grouping all object and field permissions into a single profile, permission sets enable the creation of different sets representing distinct tasks performed by a sales executive, such as lead management, opportunity approval, and more. This allows for the addition or removal of smaller permission chunks to a user at any given time.

2. Packageability: Permission sets are packageable, meaning they can be bundled and distributed as part of a package. This makes it easier to manage and deploy sets of permissions across different Salesforce instances or organizations.

3. Upgradeability: Similar to packageability, permission sets are upgradeable. When changes or enhancements are made to permission sets, they can be easily upgraded in the system without impacting other components or configurations.

To manage the potential proliferation of permission sets in an organization, permission set groups can be utilized. These groups simplify the management process by allowing multiple permission sets to be grouped together. By assigning Maria to a permission set group, she can receive the combined permissions of the grouped sets as a single artifact, streamlining the assignment process.

Overall, the flexibility, packageability, and upgradeability of permission sets make them an ideal choice for configuring object and field permissions, enabling administrators to design a fine-grained security model tailored to individual user roles and responsibilities.



Layer 2: Field-level-security

In Salesforce, granting access to objects alone is not sufficient for Maria, as she also requires access to individual fields within each object. Field-level access is controlled by profiles and permission sets. Administrators have the ability to assign read and write permissions for specific fields, or they can hide fields entirely, removing access to them for certain users. When a field is hidden using field-level security, it becomes inaccessible through any entry points, including APIs. It is considered a recommended security best practice to use field-level security instead of simply removing a field from a record page or page layout.

To manage field-level security effectively, it is recommended to utilize permission sets and permission set groups, just as with object-level security. This provides a flexible and granular approach to configuring field permissions. The graphic accompanying this text illustrates how field-level access can be granted using a permission set.

By leveraging field-level security mechanisms through permission sets, administrators can precisely control access to individual fields, ensuring that Maria has the appropriate level of access to perform her duties effectively within Salesforce.

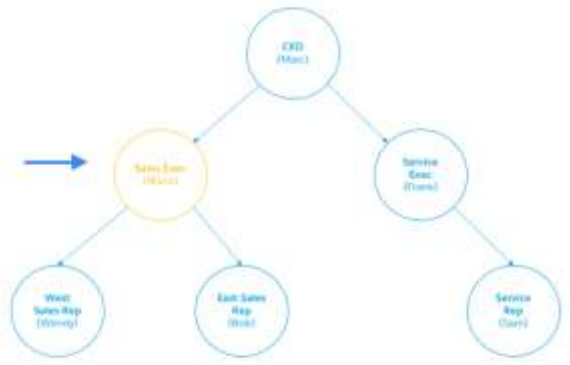
Layer 3: Record-level security

While object-level access and field-level access in Salesforce provide Maria with access to records she owns (i.e., records created by her), considering the organization structure reveals that she reports to Marc, the CEO, and supervises two sales reps, Wendy and Bob.

However, to align with the hierarchical structure and enable Maria to access records owned by

Wendy and Bob, additional security configurations are necessary. Salesforce offers various sharing tools and mechanisms to facilitate controlled access to records beyond ownership. These mechanisms can be employed to establish sharing rules, roles, or teams, allowing Maria to access relevant records based on her reporting relationships within the organization. By leveraging these sharing mechanisms, Maria can effectively collaborate with her sales reps and access the records associated with their respective roles.

This graphic illustrates the organization structure:



Record-level security, also known as the Salesforce sharing model, plays a crucial role in controlling access to records. It encompasses various mechanisms for sharing records with others and gaining access to records owned by others. Salesforce offers five methods to facilitate record sharing and access.

The first step is configuring organization-wide defaults, which establish the most restrictive level of data access as the baseline. This ensures that data is initially locked down to maintain strict security.

To provide additional access to specific users as needed, Salesforce provides a range of record-level security tools. These tools allow administrators to selectively grant access to records beyond the organization-wide defaults. By leveraging these mechanisms, organizations can precisely control record access based on business requirements and user roles.

Types of record-level security (also known as record sharing rules)

3.1 Record-level-security: organization-wide sharing defaults

In Salesforce, each record contains an "OwnerId" field that identifies the user who owns the record. Typically, the record **owner** is the individual who created it and possesses full CRUD (Create, Read, Update, Delete) access to the record. Salesforce also provides additional methods for automatically assigning ownership to users and transferring ownership between users.

It is important to note that ownership can also be granted to groups of users, such as queues. However, this particular blog post will not delve into that topic extensively.

To govern the default behavior of record access for users who do not own the record, Salesforce employs Organization-wide defaults (OWD). OWD settings control how records of a specific object (e.g., Accounts) are accessed by users at a global level.

For example, consider the following scenarios based on the OWD settings for Accounts:

1. Private: If the OWD for Accounts is set to Private, Maria would only be able to see the records she owns.

2. Public Read Only: If the OWD for Accounts is set to Public Read Only, anyone can read the record, but updates or deletions are restricted.

3. Public Read/Write: If the OWD for Accounts is set to Public Read/Write, anyone can read and update the record, but deletions are restricted.

These OWD configurations establish the initial access privileges for records, defining the baseline level of access before considering any additional sharing or permissions granted through record-level security mechanisms.

3.2 Record-level security: Role hierarchies

Within an organization, different job roles often necessitate varying levels of access to records. These roles are typically organized in a hierarchical structure, where users in higher roles should have access to the same records as users in lower roles. It's important to note that role hierarchies in Salesforce may not directly correspond to the organization's reporting structure, but rather define data access hierarchies.

Salesforce offers a convenient approach to sharing records with managers and representing role hierarchies through its role hierarchy feature. This feature enables administrators to easily configure sharing rules based on job roles and their corresponding access levels. To utilize this sharing rule, an administrator must first add a user, such as Maria, to the appropriate role within her user record. This ensures that Maria's access to records aligns with her position in the role hierarchy,

granting her access to records accessible to users in lower roles within the hierarchy.

By incorporating role hierarchies in record-level security, organizations can establish a structured and logical framework for granting record access based on job roles, fostering efficient collaboration and data sharing across the organization.

3.3 Record-level security: Sharing rules

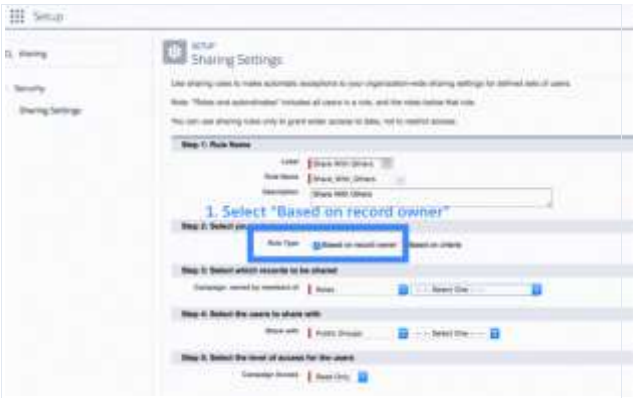
While role hierarchies facilitate upward and vertical sharing within an organization, there may be instances where lateral sharing is required. For example, there may be a need to share records owned by Maria with her peers in the service executive teams. This is where sharing rules play a crucial role by enabling lateral and ad-hoc record sharing through the use of public groups. Let's delve into the details of sharing rules.

3.3.1 Ownership-based sharing rules

Ownership-based sharing rules provide administrators with the ability to share records based on ownership by role, role-and-subordinate, and public groups. This allows for targeted sharing of records among specific user roles.

For example, using ownership-based sharing rules, it is possible to share all the records owned by individuals in the sales executive role (including Maria) with everyone in the service executive role. Similarly, it is also feasible to share all the records owned by sales executives, including their subordinates, with other designated users or groups.

By leveraging ownership-based sharing rules, administrators can define granular sharing criteria to precisely control the sharing of records, expanding the reach of data access to specific roles or groups as needed. This provides flexibility and scalability in sharing records across lateral teams and supports collaborative efforts within the organization.



This GIF demonstrates the various ownership-based sharing options that can be applied to our use case. It is important to note that a public group can be comprised of individual users, users in different roles, and other public groups. Sharing records with public groups offers a remarkably versatile approach to record sharing.

3.3.2 Criteria-based sharing rules

Criteria-based sharing rules provide users with access to records based on specific field values, regardless of the record owner. For instance, if Maria needs to interact with all accounts located in San Francisco, an administrator can establish a criteria-based sharing rule to grant Maria access to all accounts where the billing city is set to San Francisco. This ensures that Maria can effectively engage with the relevant accounts, regardless of who owns them.

3.3.3 Guest user sharing rules

A guest user sharing rule is a unique form of criteria-based sharing rule that allows unauthenticated

guest users to have read-only access to records. It is specifically designed to cater to this special scenario.

3.4 Record-level security: Manual sharing

Manual sharing serves as a mechanism for users to individually share specific records with others. This permission is accessible through the Sharing button on the record details page, empowering end-users to share specific records with designated individuals.

It's important to note that manual sharing is only available when the organization-wide defaults (OWD) for the respective object are set to private or public read-only. This is because, in scenarios where the OWD is already public read/write, there is no need for manual sharing as the access permissions are already broadly granted.

By offering the ability to manually share records, users can collaborate and selectively grant access to specific records on a case-by-case basis, ensuring that data remains secure while enabling controlled information sharing within the organization.

3.5 Record-level-security: Apex managed sharing

In certain scenarios, sharing records through the user interface or standard settings may not be sufficient, requiring the implementation of Apex code. One such instance is when Maria identifies a pattern where premium accounts consistently have a Customer Service lead user assigned to them. As a result, she finds herself manually sharing records with this user frequently. To streamline this process, Maria has approached the admin team to automate the sharing, but traditional sharing rules cannot achieve this. Consequently, the development team needs to create an Apex trigger that implements Apex managed sharing. This custom code will facilitate the automatic sharing of records based on specified conditions, alleviating the need for manual intervention and improving efficiency.

VIII. CONCLUSION

Salesforce provides three layers of security with lots of flexibility to accommodate virtually any business need. Profiles and permission sets controls object-level and field-level access, with permission sets being our recommended tool to use. Permission set groups are the next generation way to model job roles instead of profiles.

Further, there are five types of record-level security: org-wide defaults, role hierarchy sharing, sharing rules, manual sharing, and Apex-based sharing. These five control access to sets of records or even an individual record to people who don't own those records.

The conclusion section summarizes the key findings and insights obtained from the research paper on ensuring data security on Salesforce. Here's an elaboration on the key aspects covered in the conclusion:

a. Importance of Data Security on Salesforce

The conclusion emphasizes the critical importance of data security on Salesforce, given the increasing reliance on the platform for managing customer data. It highlights the potential risks and threats that organizations face, including data breaches and unauthorized access, underscoring the need for robust security measures to protect sensitive information.

b. Effectiveness of the Proposed Framework

The conclusion highlights the effectiveness of the proposed framework for enhancing data security on Salesforce. It reflects on the multi-layered approach encompassed by the framework, which covers user access management, data encryption, network security, data loss prevention, incident response, and security monitoring. The conclusion asserts that implementing these measures can significantly strengthen data security on the platform.

c. Continuous Vigilance and Adaptation

The conclusion emphasizes the importance of continuous vigilance and adaptation in the realm of data security. It acknowledges that the security landscape is dynamic, with new threats emerging and technology evolving. Organizations should remain proactive in keeping up with the latest security updates, best practices, and regulations to ensure the ongoing protection of their data on Salesforce.

d. Recommendations and Future Research

In the conclusion, recommendations are provided for organizations utilizing Salesforce to enhance their data security practices. These recommendations may include implementing regular security audits, conducting employee training on security awareness, staying informed about Salesforce's security features and updates, and actively participating in the Salesforce community for sharing knowledge and best practices.

Additionally, the conclusion identifies potential areas for future research in the field of data security on Salesforce. It encourages further exploration of emerging technologies and methodologies for data protection, as well as studying the effectiveness of the proposed framework in real-world scenarios and assessing its adaptability to evolving security threats.

Overall, the conclusion underscores the significance of prioritizing data security on Salesforce, highlights the effectiveness of the proposed framework, and provides recommendations for organizations to strengthen their data security practices. By following

these recommendations and remaining proactive in addressing emerging security challenges, organizations can ensure the confidentiality, integrity, and availability of their data on Salesforce.

REFERENCES

[1] Salesforcesecurity guide. Available at: https://help.salesforce.com/articleView?id=sf.security_guide.htm&type=5/.

[2] https://www.salesforce.com/content/dam/web/en_us/www/documents/white-papers/salesforce-security-architecture.pdf.

[3] Ren, L., & Micro, T. (2015).IoT security: problems, Challenges and Solution. Santa Clara, CA, 1-32.

[4] Shelar, D., Andhare, P., Gaikwad, S., & Thakre, P. A Mathematical Model For Access Control Through Trust Management In Ubiquitous Computing.

[5] S. Srivastava, M. Haroon, and A. Bajaj, "Webdocument information extraction using class attribute approach," 2013 4th International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, 2013, pp. 17-22, Doi: 10.1109/ICCCT.2013.6749596.

[6] Haroon, M., Tripathi, M. M., & Ahmad, F. (2020).Application of Machine Learning in Forensic Science. In Critical Concepts, Standards, and Techniques in Cyber Forensics (pp. 228-239). IGI Global.

[7] R. Khan, M. Haroon and M. S. Husain, "Different technique of load balancing in distributed system: A review paper," 2015 Global Conference on Communication Technologies (GCCT), Thuckalay, India, 2015, pp. 371-375, Doi: 10.1109/GCCT.2015.7342686.

[8] M. Haroon and M. Husain, "Interest Attentive Dynamic Load Balancing in distributed systems," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIA Com), New Delhi, India, 2015, pp. 1116-1120.

[9] Khan, R., Haroon, M., & Husain, M. S. (2015, April). Different technique of load balancing in distributed system: A review paper. In 2015 Global Conference on Communication Technologies (GCCT) (pp. 371-375).IEEE.

[10] Khan, W., &Haroon, M. (2022). An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks. International Journal of Cognitive Computing in Engineering, 3, 153-160.

[11] Suklabaidya, M., Das, A., & Das, B. (2018).A cryptography model using hybrid encryption and decryption techniques. International Journal of Computational Intelligence &IoT, 2(4).

[12] Husain, M. S., & Haroon, D. M. (2020).An enriched information security framework from various attacks in the IoT. International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN, 2347-5552.

[13] Khan, W., &Haroon, M. (2022). An efficient framework for anomaly detection in attributed social networks. International Journal of Information Technology, 14(6), 3069-3076.

[14] Haroon, M., & Husain, M. (2013).Analysis of a Dynamic Load Balancing in Multiprocessor System. International Journal of Computer Science engineering and Information Technology Research, 3(1).

[15] Anshari, M., Almunawar, M. N., Lim, S. A., & Al-Mudimigh, A. (2019). Customer relationship management and big data enabled: Personalization & customization of services. Applied Computing and Informatics, 15(2), 94-101.

[16] Husain, Mohammad Salman and Haroon, Dr. Mohammad, An Enriched Information Security Framework from Various Attacks in the IoT (JULY 12, 2020). International Journal of Innovative Research in Computer Science & Technology (IJIRCST) ISSN: 2347-5552, Volume-8, Issue-3, May 2020, Available at SSRN: https://ssrn.com/abstract=3672418

[17] Haroon, M., & Husain, M. (2013). Analysis of a Dynamic Load Balancing in Multiprocessor System. International Journal of Computer Science engineering and Information Technology Research, 3(1).

[18] Khan, W. (2021). An exhaustive review on state-of-the-art techniques for anomaly detection on attributed networks. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 6707-6722.

[19] Boban, M., Ivkovic, M., Jevtic, V., & Milanov, D. (2011, April). The data quality in CRM systems: strategy and privacy. In 1st International Conference on Information Systems and Technologies (ICIST 2011), Tebessa, Algeria (pp. 158-163).

[20] Husain, M. S. (2020). A review of information security from consumer's perspective especially in online transactions. International Journal of Engineering and Management Research, 10.

[21] Romano Jr, N. C., & Fjermestad, J. (2007).Privacy and security in the age of electronic customer relationship management. International Journal of Information Security and Privacy (IJISP), 1(1), 65-86.

[22] Osarenkhoe, A., &Bennani, A. E. (2007).An exploratory study of implementation of customer relationship management strategy. Business process management journal.

[23] Cho, Y., Im, I., & Hiltz, R. (2003).The impact of e-services failures and customer complaints on electronic commerce customer relationship management. The Journal of Consumer Satisfaction, Dissatisfaction and Complaining Behavior, 16, 106-118.

[24] Khan, N., & Haroon, M. (2022).Comparative Study of Various Crowd Detection and Classification Methods for Safety Control System. Available at SSRN 4146666.

[25] Zeng, Y. E., Wen, H. J., & Yen, D. C. (2003).Customer relationship management (CRM) in business-to-business (B2B) e-commerce. Information Management & Computer Security, 11(1), 39-44.

[26] Haroon, M., Tripathi, M. M., & Ahmad, F. (2020). Application of Machine Learning In Forensic Science. In Critical Concepts, Standards, and Techniques in Cyber Forensics (pp. 228-239).IGI Global.

[27] Soltani, Z., & Navimipour, N. J. (2016). Customer relationship management mechanisms: A systematic review of the state of the art literature and recommendations for future research. Computers in Human Behavior, 61, 667-688.

[28] Wasim Khan, Mohammad Haroon, An unsupervised deep learning ensemble model for anomaly detection in static attributed social networks, International Journal of Cognitive Computing in Engineering, Volume 3,2022,Pages 153-160,ISSN 2666-3074,

[29] https://doi.org/10.1016/j.ijcce.2022.08.002

[30] Tripathi, M. M., Haroon, M., & Ahmad, F. (2022).A survey on multimedia technology and internet of things. Multimedia Technologies in the Internet of Things Environment, Volume 2, 69-87.

[31] Peppard, J. (2000). Customer relationship management (CRM) in financial services. European Management Journal, 18(3),312-327.

[32] Siddiqui, Z. A., & Haroon, M. (2022). Application of artificial intelligence and machine learning in blockchain technology. In Artificial Intelligence and Machine Learning for EDGE Computing (pp. 169-185). Academic Press

[33] Khan, N., & Haroon, M. (2023). A Personalized Tour Recommender in Python using Decision Tree. International Journal of Engineering and Management Research, 13(3), 168-174.

[34] Haroon, M., Misra, D. K., Husain, M., Tripathi, M. M., & Khan, A. (2023). Security Issues in the Internet of Things for the Development of Smart Cities. In Advances in Cyberology and the Advent of the Next-Gen Information Revolution (pp. 123-137). IGI Global.

[35] Rud, O. P. (2001). Data mining cookbook: modeling data for marketing, risk, and customer relationship management. John Wiley & Sons.