



**sasi** INSTITUTE OF  
autonomous TECHNOLOGY &  
ENGINEERING  
TADEPALLIGUDEM

Accredited by **NBA & NAAC** with **"A" Grade**  
Recognised by **UGC** under section 2(f) & 12(B)  
Approved by **AICTE** - New Delhi  
Permanently Affiliated to **JNTUK, SBTET**  
Ranked as **"A" Grade** by Govt. of A.P.

# **INTERNSHIP REPORT ON** **KEEP DATA SECURE IN A RECRUITING APP**

**BACHELOR OF TECHNOLOGY**  
**IN**

**INFORMATION TECHNOLOGY**  
**BY**

**TANINKI PRASANNASAI**

**REG NO: 19K61A1249**

**LECTURER IN CHARGE:**

**Dr. A.V.N CHANDRA SEKHAR**

**PROFESSOR**

**SUBMISSION DATE:**

## **ABSTRACT**

Salesforce Labs is a program that lets salesforce.com engineers, professional services staff & other employees share AppExchange apps they've created with the customer community. Inspired by employees' work with customers of all sizes and industries, these apps range from simple utilities to entire vertical solutions. Salesforce Labs apps are free to use, but are not official salesforce.com products, and should be considered community projects - these apps are not officially tested or documented. For help on any Salesforce Labs app please consult the Salesforce message boards - salesforce.com support is not available for these applications. From the posting of a new position through the interviews aimed at filling it, Recruiting lets you track your company's job postings on employment websites and evaluate job applications. It gives you a single location from which to manage the scheduling of interviews, and you'll be able to easily see what kind of progress you're making toward filling a particular position. Recruiting gives hiring managers and recruiters at small to medium-sized companies one place they can go to monitor the candidate pipeline and see listings of positions and candidates. By deploying it, your company can extend its salesforce.com solution to gather measurable data to better target its recruiting efforts.

# **TABLE OF CONTENTS**

## **ABSTRACT**

<b>1. INTRODUCTION.....</b>	<b>1</b>
<b>1.1 CREATE CUSTOM PROFILES .....</b>	<b>1</b>
<b>1.2 CREATE PROFILES .....</b>	<b>2</b>
<b>1.3 CREATE AN HR RECRUITER PROFILE AND SET ITS OBJECT PERMISSIONS.....</b>	<b>2</b>
<b>1.4 RESTRICT DATA ACCESS WITH FIELD-LEVEL SECURITY, PERMISSION SETS, AND SHARING SETTINGS.....</b>	<b>3</b>
<b>1.4.1 CREATE PERMISSION SETS.....</b>	<b>3</b>
<b>1.4.2 CREATE A NEW PERMISSION SET FOR HIRING MANAGERS .....</b>	<b>3</b>
<b>1.4.3 MODIFY FIELD-LEVEL SECURITY .....</b>	<b>5</b>
<b>1.4.4 NOW SET PERMISSIONS .....</b>	<b>5</b>
<b>1.4.5 CREATE SHARING SETTINGS.....</b>	<b>6</b>
 <b>2. LITERATURE REVIEW .....</b>	 <b>8</b>
<b>2.1 OBJECTIVES .....</b>	<b>9</b>
<b>2.2 SCOPE.....</b>	<b>9</b>
 <b>3. METHODOLOGY.....</b>	 <b>10</b>
<b>3.1 PROPOSED SYSTEM .....</b>	<b>10</b>
<b>3.2 BENEFITS OF PROPOSED SYSTEM.....</b>	<b>10</b>
<b>3.3 ACTIVITY DIAGRAM.....</b>	<b>11</b>
<b>3.4 WORKING OF THE SYSTEM.....</b>	<b>11</b>
<b>3.5 SYSTEM FEASIBILITY .....</b>	<b>12</b>
<b>3.5.1. ECONOMICAL .....</b>	<b>12</b>
<b>3.5.2. TECHNICAL:.....</b>	<b>12</b>
<b>3.5.3. BEHAVIORAL:.....</b>	<b>12</b>
<b>3.6 APPLICATION DESIGN .....</b>	<b>13</b>
<b>3.6.1 ARCHITECTURAL DESIGN.....</b>	<b>13</b>

3.6.2 GET STARTED WITH SHIELD PLATFORM ENCRYPTION...	13
3.6.3 ENABLE SHIELD PLATFORM ENCRYPTION .....	14
3.6.4 ASSIGN PERMISSIONS AND CREATE A TENANT SECRET ASSIGN PERMISSIONS .....	15
3.6.5 GENERATE A TENANT SECRET .....	16
3.6.6 KEY HYGIENE: MANAGEMENT BEST PRACTICES.....	17
4. DISCUSSION .....	18
5. CONCLUSION.....	19
6. FUTURE ENHANCEMENT .....	24
7. BIBLIOGRAPHY .....	30

## LIST OF FIGURES

<b>1.3.1</b>	<b>Create an hr recruits' profile and set its object.....</b>	<b>3</b>
<b>1.4.2.1</b>	<b>Create a new permission set for hiring managers.....</b>	<b>4</b>
<b>1.4.4.1</b>	<b>New set permission.....</b>	<b>6</b>
<b>3.3.1</b>	<b>Activity diagram.....</b>	<b>11</b>
<b>3.6.1.1</b>	<b>Architectural Design.....</b>	<b>13</b>
<b>3.6.3.1</b>	<b>Enable Shield platform encryption.....</b>	<b>15</b>
<b>3.6.5.1</b>	<b>Generate a tenant secret.....</b>	<b>16</b>
<b>3.6.6.1</b>	<b>Key hygiene management best practice.....</b>	<b>17</b>

# **CHAPTER 1: INTRODUCTION**

Recruitment is a process to discover the sources of manpower to meet the requirement of the staffing schedule and to employ effective measures for attracting that manpower inadequate numbers to facilitate effective selection of efficient personnel. From the posting of a new position through the interviews aimed at filling it, Recruiting lets you track your company's job postings on employment websites and evaluate job applications. It gives you a single location from which to manage the scheduling of interviews, and you'll be able to easily see what kind of progress you're making toward filling a particular position. Recruiting gives hiring managers and recruiters at small to medium-sized companies one place they can go to monitor the candidate pipeline and see listings of positions and candidates. By deploying it, your company can extend its salesforce.com solution to gather measurable data to better target its recruiting efforts.

Cloud recruiting has fundamentally changed the way recruitment operates. Availability of cloud-based recruitment software solutions has significantly increased productivity and diminished administrative costs of businesses of all sizes. A cloud recruitment software can be accessed anywhere through any device, which gives a lot of flexibility to recruiters and hiring managers alike. In other words, with a cloud-based recruitment software, you can always stay on top of your game. With low capital investment, even a smaller business can streamline and automate their hiring processes. An applicant tracking software takes away the hassle of tracking scattered recruitment data. You can centralize your resume database, candidate communication and reports in one single unified platform. Save time, increase visibility and reduce costs through a cloud-based recruitment software.

## **1.1 CREATE CUSTOM PROFILES**

Update field-level security and create permission sets in an HR recruiting app so that sensitive data can be viewed only by those who need it.

Further restrict data access in the app by changing sharing settings.

You continue customizing AW Computing's Recruiting app, which the HR team uses as they work to place applicants into open positions in the company. Ling Wu, the vice president of HR, wants to be sure that those who are using the app only see the data they need to see.

The first step is creating an HR Recruiter profile and setting up the required data access according to Ling's specifications. It's best practice to not assign standard profiles to users. Instead, even if you're not making any changes, clone the Standard Profiles and assign the clones to users. That way, if a user needs permissions or access to a custom object in the future, the cloned profiles can be updated easily.

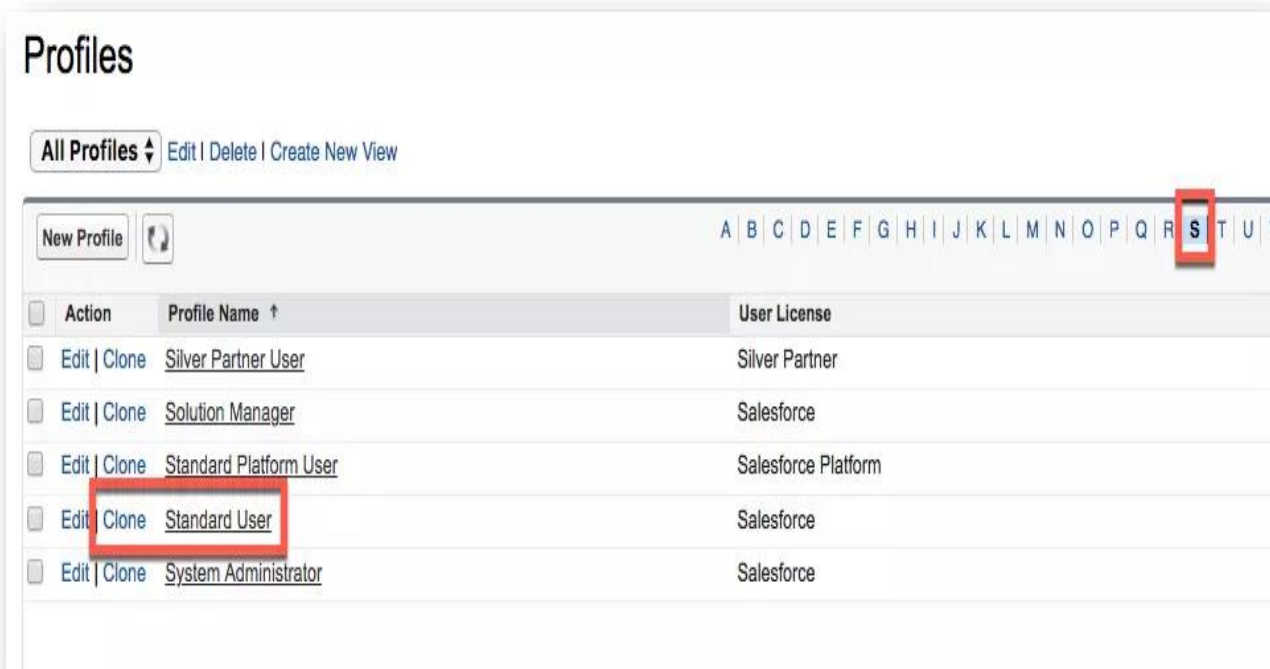
## 1.2 CREATE PROFILES

Before creating the new profile, customize how profiles are viewed

1. From Setup enter **User Management Settings** in the Quick Find box, and select **User Management Settings**.
2. Set Enhanced Profile User Interface to **Disabled** (if it's not already).

## 1.3 CREATE AN HR RECRUITER PROFILE AND SET ITS OBJECT PERMISSIONS

1. From Setup enter **Profiles** in the Quick Find box, and select **Profiles**.
2. From the list of profiles, find **Standard User**
3. Click Clone
4. For Profile Name, enter HR Recruiter.
5. Click Save.
6. While still on the HR Recruiter profile page, then click Edit
7. Scroll down to Custom Object Permissions and change the Basic Access for each object to reflect the table below, provided by the Ling.
8. Click Save.



**Fig 1.3.1:** Create an hr recruits profile and set its object

You continue tightening data security by adjusting field-level security, creating permission sets, and creating sharing settings.

## 1.4 RESTRICT DATA ACCESS WITH FIELD-LEVEL SECURITY, PERMISSION SETS, AND SHARING SETTINGS

### 1.4.1 CREATE PERMISSION SETS

Permission sets grant additional permissions to specific users, on top of their existing profile permissions, without having to modify existing profiles, create new profiles, or grant an administrator profile where it's not necessary.

### 1.4.2 CREATE A NEW PERMISSION SET FOR HIRING MANAGERS

1. From Setup, enter **Permission Sets** in the Quick Find box, and select **Permission Sets**.
2. Click New, and enter the details.

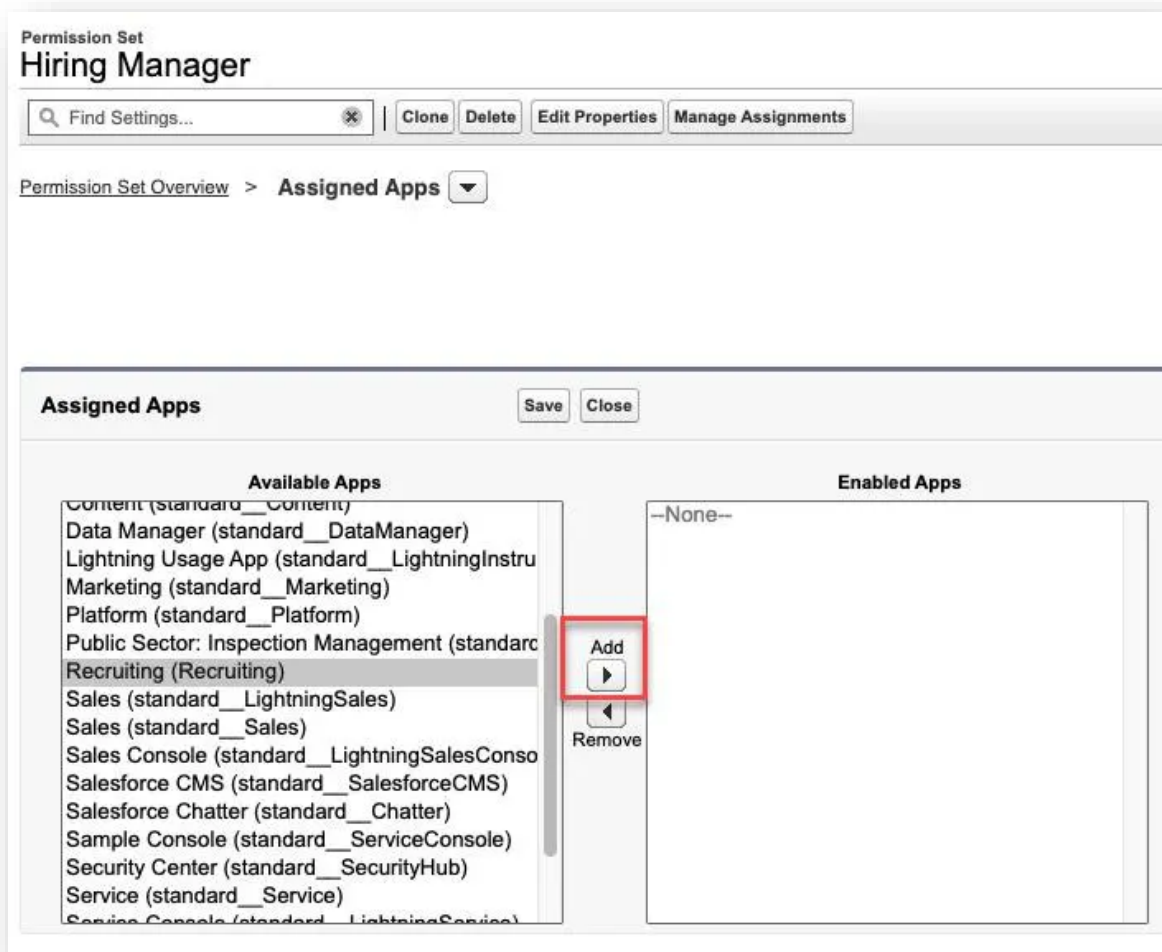


Field Label: **Hiring Manager**


Description: Temporary permission set for those Hiring Managers that need to interview candidates for positions in their department.

License: Salesforce

3. Click **Save**
4. Click **Assigned Apps** in the Apps section, then click **Edit**.
5. Select **Recruiting** from the Available Apps list and click **Add**.



**Fig 1.4.2.1:** Create a new permission set for hiring managers

1. Click **Save**.
2. click the  next to **Assigned Apps** and select **Object Settings**.
3. Select **Interviewers** from the object list, and click **Edit**.
4. Select **Visible** under Tab Settings.

5. Select **Read**, **Create**, and **Edit** from the Object Permissions list.
6. Click **Save**.
7. Repeat steps 8-11 for the **Job Applications**, **Job Postings**, **Job Posting Sites**, **Positions**, and **Reviews** objects. Set the permissions to reflect what is shown in this table provided by Ling Wu.

### 1.4.3 MODIFY FIELD-LEVEL SECURITY

All standard objects have a predefined set of fields to capture common business information. While they can't be deleted, field-level security can make them invisible. Field-level security controls which fields a profile or permission set can view and edit, overrides any less-restrictive field access, and controls settings in page layouts and search layouts.

Field-level security is universally enforced regardless of how a user is accessing Salesforce—page layout, related lists, report, and so forth. For this reason, field-level security is the preferred way to secure sensitive and confidential information, like salary ranges HR recruiters and hiring managers work with in their app

Start by setting field-level security for Salary Range field:

1. From Setup, click **Object Manager**, and select **Position**.
2. Click **Fields & Relationships**, then select **Salary Range**.
3. Click **Set Field-Level Security**.
4. For HR Recruiter and System Administrator, select **Visible**. (Ensure Visible is deselected for all other profiles.)
5. Click **Save**.

### 1.4.4 NOW SET PERMISSIONS

1. From Setup, enter **Permission Sets** in the Quick Find box, and 1. select **Permission Sets**.
2. Select **Hiring Manager**.
3. Click **Object Settings** in the Apps section.
4. Click **Positions** from the list of object names, and click **Edit**.
5. Under Field Permissions, select **Read Access** and **Edit Access** for Salary Rang

## 6. Click Save

### Field Permissions

Field Name	Read Access	Edit Access
Approval Status	<input type="checkbox"/>	<input type="checkbox"/>
Created By	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Department	<input type="checkbox"/>	<input type="checkbox"/>
Education	<input type="checkbox"/>	<input type="checkbox"/>
Hiring Manager	<input type="checkbox"/>	<input type="checkbox"/>
Job Description	<input type="checkbox"/>	<input type="checkbox"/>
Last Modified By	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Legacy Position Number	<input type="checkbox"/>	<input type="checkbox"/>
Location	<input type="checkbox"/>	<input type="checkbox"/>
Operating Systems	<input type="checkbox"/>	<input type="checkbox"/>
Owner	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Pay Grade	<input type="checkbox"/>	<input type="checkbox"/>
Programming Languages	<input type="checkbox"/>	<input type="checkbox"/>
Record Type	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Related Position	<input type="checkbox"/>	<input type="checkbox"/>
Salary Range	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Skills Required	<input type="checkbox"/>	<input type="checkbox"/>
Status	<input type="checkbox"/>	<input type="checkbox"/>
Title	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Fig 1.4.4.1:** New set permission

## 1.4.5 CREATE SHARING SETTINGS

In order to access a record, users must have the appropriate object permission on their profile or a permission set. By changing sharing settings from the organization-wide defaults, you set the default level of access users have to records they do not own in each object.

Ling Wu would like job postings to be the only HR custom object with public access. Achieve this by changing the organization-wide default sharing settings.

Set the organization-wide defaults for Recruiting app objects:

1. From Setup, enter **Sharing Settings** in the Quick Find box and select **Sharing Settings**.
2. Click **Edit** in the Organization-Wide Defaults section.
3. Select **Private** for the Candidate object.
4. Select **Private** for the Interviewer object.
5. Select **Private** for the Job Application object.
6. Select **Public Read Only** for the Job Posting Site object.
7. Select **Private** for the Position object.
8. Click **Save**.

By creating a custom profile, creating permission sets, updating field-level security, and modifying organization-wide default sharing settings, you've made AW Computing's recruiting app a more secure tool. Ling Wu can rest easy knowing that her team—and anyone else accessing the app—will only see the data they're authorized to see.

## **CHAPTER 2: LITERATURE REVIEW**

Cloud Computing is a technology where the computer resources like hardware and software are provided as a service over the internet. The information used is stored on computers somewhere else instead of local PC and can be accessed from anywhere at any time. Due to this, the shifting of business applications from traditional software to cloud has increased tremendously. Traditional business applications are very expensive and complicated. The hardware and software required to run them are daunting. A whole team of experts is needed to install, configure, test, run, secure, and update them. With cloud computing, all these headaches are automatically eliminated because one need not require managing the hardware and software—experienced vendor like force.com handles this responsibility.

Cloud computing does not have any definition which is commonly accepted yet. The five important features of cloud computing given by the National Institute of Standards and Technology (NIST) are self-service on demand, resource pooling, broad network access, rapid expansion, and measured service. Cloud-based applications cost less. With a cloud app, we just need to open a browser, log in, do the customization, and start to use it. It is seen that some of the world's largest companies have shifted their applications to the cloud with salesforce.com after rigorously testing the reliability and security of their infrastructure. A number of terminologies like SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) have come up with the evolution of cloud computing. The concept of cloud-based services is hierarchically built from bottom to top in the order of IaaS, PaaS and SaaS. Virtualization is such a technology that goes hand in hand with the concept of cloud computing. It is this technology that complements cloud services specially in the form of PaaS and SaaS where one physical infrastructure contains services or platforms to deliver a number of cloud users simultaneously. Security in cloud is anytime good than other traditional systems.

## **2.1 OBJECTIVES**

1. To develop a Recruitment Application that helps the HR to conduct recruitment process and assign positions to hired candidates.
2. To provide the storage to store the data.
3. To remove the manual creating multiple sheets which consume lot of time and hard work.
4. To provide the facility to HR to access the list of candidates and able to select the candidates that fulfil the requirements of the organization

## **2.2 SCOPE**

This application automates the recruitment process and make it easy and simple. Recruitment application provides HR to access the list of candidates and able to select the candidates that fulfil the requirements of the organization. This application keeps the record of the candidates who are selected in each step of selection process. HR can assign positions to selected candidates, their salary, location, duration and job description. This application provides HR to track the candidate details before and after the HR can send them email about location, job profile, salary details and new updates about the company.

## **CHAPTER 3: METHODOLOGY**

### **3.1 PROPOSED SYSTEM**

To solve this problem Recruitment application not only tracks the candidates but also it can automate the interview procedure to recruit the candidate. This application provides the auto mail generation to shortlisted candidates. These sites do not provide to storage to store your data. This application holds the list of selected students after each round of interview. This application easily accessible anywhere, anytime there is no need to keep this application all your data stored on cloud. You can also access it through your mobile device only you need to install Sales force mobile app.

Development of an application for recruiting candidates for the company will allow it to move away from the Microsoft Word documents and Microsoft Excel spreadsheets that it has traditionally used, to an application that's available on demand. Thus this “Recruiting App” will be beneficial for hiring of candidates in company thus saving manual efforts and time. This Recruiting App will be developed in Cloud with force.com platform using Visual Force framework and Apex language.

### **3.2 BENEFITS OF PROPOSED SYSTEM**

1. Improves recruiter's productivity
2. This App is built on Force.com i.e., cloud platform. Therefore, it also inherits Force.com platform's benefits stated above
3. Through this app the candidates will get reviews of the recruiters which will help them to improve.
4. Through a feature called CHATTER, candidates can get updates like change in location, etc.
5. Direct interaction between employees of company & candidates is now possible through this app
6. This app also provides Automatic Report generation about candidate reviews, hired positions, etc.

### 3.3 ACTIVITY DIAGRAM

#### Recruiting App

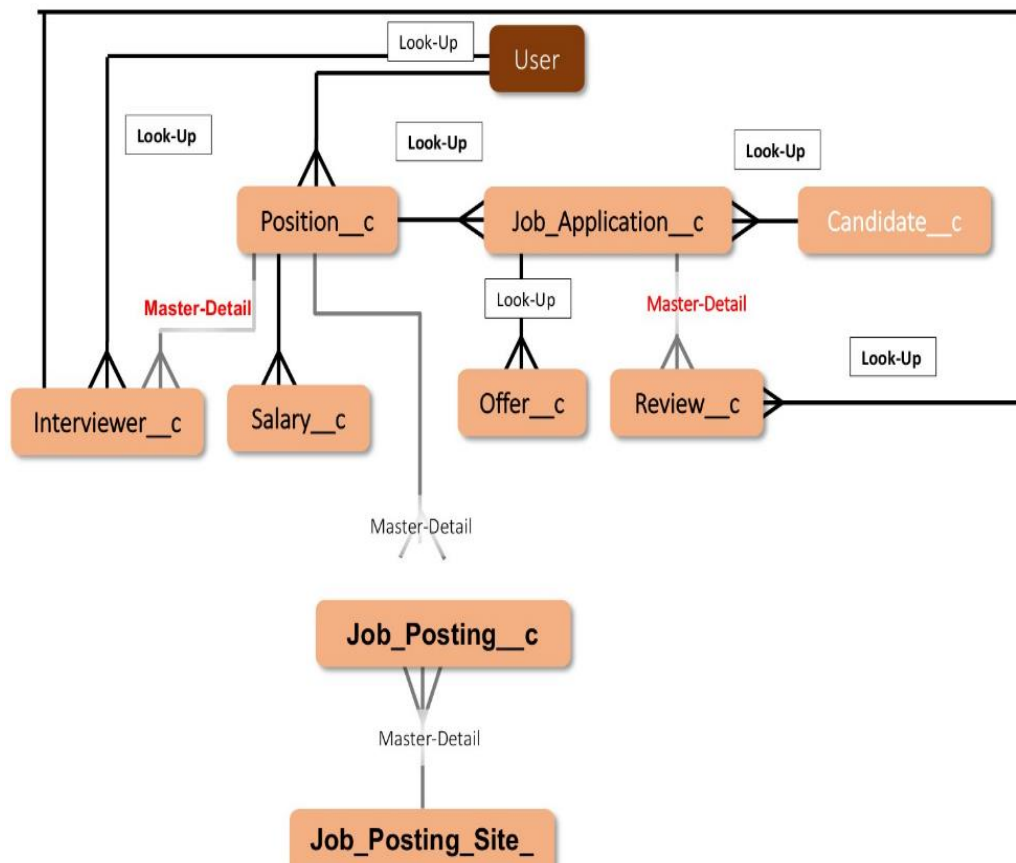


Fig 3.3.1: Activity diagram

### 3.4 WORKING OF THE SYSTEM

Firstly, the candidates looking for the job will register to this app. With any job position available in company the HR will post it on the app. The candidate can search for appropriate jobs and upload their resumes. Based on the resumes first round of short-listing candidates will be done. The information of candidates in the resumes will be extracted through the system and will be checked if it fits in the criteria set by the company. This extraction of information from the resumes will be done using the workflow rules, validation rules and SOQL (Sales force Object Query Language)



The candidates who satisfy the criteria are notified through automatic email-alerts. The candidates will be called for interview. Based on interview, final selection of candidates will be done and HR will display their results through the app. Based on their results reports will be generated and candidates can check their status, reviews of recruiters about them, etc. on the app. The Recruiting App will also have Google Map Integration which will help candidates find exact location of company and where the branches of company are located. It will also be useful to company through which they can find how many candidates are applying from which city, etc.

### **3.5 SYSTEM FEASIBILITY**

#### **3.5.1. ECONOMICAL:**

In economic feasibility, cost benefit analysis is done in which expected costs and benefits are evaluated. Economic analysis is used for evaluating the effectiveness of the proposed system. As the name suggests, it is an analysis of the costs to be incurred in the system and benefits derivable out of the system.

#### **3.5.2. TECHNICAL:**

The objective of a feasibility study is to find out if an information system project can be done and to suggest possible alternative solutions. A large part of determining resources has to do with assessing technical feasibility. It considers the technical requirements of the proposed project.

#### **3.5.3. BEHAVIORAL:**

There is simple form to fill and service requires no ambiguous entries, all the behavioural entries are simple and GUI based. The application should be used by Admin to feed the application with reliable and error free data to generate correct results.

## 3.6 APPLICATION DESIGN

### 3.6.1 ARCHITECTURAL DESIGN

Architectural Design is a concept that focuses on components or elements of a structure. An architect is generally the one in charge of the architectural design. They work with space and elements to create a coherent and functional structure. An architecture model encompassing data architecture and program structure is created during architectural design. In addition, component properties and relationship (interactions) are described.

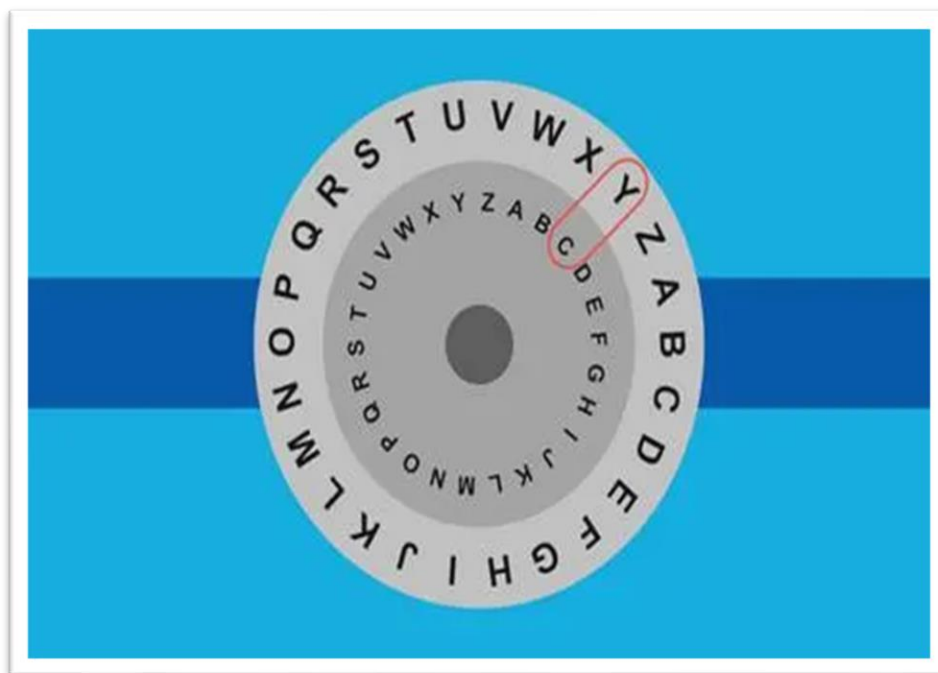


Fig 3.6.1.1: Architectural Design

### 3.6.2 GET STARTED WITH SHIELD PLATFORM ENCRYPTION

#### A. Encryption

At its most basic level, encryption scrambles information so that only those people with the right decoder key can unscramble it. These scrambling mechanisms vary in complexity. Some use simple substitution, like exchanging a number for a letter. For example, if we used this method with the encryption key in the graphic below, “Trailhead” would look like “Overplied”.

Systems use complex algorithms that use multiple keys to scramble and unscramble data. In this way, encryption helps prevent unauthorized people from accessing your data.

### **3.6.3 ENABLE SHIELD PLATFORM ENCRYPTION**

Salesforce offers you two ways to encrypt data. Classic encryption is included in the base price of your Salesforce license. With classic encryption, you can protect a special type of custom text field that you create for data you want to encrypt. The custom field is protected with industry-standard 128-bit Advanced Encryption Standard (AES) keys.

Shield Platform Encryption is available for free in Developer Edition orgs. All other editions require you to purchase a license. With Shield Platform Encryption, you can encrypt all kinds of confidential and sensitive data at rest on the Salesforce Platform. “At rest” means any data that’s inactive or stored in files, spreadsheets, standard and custom fields, and even databases and data warehouses. The data is encrypted with a stronger 256-bit AES key, and subscribers can manage access to their data with a wider range of keys and permissions. Shield Platform Encryption even allows you to search for encrypted data in databases.

Shield Platform Encryption gives customers an encryption advantage because it allows you to prove compliance with regulatory and industry requirements and show that you meet contractual obligations for securing private data in the cloud.

Turning on Shield Platform Encryption is as easy as 1-2-3.

Provision your license. Contact Salesforce to get one. Shield Platform Encryption is automatically available in Developer Edition orgs created on or after the Summer of 2015.

Assign permissions. To enable Shield Platform Encryption, you need the Customize Application and Manage Encryption Keys permissions. After you enable encryption, you can give others permission to complete administration tasks on the Encryption Policy page. However, you likely don’t want everyone managing encryption keys. Assign permissions with these scenarios in mind.

	Manage Encryption Keys	Customize Application	View Setup and Configuration	Manage Certificates	Modify All Data
View Platform Encryption Setup pages		✓	✓		
Edit Platform Encryption Setup pages, excluding Key Management and Advanced Settings		✓			
Generate, destroy, export, and import tenant secrets	✓				
Query TenantSecret object via the API	✓				
Edit, upload, and download HSM-protected certificates with the Shield Platform Encryption Bring Your Own Key service	✓			✓	
Edit options on the Advanced Settings page					✓

**Fig 3.6.3.1:** Enable Shield platform encryption

For example, as an admin, assign yourself the View Setup and Configuration permission. This lets you enable encryption features for fields, files, attachments, and apps.

Enable Shield Platform Encryption for your org. When you have your license and permissions set up, you can enable Shield Platform Encryption on your orgs. You then create org-specific tenant secrets and customize your encryption settings for each org.

### 3.6.4 ASSIGN PERMISSIONS AND CREATE A TENANT SECRET ASSIGN PERMISSIONS

Because Doc Mosely's going to be busy with patients, he asked you to handle the Shield Platform Encryption setup. Doc Mosey goes through the steps to give you the "Customize Application" and "Manage Encryption Keys" permissions.

1. From Setup, enter Permission Sets in the Quick Find box, then select **Permission Sets**.
2. Click **New**.
3. Create a label for the set of permissions, for example, Key Manager. The API name populates with a variation of your chosen label.

4. Click **Save**.
5. In the System section of the Key Manager page, select **System Permissions**.
6. Click **Edit**, and enable the Customize Application and Manage Encryption Keys permissions.
7. Click **Save**.
8. From Setup, enter Users in the Quick Find box, then select **Users**.
9. Select the name you want in the User list (in this case, that's yours
10. Scroll down to Permission Set Assignments, and select **Edit Assignments**.
11. Select **Key Manager**, then add it to the Enabled Permission Sets list.
12. Click **Save**.

### 3.6.5 GENERATE A TENANT SECRET

As we learned in the last unit, tenant secrets are used to derive your encryption keys. They work with the Salesforce-generated master secret, but your tenant secret is specific to your org. In this way, the data in each of your orgs is encrypted with keys unique to that org.



**Fig 3.6.5.1:** Generate a tenant secret

1. From Setup, in the Quick Find box, enter Platform Encryption, and then select **Key Management**.
2. Select **Data in Salesforce** from the Choose Tenant Secret Type list. Tenant secret types allow you to specify which kind of data you want to encrypt with a tenant secret. We'll start by encrypting data in the core Salesforce database for now.
3. Select **Generate Tenant Secret**

It's as easy as that. Now you have a tenant secret that the Salesforce key management service can use to create the keys. Those keys encrypt and decrypt the clinic's data

### 3.6.6 KEY HYGIENE: MANAGEMENT BEST PRACTICES

Doc Mosey is fastidiously clean by trade and habit, and he encourages you to regularly update your org's tenant secret. Just like updating a password, frequently updating tenant secrets reduces the likelihood that malicious third parties can brute-force their way into your org.

The screenshot displays the Salesforce Key Management page. At the top, there's a header 'Key Management' with a 'Help for this Page' link. Below the header, there's introductory text about Platform Encryption and tenant secrets. A dropdown menu for 'Choose Tenant Secret Type' is set to 'Data in Salesforce'. Below this, there's a table of tenant secrets. The table has columns: Actions, Version, Tenant Secret Type, Status, Tenant Secret Source, Key Derivation, Created By, and Last Modified By. The 'Generate Tenant Secret' button is highlighted with a red box. The 'Status' column in the table is also highlighted with a red box.

**Key Management** [Help for this Page](#)

Platform Encryption helps you protect your data and meet compliance requirements.

You can manage tenant secrets and certificates for each encryption use-case. This includes Salesforce-generated tenant secrets and customer-supplied tenant secrets (Bring Your Own Key).

Use the dropdown menu to select which type of tenant secret you want to manage.

Read more about [Platform Encryption best practices](#) and [tradeoffs](#) before you get started.

Choose Tenant Secret Type **Data in Salesforce**

These keys encrypt data stored in the Salesforce database. This includes data in fields, files, and attachments.

---

**Key Management** [Key Management Help](#)

**Generate Tenant Secret** **Upload Tenant Secret** [i](#)

Actions	Version	Tenant Secret Type	Status	Tenant Secret Source	Key Derivation	Created By	Last Modified By
<b>Export</b>	3	Data in Salesforce	ACTIVE	HSM Generated	✓	Admin User, 1/22/2018 11:31 AM	Admin User, 1/22/2018 11:31 AM
<b>Destroy</b> <b>Export</b>	2	Data in Salesforce	ARCHIVED	HSM Generated	✓	Admin User, 1/22/2018 11:26 AM	Admin User, 1/22/2018 11:31 AM
<b>Import</b>	1	Data in Salesforce	DESTROYED	HSM Generated	✓	Admin User, 1/8/2018 4:38 PM	Admin User, 1/22/2018 11:31 AM

**Fig 3.6.6.1:** Key hygiene management best practice

## **CHAPTER 4: DISCUSSION**

Hiring is not an easy process. The cost/benefit analysis of establishing a paperless process needs to be evaluated in order to determine the approach to be taken for each process. A more efficient process may or may not reduce the number of staff. Personnel costs may shift from the business function to IT/support resources, either internal to the University or external to a vendor support the new paperless process. Technology costs may increase and need to be carefully evaluated to ensure hidden costs to supporting new components are included on an ongoing basis. Also, the ongoing technical training costs need to be considered. These overall costs may be offset by reduced resources needed to support the existing paper-based process.

Permission sets grant additional permissions to specific users, on top of their existing profile permissions, without having to modify existing profiles, create new profiles, or grant an administrator profile where it's not necessary.

The first step is creating an HR Recruiter profile and setting up the required data access according to Ling's specifications. It's best practice to not assign standard profiles to users. Instead, even if you're not making any changes, clone the Standard Profiles and assign the clones to users. That way, if a user needs permissions or access to a custom object in the future, the cloned profiles can be updated easily.

## CHAPTER 5: CONCLUSION

This paper presents different concepts about cloud computing and its platforms which is a recent technology in present world. It is a development trend in near future. This technology provides us with an infinite capability of computing, huge memory, fast microprocessor, high-speed network, reliable system architecture etc. The paper also describes about the leading Force.com platform for creating and deploying next generation cloud apps and its benefits. Also tells about how using this platform and cloud technology proves beneficial for developing the Recruiting Application. This application aims at reducing manual efforts and time of the company by making the recruitment and hiring procedure automated and also proves useful to the candidates searching for jobs. By creating a custom profile, creating permission sets, updating field-level security, and modifying organization-wide default sharing settings, you've made AW Computing's recruiting app a more secure tool. Ling Wu can rest easy knowing that her team—and anyone else accessing the app—will only see the data they're authorized to see. In order to access a record, users must have the appropriate object permission on their profile or a permission set. By changing sharing settings from the organization-wide defaults, you set the default level of access users have to records they do not own in each object.

Ling Wu would like job postings to be the only HR custom object with public access. Achieve this by changing the organization-wide default sharing settings, All standard objects have a predefined set of fields to capture common business information. While they can't be deleted, field-level security can make them invisible. Field-level security controls which fields a profile or permission set can view and edit, overrides any less-restrictive field access, and controls settings in page layouts and search layouts.



Field-level security is universally enforced regardless of how a user is accessing Salesforce—page layout, related lists, report, and so forth. For this reason, field-level security is the preferred way to secure sensitive and confidential information, like salary ranges HR recruiters and hiring managers work with in their app.

If you would like to get ahead of the curve, show this article to your IT and operations team to see what disruptive Salesforce technologies you can adopt to help your organization achieve maximum ROI.

Whatever the new Salesforce feature is that you choose to add on, be sure to invest in the analytics-driven and personalized digital adoption platform What fix to get users comfortable with the functionalities.

When Salesforce leaders started to think about operationalizing this, one challenge they knew they had to solve was capacity planning. Moving from a majority 80% in-office employee base, to an employee base coming in 1-3 days a week, with their team, for specific projects, means an added layer of complexity as it comes to figuring out precisely where teams will work in the office, and how to utilize space in such a way that makes the office feel alive.

“People are going to be purposeful in how they use the office moving forward, and our surveys tell us what we need the office to be for all our employees,” said Michele Schneider, SVP Global Workplace Services, Salesforce. “Thinking about the technology needed and the design needed for increased face-to-face meetings and collaboration, the office needs to support our teams and help our employees’ career development.”

Becoming a successful business is a difficult task, but sustaining yourself is much more challenging. In today’s world of immense cybersecurity risks it is really important for you to be pre-equipped with the security tools and privacy enhancements that are needed to safeguard your most valuable asset - your data.

The situation has changed once commercial AI vendors started to build connectors to open-source AI and ML platforms and provide affordable solutions that do not require complex configurations. What’s more, commercial vendors

offer the features open-source platforms currently lack, such as ML model management and reuse.

Meanwhile, experts believe that computers' ability to learn from data will improve considerably due to the application of unsupervised machine learning approach, deeper personalization, and cognitive services. As a result, there will be machines that are more intelligent and capable to read emotions, drive cars, explore the space, and treat patients.

The situation has changed once commercial AI vendors started to build connectors to open-source AI and ML platforms and provide affordable solutions that do not require complex configurations. What's more, commercial vendors offer the features open-source platforms currently lack, such as ML model management and reuse.

Meanwhile, experts believe that computers' ability to learn from data will improve considerably due to the application of unsupervised machine learning approach, deeper personalization, and cognitive services. As a result, there will be machines that are more intelligent and capable to read emotions, drive cars, explore the space, and treat patients.

XDR technology provides a unified incident response and security platform to collect and correlate data from several proprietary components. Importantly, these solutions offer platform-level integration out of the box. This means they do not require organizations to purchase and integrate multiple tools.

Organizations that run their workloads on public clouds face many security risks, such as misconfiguration, insecure APIs, insider threats, and unauthorized access. In response to these threats, XDR addresses the following challenges:

Securing identity management—XDR tools monitor end-users and service roles, and collect data from several cloud environments. XDR solutions can identify anomalous behaviour on privileged accounts and prompt security teams with alerts.

Analysing cloud logs—cloud workloads generate massive volumes of logs, which can be challenging to analyse manually. XDR tools can process cloud logs and apply artificial intelligence (AI) algorithms to identify risks.

Analysing network flows—public cloud networks are complex and often difficult to monitor for threats. XDR tools analyse network traffic across the entire cloud ecosystem. XDR tools use intelligent analysis to identify network security incidents, and even respond automatically, using network segmentation to isolate an infected system.

### **Secure Access Service Edge (SASE)**

Secure Access Services Edge (SASE) technologies help organizations secure access to cloud services, private applications, and websites. They can also reduce the complexity of endpoint protection. This makes SASE particularly helpful for securing virtual workforces, digital customer experience, and digital-first businesses.

Notable SASE features include access controls for endpoints, advanced threat protection, security monitoring, and data security. In addition, SASE offers centralized controls for acceptable use, which are enforced by API-based integration.

SASE is often delivered as a cloud service, but some vendors provide on-premises and agent-based components. According to Gartner, SASE solutions should also provide zero-trust and least-privileged access based on context and identity.

### **How will it change cloud security?**

SASE recognizes that in cloud environments, remote access is a first-class citizen. It goes beyond aging technologies like VPN, providing secure access for remote users with granular permissions and advanced anomaly detection.

Cloud security is gaining centre stage, and attackers are growing more sophisticated. Luckily, the security industry is rising to the challenge with new security tools and platforms:

- **XDR**—providing unified threat detection and response across cloud, on-premise networks, and endpoints.

- **SSE**—comprehensively securing access for remote users.
- **SSPM**—locking down SaaS applications.
- **ZTNA**—centralized access control built for dynamic cloud environments.
- **WAAP**—securing web applications and APIs, the user-facing interfaces of cloud systems.

### **Awareness:**

Understanding and being aware of what the company assets are as well as what their weak points could be can help predict possible cyberattacks.

### **Response System:**

Companies should be equipped with the proper tools that provide an automated counter-attack and stop any incoming threats.

### **Updates and modifications:**

any security framework should constantly be updated and modified to keep up with the digital era trends.

### **Fast big-data platforms:**

Equipped Big Data platforms produce results in real-time, able to detect real-time risks.

As technology develops, it pushes corporations to improve consumer experiences, causing companies to rush into digital transformation, leaving them increasingly more vulnerable to data security threats. Especially post-pandemic, It is highly important for organizations to make security a founding stone of digital transformation, and not an afterthought, as digital transformations will keep developing with the times and becoming more complex. This is why security approaches are so fundamental to make sure data protection cannot be breached.

However, the journey of a thousand steps starts with one: understanding the importance of your data and why it is valuable and prone to attacks. In case you still haven't found the answer, Intalio offers you a set of products and solutions such as Records Management, Digital Signature, Data Insights or others which may add another security consideration to your information.

## CHAPTER 6: FUTURE ENHANCEMENT

- 1. Lightning strikes harder:** Salesforce announced that only the more user-friendly and intuitive Salesforce 2.0 (dubbed 'Lightning') will receive useful upgrades. This means that users of the older 'Classic' version will miss out on several cool, productivity-enhancing features. Already, several exciting new features are ONLY available on Lightning – including customizable dashboard, calendar enhancements, Einstein, Snap-in chat, and Smart Macros. So now, a stage has been reached wherein organizations will have to urgently migrate from Classic to Lightning or risk being left behind in the race for efficiency and effectiveness.
- 1. Big year for system and data integration:** Customers have begun to expect seamless and connected experiences, based on the information they share at various touchpoints (social media, physical forms, phone support, etc). But according to the latest Salesforce Connected Customer report, only 50% of companies are able to customize their engagement based on past interactions.
- 2. AI and data-driven intelligence is king:** The AI-powered Sales Cloud Einstein was launched in 2017 to deliver data-driven predictions, insights, and recommendations that help make better lead/sales decisions. It does this, while continually learning from your CRM data about team performance, whitespace, and pipeline trends. Think of the saving, in terms of time, manpower, and opportunity costs, that Einstein brings to the table by automating data analytics.
- 3. Focus on customer satisfaction:** Data and system integration, data analysis, and AI are all striking trends. But undeniably, all of it leads to improving customer satisfaction and experience. And this is currently banging at the centre of the 'Goliath' CRM's strategy.
- 4. More industry-specific CRM solutions:** Salesforce platform has been widely used in industries such as financial software development services, manufacturing, media, and retail industry. And the cloud-based software company has clearly stated that it will focus its energies on certain industry verticals, in order to deliver more targeted solutions that meet their specific challenges. The CRM behemoth seeks to build on its CRM and cloud expertise with a layer of industry-based depth.

- 5. Enhanced Sales Insights:** Google joined hands with Salesforce last year and it was one of the most profound cloud computing alliances yet. This partnership will open the doorway for Salesforce to use Google's cloud infrastructure for fruitful expansion of its core services. The integration of Google Analytics 360 will be the highlight of this year and this platform will help the customers to connect their CRM insights with powerful data in analytics. It could be followed by Lightning for Gmail, Quip Live apps for Google Drive, etc. Salesforce will soon provide connectors to Google's data warehouse service, Google Big Query which will enable the users to combine their data with other available enterprise datasets.
- 6. Lightning Experience:** The creators believe that the platform's new UI edition with impeccable analysing and visual features as well as with competitive pricing will result in huge implementation and a tremendous increase in demand. There is also a lot of expectation that the existing clients will gradually make a shift to the Salesforce Lightning Experience from the Classic view. However, the new ones shall be adapting to it more willingly and quickly. This year will moreover witness Salesforce add new functionalities to the Lightning UI.
- 7. Identify Sensitive Data:** For companies, it is really important to be aware of where their most important data and sensitive business information lies. This will ensure you have the right information and allocate more resources to protecting your most sensitive and crucial assets. Although sensitive business data is only probably around 5-10% of your total business data, a data compromise involving sensitive or personal data could result in an immense loss of reputation and revenue to a company. If we go back to access management and rights, we should be putting more strict measures on sensitive data over other business data.
- 8. Pre-Planned Data Security Policy:** When looking at the operations and processes needed to mitigate a cyber-attack, an important step is to prepare a list of security measures and data security policies. This sort of plan by an organization could help significantly in critical situation and times of incident response. Through policies, you can immediately react in order to prevent extreme impacts of a cyber-attack. As with access management and rights, employee access could be identified easily and you would remain aware of which users in your organization could have potentially been breached. It's important to remember that a policy and process plan is

only as good as it's last revision. Technology, industry regulation and best practice is always changing. Someone therefore needs to own this policy and process guide and always look at new ways of updating it to keep it relevant.

- 9. Strong and Different Passwords for Every Department:** Sensitive data in an organization should be locked away with strong passwords. Making stronger passwords is necessary for fighting a number of password hacking tools that are easy to get on the market. Try ensuring that there are a combination of different characters including alphabets, numbers, symbols and other capital letters. Additionally, using the same passwords for different programs and access is also a risk. Once your password is cracked, a hacker will try the same password on all major accounts you own.

Therefore, organizations should keep unique passwords for all employees as well as the departments. This can be easily managed using a password manager tool and ensuring that all employees receive proper data security training and password tips.

Where possible, it is also advised that multi-factor authentication is used. Adding another step to a password login means another step that hackers need to crack, making the hack much more unlikely and difficult. Some good examples of multi-factor authentication include biometrics, push notifications to phones, smartcards and token authentication.

- 10. Regular Data Backup and Update:** Last on the list of important data security measures is having regular security checks and data backups. For an unexpected attack or data breach, it is really helpful to have an organization back up their data. To have a successful business, you must keep a habit of automatic or manual data backup on a weekly or daily basis. In addition, the data should be protected through updated software and efficient antivirus tools. However, to attain this, you must have progressive and efficient IT department. Make sure you are hiring someone with the right skills who you can trust to do the job properly.

- 11. Zero Trust Frameworks for Remote Employees:** In a matter of days and with no notice, offices around the world were forced to transition to totally remote workforces. In this newly distanced world, it quickly became clear that traditional, network-based security controls were not going to cut it. Enter zero trust security. A zero-trust framework is predicated on the idea that organizations should never automatically trust anything inside or out of its perimeters without verification. Instead, zero trust security gates individual access using granular policies, utilizing dynamic user and device risk signals and other telemetry to prevent data breaches and support a remote workforce. The zero-trust security market is expected to grow 10% annually from 2020 to 2025.
- 12. Vishing Scams and Attacks:** Voice phishing, otherwise known as vishing, has gained momentum this year, with the FBI and Cybersecurity and Infrastructure Security Agency releasing an official alert in August of 2020. Much like a traditional phishing attack, vishing attacks lure unsuspecting victims into providing log-in credentials, payment information or other sensitive data over the phone. Hackers scam individuals by pretending to be a bank or credit card representative, an employee from the IRS or an official from Medicare or Social Security offices. For organizations, the threat lies in spear-vishing attacks, which target key employees in an attempt to gain log-in credentials. A sophisticated vishing attack could even use deepfake audio to mimic the voice of a trustworthy party. Such was the case in 2019 when a chief executive at a UK energy company was tricked by a convincing deepfake audio call asking him to send \$220,000 USD to a Hungarian supplier.
- 13. Peer-to-Peer Botnets:** Botnet attacks are not a new enemy in the data security landscape, but this year, a botnet dubbed Frit Frog donned a powerful new weapon: a peer-to-peer network. Ordinarily, botnet networks operate with a central command and control centre that sends commands and receives stolen data. With its administration centralized, it is much easier for security experts to trace the illegal activity to its origins. However, peer-to-peer botnets like Frit Frog are avoiding detection by spreading administration over several infected nodes. Without a centralized server, peer-to-peer botnets are more difficult to detect and defuse. Since its discovery in January, Frit Frog has targeted tens of millions of IP addresses, from government agencies and financial



institutions to telecom companies and well-known universities—and it has yet to be taken down.

**14. Micros Harding:** While hackers flex the power of distribution with peer-to-peer botnets, security experts are using the same concept to improve their data protection and performance with micros Harding. Micros Harding takes the familiar data security practice of sharing to the next level. Micros Harding splits a file into multiple, very small pieces that may be as small as a single byte. Micro shards are then stored in separate locales, distributed across different cloud providers and on-premise locations. By reducing the attack surface, micosharding more effectively protects the data of customers, employees and organizations. It may also reduce scope, devaluing data in the same way that a paper shredder renders sensitive documents useless.

**15. Contactless Payments and Payment Protection:** At long last, the U.S. is catching up to the rest of the globe when it comes to contactless payments. Spurred by the coronavirus, contactless payments jumped 40% in the first quarter of 2020, and this new consumer behaviour is expected to stick around. But with new payment trends come new security vulnerabilities. As contactless payments become more common this year and beyond, it's crucial that merchants keep encryption in mind. In an interview with Digital Transactions, Miles Ruston, founder and adviser of Bluefin Payment Systems, warned that not all POS devices that accept contactless payments encrypt data as it enters the terminal. That's why it is critical for merchants to employ point-to-point encryption, or P2PE. With a P2PE-certified solution, clear-text data never traverses the merchant's system, ensuring that contactless payments are secure from the first tap.

**16. Devalue Your Sensitive Data:** As hackers develop new technologies to pilfer payment information, log-in credentials and more, it's critical that merchants devalue their data. At Bluefin, we help organizations protect their POS and online transactions with certified P2PE and tokenization solutions that render stolen data useless to cyberthieves. To find out more about our industry-leading cybersecurity solutions, contact Bluefin today.

### **Database:**

A Vulnerability and risk database that includes the vulnerabilities that the corporation needs to take into consideration.

**Product Solutions:**

The use of security solutions that are either standalone product solutions, features, or available resources that employees at every level can use.

**Decentralization:**

The process of decentralized information and transactions protects information in case one information site has been breached, securing the rest of the data while security is being heightened to fix the original breach.

**Solution Automation:**

Finally, the automation of cybersecurity solutions which get implemented into AI systems in order to detect threat patterns and automatically counter-attack any breaches.

## CHAPTER 7: BIBLIOGRAPHY

- Brooks, C., 2014. Beyond the Bottom Line: How Data Loss Affects Employees. [online] Business News Daily. Available at: <<http://www.businessnewsdaily.com/6407-employees-suffer-data-loss.html>> [Accessed 1 December 2015].
- Smith, D., 2015. The Cost of Lost Data - Graziadio Business Review | Graziadio Business Review | Graziadio School of Business and Management | Pepperdine University. [online] Gbr.pepperdine.edu. Available at: <<https://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/>> [Accessed 1 December 2015].
- Wright, A., 2015. Data Loss: The true cost for your business. [online] Thepulseofit.com. Available at: <<http://www.thepulseofit.com/article/data-loss-the-big-cost-for-small-businesses>> [Accessed 1 December 2015].
- Stedman, J. ed. [ebook] Available at: <[http://www.ey.com/Publication/vwLUAssets/Protecting\\_your\\_data/\\$FILE/EY\\_Protecting\\_your%20data\\_Our\\_%20approach\\_to\\_data\\_privacy\\_and\\_information\\_security.pdf](http://www.ey.com/Publication/vwLUAssets/Protecting_your_data/$FILE/EY_Protecting_your%20data_Our_%20approach_to_data_privacy_and_information_security.pdf)> [Accessed 1 December 2015].

# CERTIFICATE:



In Partnership With



## CERTIFICATE OF COMPLETION

July 08, 2022

**TANINKI PRASANNASAI**

### Salesforce Developer Virtual Internship

During the 8 Weeks period of Virtual Internship (**April-June 2022**), TANINKI PRASANNASAI has completed the following Salesforce Trailhead modules

Salesforce Fundamentals  
Organizational Setup  
Relationship & Process Automation  
Types Of Flows & Security  
Apex, Testing & Debugging  
VS Code Setup & CLI Setup  
Lightning Web Components (LWC) & API

Super Badge - Apex Specialist  
Super Badge - Process Automation Specialist

Certificate ID: SISFVIPAD2022-9331 | Verify this certificate @  
[https://smartinternz.com/internships/salesforce\\_certificates/bd9d03102a312711b0a71ecb44581d9d](https://smartinternz.com/internships/salesforce_certificates/bd9d03102a312711b0a71ecb44581d9d)

**Shri Buddha Chandraseker**

Chief Coordinating Officer(CCO),  
NEAT Cell-AICTE

**Mr Amarender Katkam**

Founder & CEO, TheSmartBridge &  
SmartInternz