sasi INSTITUTE OF TECHNOLOGY & ENGINEERING
autonomous

...Values We Live...

Accredited by 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.

Department of Information Technology

A

SEMINAR REPORT ON

KEEP DATA SECURE IN A RECRUITING APP

PRESENTED

BY

GANDHAM HARSHITHA

(19K61A1215)

SUBMITTED TO:

Dr. A.V.N. CHANDRA SEKHAR

PROFESSOR

DEPARTMENT OF INFORMATION TECHNOLOGY

DECLARATION:

I hereby declare that the report embodied in this dissertation entitled “Keep Data secure in a recruiting app” is carried out by me during the year 2022-2023 for a seminar is to gain knowledge on the curriculum courses.

BY:

G. HARSHITHA

19K61A1215

SASI AUTONOMOUS INSTITUTE OF TECHNOLOGY & ENGINEERING TADEPALLIGUDEM WEST GODAVARI DIST

KEEP DATA SECURE IN A RECRUITING APP

PRESENTED BY:

G Harshitha (19K61A1215)

LECTURER IN CHARGE:

Dr.A.V.N.CHANDRA SEKHAR

PROFESSOR

SITE

Contents

1. Abstract
2. Introducion
3. Literature Survey
4. Methodology
5. Sharing Settings
6. Result
7. Conclusion

Abstract

Updates 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,also restricts the data access in app by changing sharing settings.

Introduction

- We can continue customizing Computing's Recruiting app, which the HR team uses as they work to place applicants into open positions in the company,lets consider a example a companys
- Existing system uses notification via twitter app and through mail, our system sends notification via telegram.
- Due to popularity and flexibility of using current social network for all type of generation, we are proposing home security system using Telegram notification.

Literature Survey

- In 2021 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access ControlAlgorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud serviceproviders to avoid security related issues in cloud computing. The results of this paper showed data confidentiality, integrity and availability which is the three most important aspect of datasecurity was achieved.

- In 2021, Dimitra A. Geogiou wrote a paper to present security policies for cloud computing. The purpose of the security policies is to protect people and information, set rules for expected behavior by users, minimize risks and help to track compliance with regulation.This paper scrutinized the security requirements of a cloud service provider taking into consideration Case study of E-health system of Europe.

Literature Survey...

- In 2021 Sarojini et.al proposed a technique known as Enhanced Mutual Trusted Access Control Algorithm (EMTACA). This technique presents a mutual trust for both cloud users and cloud service providers to avoid security related issues in cloud computing. The results of this paper showed data confidentiality, integrity and availability which is the three most important aspect of data-security was achieved.

- In 2020 Afnan Ullah Khan proposed a technique known as Access Control and Data Confidentiality(ACDC) in his paper titled Data Confidentiality and Risk Management in Cloud Computing. The aim of the paper was to develop a novel scheme that would enforce access control policies on cloud computing scenarios. The paper focused on Infrastructure as a Service as its deployment model whereas data confidentiality and authentication were achieved through the proposed technique

Literature Survey...

- In 2019 Aastha Mishra proposed an Advanced Secret Sharing Key Management Scheme. The aim of this paper is to propose a more reliable decentralized light weight key management technique for cloud systems which provide more efficient data security and key management in cloud systems. In this paper, the technique used also brings to bear better security against byzantine failure,server colluding and data modification attacks.

- In 2019 Sudhansu Ranjan Lenka et.al wrote a paper titled “Enhancing Data Security in CloudComputing using RSA Encryption and MD5 Algorithm.In this paper, the RSA Algorithm is used for secured communication and file encryption and decryption purpose whilst MD5 Algorithm is used fordigital signature as well as covering the tables for unauthorized users.

Methodology

- **Create Profile:** Before creating the new profile, customize how profiles are viewed. From Setup enter User Management Settings in the Quick Find box, and select User Management Settings,Set Enhanced Profile User Interface to Disabled,Now create an HR Recruiter profile and set its object permissions,From Setup enter Profiles in the Quick Find box, and select Profiles. From the list of profiles, find Standard User. Click Clone.For Profile Name, enter HR Recruiter.Click Save.While still on the HR Recruiter profile page, then click Edit.Scroll down to Custom Object Permissions and change the Basic Access for each object to reflect the table below.

- 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.

Methodology...

- **Create a new permission set for hiring managers** Click Save. Click Assigned Apps in the Apps section, then click Edit. Select Recruiting from the Available Apps list and click Add.
- From Setup, enter Permission Sets in the Quick Find box, and select Permission Sets. 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.

Sharing Settings

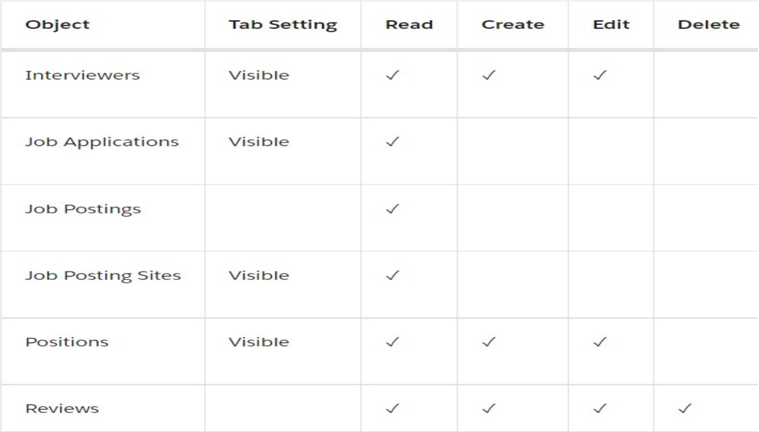
- Ling Wu would like job postings to be the only HR custom object with public access. Achieve this by changing the organization-wide default sharing settings.

- From Setup, enter Sharing Settings in the Quick Find box and select Sharing Settings. Click Edit in the Organization-Wide Defaults section. Select Private for the Candidate object. Select Private for the Interviewer object. Select Private for the Job Application object. Select Public Read Only for the Job Posting Site object. Select Private for the Position object. 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.

Result

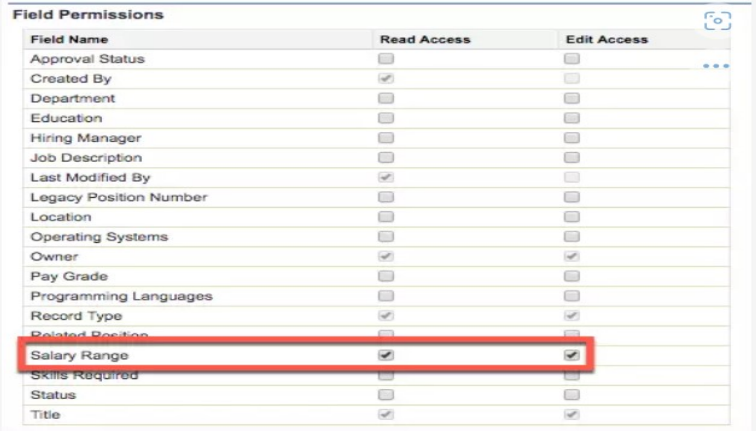
- **Modify Field-Level Security**



Object	Tab Setting	Read	Create	Edit	Delete
Interviewers	Visible	✓	✓	✓	
Job Applications	Visible	✓			
Job Postings		✓			
Job Posting Sites	Visible	✓			
Positions	Visible	✓	✓	✓	
Reviews		✓	✓	✓	✓

Result...

- Permission Sets

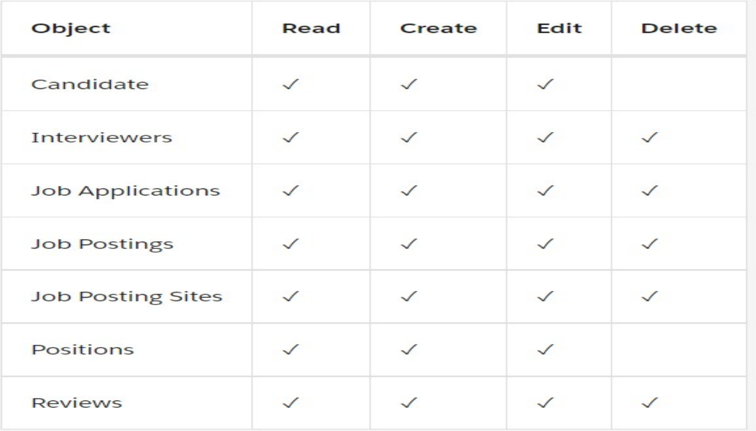


Field Permissions

Field Name	Read Access	Edit Access
Approval Status	□	□
Created By	☑	□
Department	□	□
Education	□	□
Hiring Manager	□	□
Job Description	□	□
Last Modified By	☑	□
Legacy Position Number	□	□
Location	□	□
Operating Systems	□	□
Owner	☑	☑
Pay Grade	□	□
Programming Languages	□	□
Record Type	☑	☑
Related Position	□	□
Salary Range	☑	☑
Skills Required	□	□
Status	□	□
Title	☑	☑

Result...

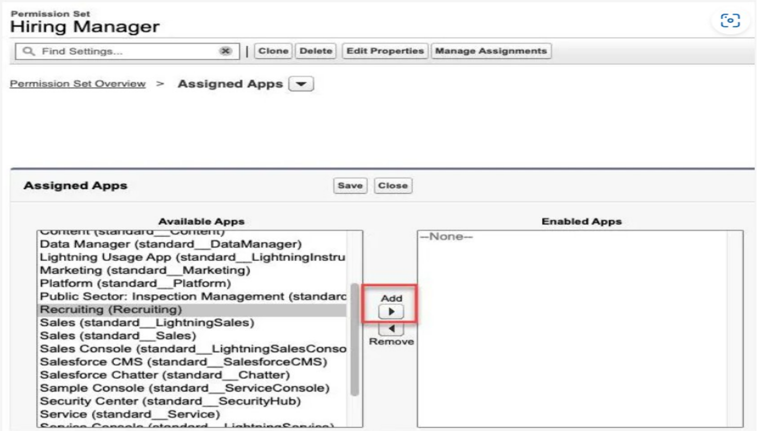
- **Profiles**



Object	Read	Create	Edit	Delete
Candidate	✓	✓	✓	
Interviewers	✓	✓	✓	✓
Job Applications	✓	✓	✓	✓
Job Postings	✓	✓	✓	✓
Job Posting Sites	✓	✓	✓	✓
Positions	✓	✓	✓	
Reviews	✓	✓	✓	✓

Result...

- Assigned Apps in Recruiting form



Hiring Manager

Assigned Apps

Available Apps

Content (standard__Content)
Data Manager (standard__DataManager)
Lightning Usage App (standard__LightningInstru
Marketing (standard__Marketing)
Platform (standard__Platform)
Public Sector: Inspection Management (standarc
Recruiting (Recruiting)
Sales (standard__LightningSales)
Sales (standard__Sales)
Sales Console (standard__LightningSalesConso
Salesforce CMS (standard__SalesforceCMS)
Salesforce Chatter (standard__Chatter)
Sample Console (standard__ServiceConsole)
Security Center (standard__SecurityHub)
Service (standard__Service)
Service Console (standard__LightningService)

Enabled Apps

--None--

Result...

- 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.

- Successfully implemented the organization-wide defaults for Recruiting app objects.

Conclusion

- In a global, digital world, the most important currency for any business is trust,trust is something you earn over many years by diligently safeguarding your customer's personal data. They trust you with a lot of essential information – their address, their payment details, their preferences, even their bio metric data.
- Data security isn't easy. Cyberthreats are constantly evolving, and employees struggle to keep up with ever-changing protocols. The new normal of remote work has added another layer of risk to an already challenging world.
- It starts with strategy, with people and with education. But the most important part is getting the infrastructure right. A good ETL vendor can help you build a secure data pipeline that keeps sensitive information out of the wrong hands. Your customers will rest easy knowing their personal data is safe.