



INSTITUTE OF
TECHNOLOGY &
ENGINEERING
TADEPALLIGUD^{cm}
WEST GHANAVARI NEST



KEEP DATA SECURE IN A RECRUITING APP

PRESENTED BY:

G Harshitha

(19K61A1215)

LECTURER IN CHARGE:

Dr.A.V.N.CHANDRA SEKHAR

PROFESSOR

SITE



- 1 Abstract
- 2 Introduction
- 3 Literature Survey
- 4 Methodology
- 5 Sharing Settings
- 6 Result
- 7 Conclusion



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.



- 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.



- 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 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.



- 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



- 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 Cloud Computing 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 for digital signature as well as covering the tables for unauthorized users.



- **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.



- **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.



- 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.




• 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		✓	✓	✓	✓



● Permission Sets

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"/>	



● Profiles

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

● Assigned Apps in Recruiting form

Permission Set
Hiring Manager

Find Settings... | Clone | Delete | Edit Properties | Manage Assignments

Permission Set Overview > Assigned Apps

Assigned Apps [Save] [Close]

Available Apps		Enabled Apps
Content (standard__Content)	<div>Add Remove</div>	—None—
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)		



- 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.



- 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.