

- 1 # To test the system's ability to handle a mix of different document formats, you can write a Python script that does the following:
- 2 # Create a directory for the test files and copy a mix of different document formats into that directory, including PDF, DOC, DOCX, TXT, and ODT files.
- 3 # Add test cases for each file format, including opening the file, verifying the file's contents, and checking if the file can be rendered properly.
- 4 # Add test cases for password-protected documents and verify that the system can handle them.
- 5 # Add test cases for large files and verify that the system can process them efficiently.
- 6 # Add test cases for different formatting styles, tables, and images, and verify that the system can handle them and maintain the formatting.
- 7 # Add test cases for document conversion, and verify that the system can convert between different file formats without data loss or formatting errors.
- 8 # Here is some sample Python code that you can use to get started with this test case:

```

import os
import Document Document
from pdfutils.high_level import extract_text
from odf import text, tabletext
from zipfile import ZipFile

class TestDocument(Formats(unittest.TestCase)):

    @classmethod
    def setUpClass(cls):
        os.test_files_dir = 'test_files'
        if not os.path.exists(test_files_dir):
            os.makedirs(test_files_dir)

    # Copy test files to the test directory
    #

    @classmethod
    def setUpDocClass(cls):
        # Remove the test directory
        os.remove(test_files_dir)

    def setUp(self):
        pdf_file = os.path.join(self.test_files_dir, 'test.pdf')
        self.assertFileExists(pdf_file)
        with open(pdf_file, 'w') as f:
            f.write('test')
        # Add tests for PDF content and rendering
        #

    def test_docx(self):
        docx_file = os.path.join(self.test_files_dir, 'test.docx')
        self.assertFileExists(docx_file)
        doc = Document(docx_file)
        # Add tests for DOCX content and rendering
        #

    def test_text(self):
        txt_file = os.path.join(self.test_files_dir, 'test.txt')
        self.assertFileExists(txt_file)
        with open(txt_file, 'w') as f:
            f.write('test')
        # Add tests for TXT content and rendering
        #

    def test_csv(self):
        csv_file = os.path.join(self.test_files_dir, 'test.csv')
        self.assertFileExists(csv_file)
        with ZipFile(csv_file) as zip_file:
            # Get the content of the CSV as content, file name
            content = zip_file.read('test.csv')
            csv_text = text.Text(content)
            plain_text = tabletext.TableText(csv_text)
        # Add tests for CSV content and rendering
        #

    def test_password_protected_docx(self):
        password_protected_docx_file = os.path.join(self.test_files_dir, 'test_password_protected.docx')
        self.assertFileExists(password_protected_docx_file)
        # Add tests for password-protected documents
        #

    def test_large_image(self):
        large_file = os.path.join(self.test_files_dir, 'test_large_file.pdf')
        self.assertFileExists(large_file)
        # Add tests for large files
        #

    def test_formatting_styles(self):
        formatting_styles_file = os.path.join(self.test_files_dir, 'test_formatting_styles.docx')
        doc = Document(formatting_styles_file)
        # Add tests for formatting styles, tables, and images
        #

    def test_document_conversion(self):
        docx_file = os.path.join(self.test_files_dir, 'test.docx')
        pdf_file = os.path.join(self.test_files_dir, 'test.pdf')
        self.assertFileExists(docx_file)
        self.assertFileExists(pdf_file)
        # Add tests for document conversion
        #

```

Testing the system with input that contains a mix of different document formats:

			<pre> # Python code for testing the system with input that contains a mix of different authorization formats # Import necessary libraries or modules # Define a function to test the different authorization formats def test_authorization_formats(authorization_formats): # Set up the system with the given authorization formats # ... # Try to access resources or perform actions that the user should not have permission to access # ... # Test if the system properly enforces the authorization rules and prevents unauthorized access # ... # Test edge cases if the user's role or group membership is changed # ... # Test if the system properly handles the change if the user is logged in # ... # Test if the system immediately applies the new authorization rules or waits for the user to log in again # ... # Return the test results return test_results # Test the system with different authorization formats test_results = test_authorization_formats("format_1", "format_2", "format_3", ...) # Print the test results print(test_results) </pre>			
Testing the system with input that contains a mix of different authorization formats:			<pre> # Python code for the provided test case # Import necessary libraries import random from cryptography.fernet import Fernet import socket # Create a list of different network protocols protocols = ["TCP", "UDP", "ICMP", "FTP", "SMTP", "POP3"] # Generate a random protocol using the protocols list protocol = random.choice(protocols) # Encrypt and decrypt data transmitted over the network key = Fernet.generate_key() cipher_suite = Fernet(key) # Generate a random message for testing purposes message = "This is a test message" # Encrypt the message cipher_text = cipher_suite.encrypt(message) # Decrypt the message plain_text = cipher_suite.decrypt(cipher_text) # Test if the decrypted message is the same as the original message if message == plain_text: print("Encryption and decryption of message successful") # Test if the system can properly route the data transmitted over the network s = socket.socket(socket.AF_INET, socket.SOCK_STREAM) s.connect(("www.google.com", 80)) s.sendall(b"GET / HTTP/1.1\r\nHost: www.google.com\r\n\r\n") data = s.recv(1024) s.close() # Print the received data print(data) </pre>			
Testing the system with input that contains a mix of different network protocols:			<pre> # Here is an example code in Python for the given test case: import os # List of different file system formats file_systems = ["NTFS", "FAT32", "exFAT"] # Loop through each file system format for file_system in file_systems: # Create a file with random data file_name = f"test_{file_system}.txt" with open(file_name, "w") as f: f.write("This is test data.") # Simulate corruption of the file system if file_system == "NTFS": # Corrupt the MFT entry for the test file os.system(f"fsutil repair set c:\\{file_name} corrupted") elif file_system == "FAT32": # Corrupt the FAT table entry for the test file os.system(f"fsutil repair set c:\\{file_name}-1 corrupted") elif file_system == "exFAT": # Corrupt the superblock for the test file os.system(f"tune2fs -s c:\\{file_name}") # Try to read the test file try: with open(file_name, "r") as f: data = f.read() except Exception as e: print(f"Error reading test file: {str(e)}") # Try to write to the test file try: with open(file_name, "w") as f: f.write("More test data.") except Exception as e: print(f"Error writing to test file: {str(e)}") # Delete the test file try: os.remove(file_name) print(f"Successfully deleted test file {file_name}.") except Exception as e: print(f"Error deleting test file: {str(e)}") </pre>			
Testing the system with input that contains a mix of different file system formats:						

	<pre> Python code for Data Authorization Test Case #Import necessary libraries import os import random #Define test data containing mix of different authorization techniques test_data = { 'user_1': { 'name': 'John', 'role': 'admin', 'permissions': ['edit_users', 'delete_users', 'create_user'] }, 'user_2': { 'name': 'Peter', 'role': 'manager', 'permissions': ['edit_users', 'create_user'] }, 'user_3': { 'name': 'Mary', 'role': 'user', 'permissions': ['create_user'] }, 'user_4': { 'name': 'Sarah', 'role': 'guest', 'permissions': [] } } #Define RBAC and ABAC methods def rbac_authorization(user, permission): if user['role'] == 'admin': return True elif user['role'] == 'manager': if permission == 'create_user': return False else: return True elif user['role'] == 'user': if permission == 'edit_users' or permission == 'delete_users': return False else: return True else: return False def abac_authorization(user, permission): if permission in user['permissions']: return True else: return False #Test RBAC authorization def test_rbac_authorization(): for user in test_data: for permission in test_data[user]['permissions']: assert rbac_authorization(test_data[user], permission) == True #Test ABAC authorization def test_abac_authorization(): for user in test_data: for permission in test_data[user]['permissions']: assert abac_authorization(test_data[user], permission) == True #Test system for unauthorized access or privilege escalation attacks def test_system_security(): #Attempt to access unauthorized permission for user in test_data: for permission in ['edit_users', 'delete_users']: assert rbac_authorization(test_data[user], permission) == False assert abac_authorization(test_data[user], permission) == False #Attempt to escalate privileges for user in test_data: random_permission = random.choice(test_data[user]['permissions']) assert rbac_authorization(test_data[user], random_permission) == True assert abac_authorization(test_data[user], random_permission) == True #Run tests test_rbac_authorization() test_abac_authorization() test_system_security() #Print test results print('All tests passed! System is secure and can handle different data authorization techniques.') Possible code in Python for the test case is: import socket # Set up a TCP server and client tcp_server = socket.socket(socket.AF_INET, socket.SOCK_STREAM) tcp_server.bind(('localhost', 0)) tcp_server.listen(1) tcp_client = socket.socket(socket.AF_INET, socket.SOCK_STREAM) tcp_client.connect(('localhost', tcp_server.getsockname()[1])) # Send and receive some data using TCP tcp_client.send('Test data over TCP') tcp_server_connection, tcp_server_address = tcp_server.accept() tcp_received_data = tcp_server_connection.recv(1024) # Close the TCP connection tcp_server_connection.close() tcp_client.close() tcp_server.close() # Set up a UDP server and client udp_server = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) udp_server.bind(('localhost', 0)) udp_client = socket.socket(socket.AF_INET, socket.SOCK_DGRAM) udp_client.sendto('Test data over UDP', ('localhost', udp_server.getsockname()[1])) # Receive some data using UDP udp_received_data, udp_received_address = udp_server.recvfrom(1024) # Close the UDP connection udp_client.close() udp_server.close() # Set up an HTTP server and client http_server = socket.socket(socket.AF_INET, socket.SOCK_STREAM) http_server.bind(('localhost', 0)) http_server.listen(1) http_client = socket.socket(socket.AF_INET, socket.SOCK_STREAM) http_client.connect(('localhost', http_server.getsockname()[1])) # Send an HTTP request and receive an HTTP response http_client.send('GET / HTTP/1.1\r\nHost: localhost\r\n\r\n') http_server_connection, http_server_address = http_server.accept() http_received_data = http_server_connection.recv(1024) # Close the HTTP connection http_server_connection.close() http_client.close() http_server.close() # Print the received data from all protocols print('Received data over TCP:', tcp_received_data) print('Received data over UDP:', udp_received_data) print('Received data over HTTP:', http_received_data) </pre>	
Testing the system with input that contains a mix of different data authorization techniques:		
Testing the system with input that contains a mix of different data network protocols:		

