Introduction to Robotic Process Automation

PASSWORD CHANGE REMAINDER BOT

Reg no:220701009
Name: Abisheak C
Guide name: Mrs. J. Jinu Sophia
Computer Science and Engineering

RAJALAKSHMI
ENGINEERING COLLEGE

Abstract

- The Password Change Reminder Bot is an automated solution developed using UiPath to streamline the process of managing password updates across organizational systems. This bot proactively reminds users to change their passwords before they expire, ensuring compliance with security policies and reducing the risk of account lockouts. Leveraging UiPath's robust automation capabilities, the bot integrates with email systems, directories, and other enterprise tools to fetch password expiration dates, generate timely notifications, and guide users through the password change process. By minimizing manual intervention and enhancing user convenience, the bot significantly improves security posture while reducing administrative overhead.

Need for the Proposed System

- The need for The Password Change Reminder Bot arises from the critical importance of maintaining robust cybersecurity measures in organizations. Frequent password updates are essential to protect sensitive information from unauthorized access; however, users often overlook or forget to change their passwords on time, leading to account lockouts, operational disruptions, and potential security vulnerabilities. The manual process of monitoring password expiry and sending reminders is time-consuming and prone to errors, placing additional strain on IT support teams. The proposed system addresses these challenges by automating password expiration tracking and notifications, ensuring timely updates while reducing administrative efforts and enhancing overall system security and user productivity.

Advantages of the Proposed System

- **Improved Security:** Ensures timely password changes, reducing the risk of breaches and unauthorized access.
- **Minimized Downtime:** Prevents account lockouts, ensuring uninterrupted access to critical systems and workflows.
- **Operational Efficiency:** Automates the process of tracking password expiry and sending reminders, reducing the workload on IT teams.
- **User Convenience:** Provides proactive and timely notifications, allowing users to update passwords without last-minute stress.
- **Cost Savings:** Reduces the need for manual interventions and IT support for account recovery, cutting operational costs.
- **Compliance Assurance:** Helps organizations adhere to password management policies and regulatory requirements.

Literature Survey

- Paper 1: "Automating IT Operations with Robotic Process Automation: A Case Study"
- Summary: This paper explores how Robotic Process Automation (RPA), particularly UiPath, is used to automate IT tasks like password expiry notifications. The case study demonstrates the efficiency improvements and error reduction achieved through automation in managing password reminders.
- Advantages:
- Improved Efficiency: Reduces manual effort, allowing IT teams to focus on more complex tasks.
- Error Reduction: Minimizes mistakes in password expiry tracking and reminder notifications.
- Disadvantages:
- Complex Setup: Initial configuration of RPA bots requires time and technical expertise.
- Maintenance Costs: Ongoing maintenance and updates to RPA bots can incur additional costs.

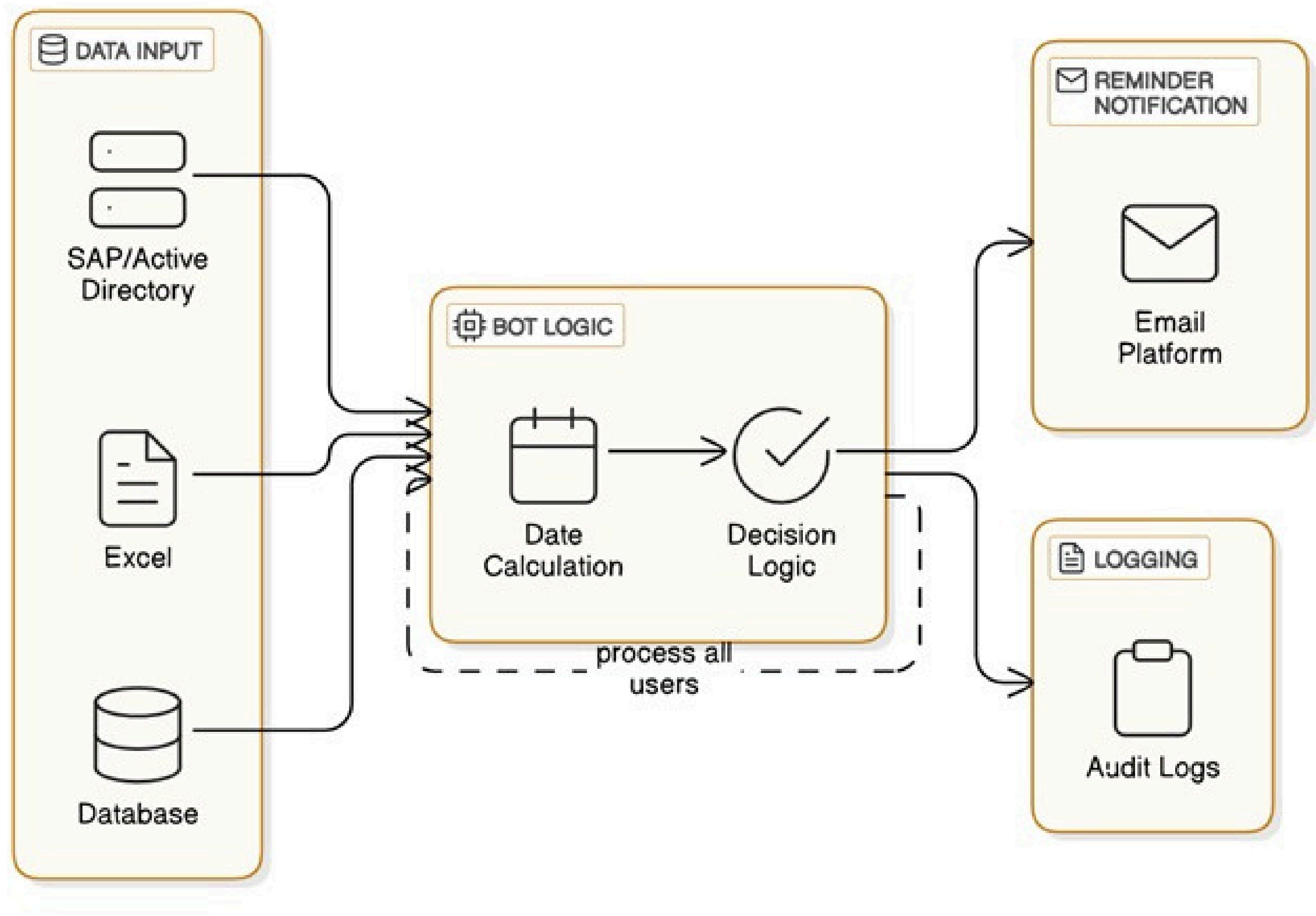
Literature Survey

- Paper 2: "The Role of User Behavior in Password Management Systems"
- Summary: This paper discusses user behavior challenges in password management, emphasizing the importance of automated reminders to encourage timely password changes and improve compliance with security policies.
- Advantages:
- Increased Compliance: Automated reminders enhance user adherence to password policies.
- User Awareness: Regular reminders can improve user understanding of security best practices.
- Disadvantages:
- User Frustration: Excessive reminders may annoy users, reducing their effectiveness.
- Limited Engagement: Users may ignore reminders, necessitating further follow-ups or escalations

Main Objective

- The main objective of the Password Change Reminder Bot is to automate the process of tracking password expiration and notifying users to ensure timely password updates, thereby enhancing system security and operational efficiency. By integrating with organizational systems, the bot eliminates manual monitoring and reduces the risk of account lockouts, ensuring uninterrupted user access to critical resources. Additionally, the bot aims to ease the administrative burden on IT support teams, improve user compliance with security policies, and support organizational efforts to safeguard sensitive data from potential threats.

Architecture



System Requirements

Hardware Requirements

- **Processor:** Intel i3 or above (or equivalent)
- **RAM:** Minimum 4 GB (8 GB or higher recommended)
- **Storage**: At least 10 GB of free disk space
- **Operating System**: Windows 10 or above
- **Network**: Stable internet connection for bot execution and notifications

System Requirements

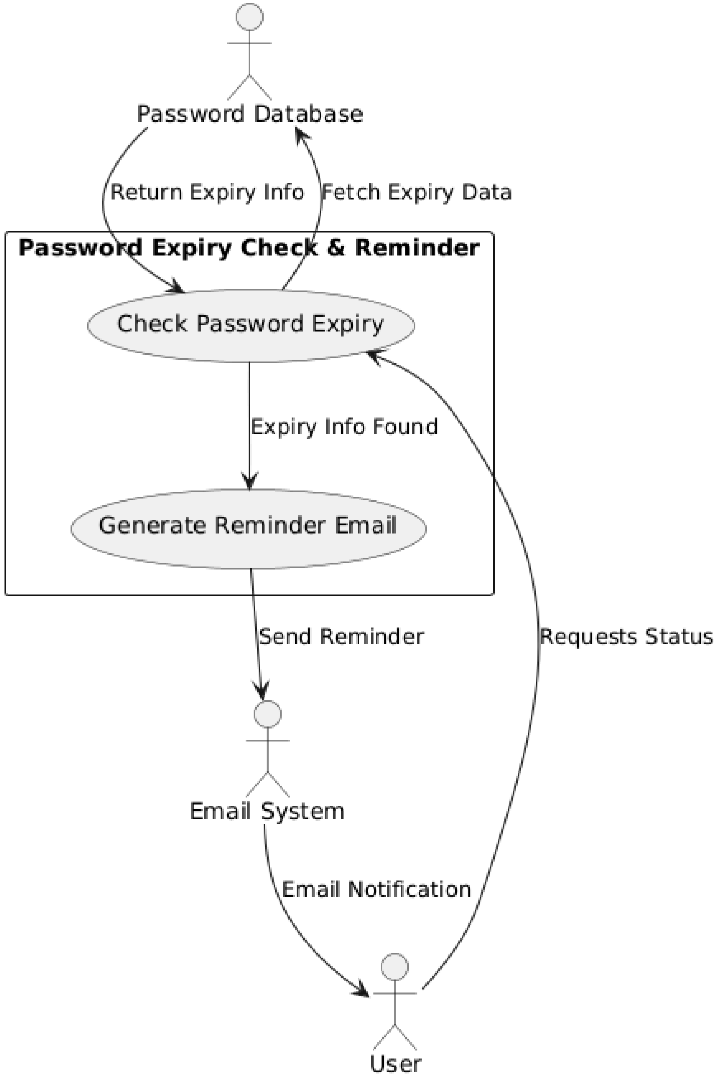
Software Requirements

- **UiPath Studio:** Latest stable version
- **Email Client:** Supported email system (e.g., Outlook or Gmail) for sending notifications
- **Browser:** Google Chrome or Microsoft Edge for web-based access
- **Required Packages in UiPath:**
- UiPath.Mail.Activities
- UiPath.System.Activities
- UiPath.Database.Activities (if database integration is needed)
- UiPath.WebAPI.Activities (if APIs are used for password expiration tracking)

Functional Description

- Module 1: Password Expiry Check and Reminder

This module is responsible for checking the password expiry status of users and sending them reminder notifications. It fetches data from the user database, checks if any passwords are nearing expiration, and triggers an email reminder to the user.



Functional Description

Module 2: User Response Tracking and Escalation

This module tracks user responses to password reminders and escalates the issue if the user fails to change the password within a specified period. It ensures that if the user does not act on the reminder, the issue is forwarded to the IT admin for manual intervention.

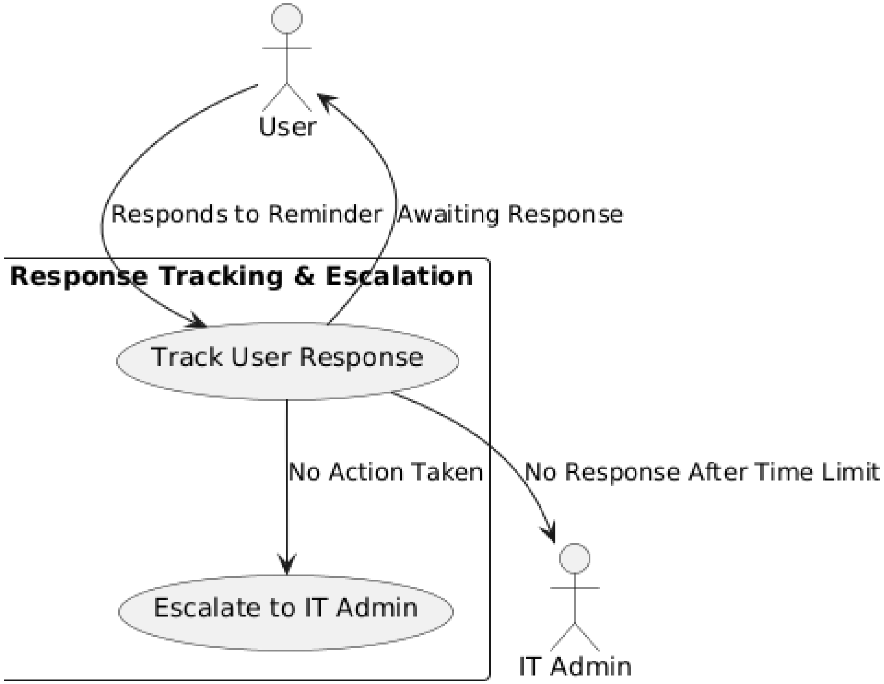
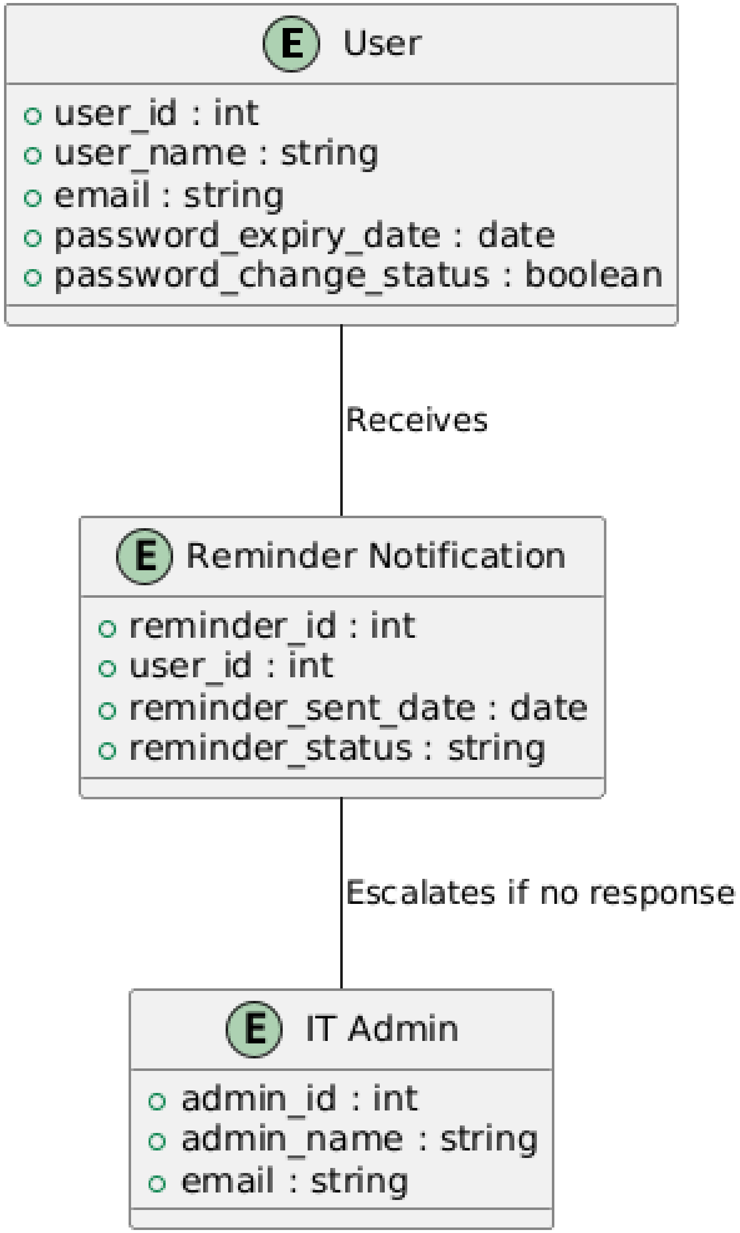


Table Design



E User

o user_id : int
o user_name : string
o email : string
o password_expiry_date : date
o password_change_status : boolean

Receives

E Reminder Notification

o reminder_id : int
o user_id : int
o reminder_sent_date : date
o reminder_status : string

Escalates if no response

E IT Admin

o admin_id : int
o admin_name : string
o email : string

Process Design

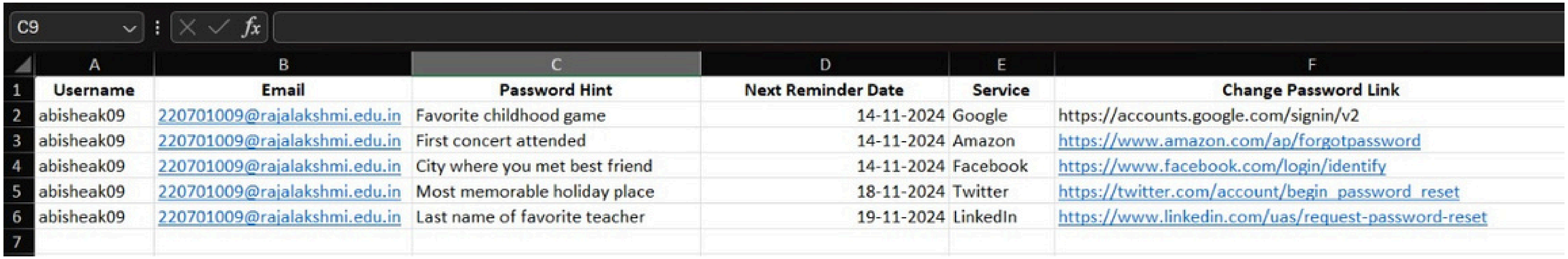
- **Main Process: Password Expiry Check and Reminder**
- The main process involves checking password expiry, notifying users, and tracking their responses to ensure timely password changes.
- **Steps in the Main Process:**
- **Fetch User Data:**
- Retrieve data related to user accounts and their password expiry from the database or Active Directory.
- **Check Password Expiry:**
- Determine whether the user’s password is nearing expiration by comparing the current date with the expiration date stored in the database.
- **Send Reminder Notification:**
- If the password is near expiry, trigger the system to send an email reminder to the user.
- **Monitor User Response:**
- Track whether the user has updated their password or ignored the reminder.

Process Design

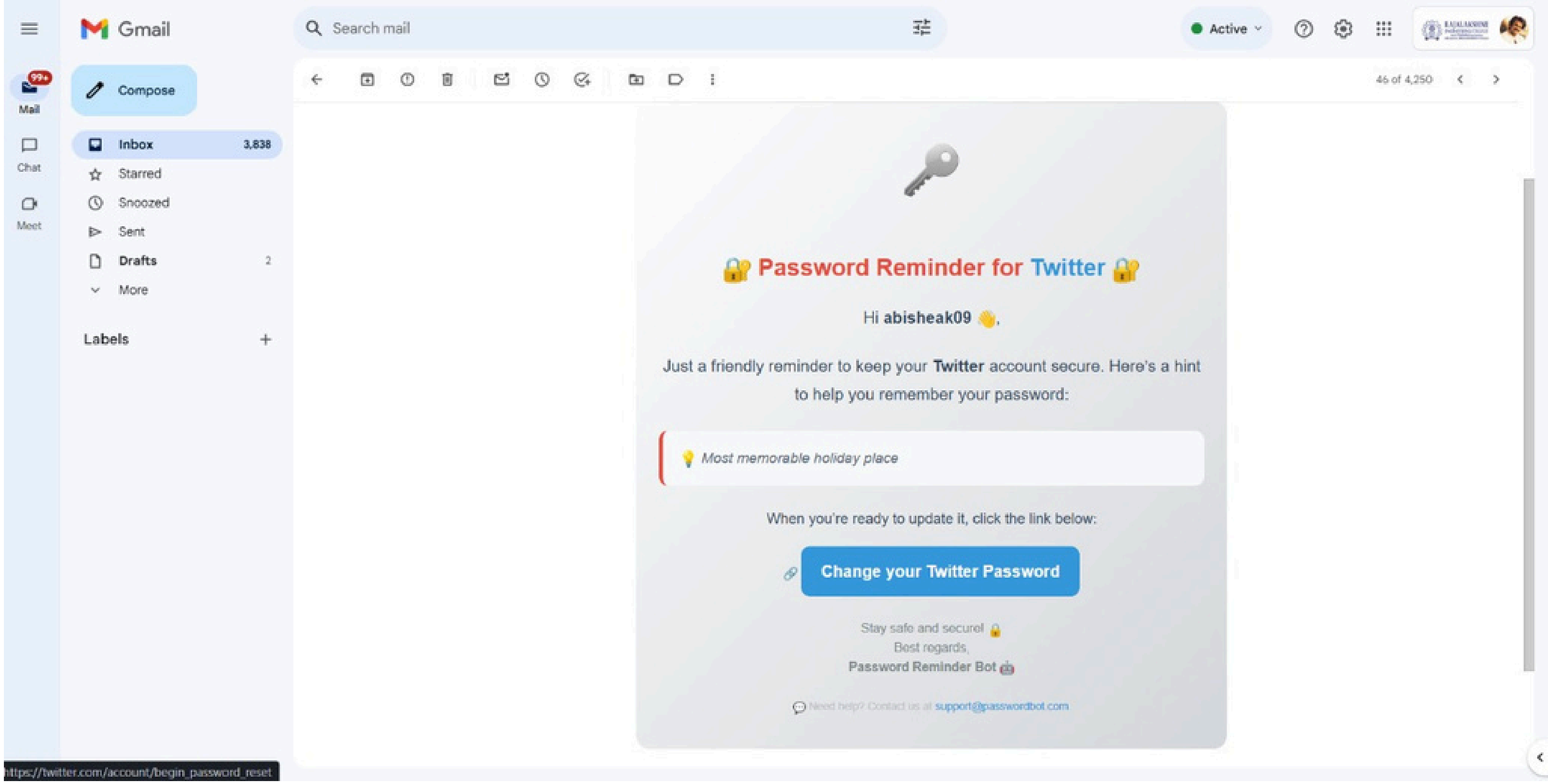
Sub Processes

1. Fetch User Data
   - Input: User details from the database (username, password expiry date).
   - Action: The system queries the database to retrieve user information.
   - Output: A list of users and their respective password expiry dates.
2. Check Password Expiry
   - Input: User data, current date.
   - Action: The system compares the password expiry date with the current date to identify users with passwords nearing expiration.
   - Output: A list of users with passwords expiring soon.
3. Generate and Send Reminder Notification
   - Input: List of users with expiring passwords, email templates.
   - Action: The system formats and sends an email reminder to the users about their password expiration.
   - Output: Reminder emails are sent to the users.
4. Track User Response
   - Input: User activity (whether the user updates their password or not).
   - Action: The system monitors if users take action to change their passwords after receiving the reminder.
   - Output: Updated status of users (password changed or reminder still pending).

Implementation



	A	B	C	D	E	F
1	Username	Email	Password Hint	Next Reminder Date	Service	Change Password Link
2	abisheak09	220701009@rajalakshmi.edu.in	Favorite childhood game	14-11-2024	Google	https://accounts.google.com/signin/v2
3	abisheak09	220701009@rajalakshmi.edu.in	First concert attended	14-11-2024	Amazon	https://www.amazon.com/ap/forgotpassword
4	abisheak09	220701009@rajalakshmi.edu.in	City where you met best friend	14-11-2024	Facebook	https://www.facebook.com/login/identify
5	abisheak09	220701009@rajalakshmi.edu.in	Most memorable holiday place	18-11-2024	Twitter	https://twitter.com/account/begin_password_reset
6	abisheak09	220701009@rajalakshmi.edu.in	Last name of favorite teacher	19-11-2024	LinkedIn	https://www.linkedin.com/uas/request-password-reset
7						



🔐 Password Reminder for Twitter 🔐

Hi **abisheak09** 👋,

Just a friendly reminder to keep your **Twitter** account secure. Here's a hint to help you remember your password:

💡 *Most memorable holiday place*

When you're ready to update it, click the link below:

🔗 **Change your Twitter Password**

Stay safe and secure! 🔒
Best regards,
Password Reminder Bot 🤖

💬 Need help? Contact us at support@passwordbot.com

Testing

- **Unit Testing**
- Purpose: To test individual components of the system in isolation to ensure they work correctly.
- Test Cases:
  - Validate that the system correctly fetches user password data from the database.
  - Test the logic that checks if the password expiration date is valid and if it is within the threshold.
  - Ensure that email notifications are being generated and sent correctly.
  - Test the functionality of tracking user responses (whether the user updated their password).
- **Integration Testing**
- Purpose: To verify that different modules of the system work together as expected.
- Test Cases:
  - Check if the system correctly integrates with the database to fetch password expiry data.
  - Test the interaction between the password expiry checking system and the email notification system.
  - Ensure that the escalation process works seamlessly, sending notifications to the IT Admin if the user does not respond.
- **System Testing**
- Purpose: To verify that the entire system works together and fulfills the functional requirements.
- Test Cases:
  - Test the entire flow from password expiry detection to email notification and user response tracking.
  - Simulate scenarios where users receive reminders, update passwords, or fail to respond.
  - Test the escalation process to ensure it triggers correctly when users fail to act.
- **Acceptance Testing**
- Purpose: To ensure the system meets the business requirements and user expectations.
- Test Cases:
  - Verify that users receive reminders well before their passwords expire.
  - Ensure that IT Admins are notified in a timely manner when escalations are needed.
  - Confirm that the system meets the expected performance and functionality, with no delays in email delivery or user response tracking.

Conclusions

The Password Change Reminder Bot project automates the process of notifying users about upcoming password expirations, ensuring compliance with security policies while reducing manual workload for IT teams. By leveraging UiPath for Robotic Process Automation (RPA), the system efficiently checks password expiry dates, sends reminders to users, and tracks responses. If users fail to update their passwords, the system escalates the issue to IT Admins, maintaining security without extensive manual intervention. The system enhances operational efficiency, minimizes errors, and improves overall security by ensuring timely password changes. Thorough testing has validated the system's reliability, security, and scalability, making it a valuable tool for automating password management and reducing administrative overhead.

Future Enhancement

- Multi-factor Authentication (MFA) Reminders: A potential future enhancement for the Password Change Reminder Bot is the integration of multi-factor authentication (MFA) reminders. In addition to notifying users about password expirations, the system could also notify users when their MFA setup needs updating or verification, further enhancing account security by ensuring both password and MFA configurations are current.

- AI-based Analytics for Personalized Reminders: Another improvement could be incorporating AI-based analytics to monitor user behavior patterns and provide personalized reminders. The system could suggest password changes based on inactivity, detected vulnerabilities, or even compromised account detections. This enhancement would make the bot more dynamic and proactive in managing security risks, increasing both user compliance and overall protection.

IEEE Paper

- Paper Title: A Holistic Approach to Ensure Security and Compliance while using Robotic Process Automation
- Authors: Unknown (listed as IEEE team authors)
- Abstract: The paper discusses the integration of Robotic Process Automation (RPA) with security and compliance frameworks. It emphasizes how RPA tools can be applied to ensure sensitive processes like password management and reminders are automated securely while adhering to organizational policies.
- Published In: IEEE Access
- DOI: 10.1109/ACCESS.2020.2973895

- Paper Title: Benefits Realization of Robotic Process Automation (RPA) Initiatives in Supply Chains
- Authors: Reinaldo Morabito, João Batistella, Silvia Borin, and others
- Abstract: This paper explores the benefits of RPA implementation within the supply chain sector. It highlights key advantages like operational efficiency, reduction of errors, and automation of repetitive tasks—insights that can be applied to the automation of administrative processes such as password expiration reminders.
- Published In: IEEE Journals & Magazine
- DOI: 10.1109/ACCESS.2024.10098777

References

"Robotic Process Automation: A Survey and Future Directions"
Authors: S. Avasarala, R. S. Gorthi, and S. J. Arora.
Published in: International Journal of Computer Applications (2017).
This paper provides an in-depth analysis of RPA technology, its applications in various domains, and the challenges associated with automating routine tasks. It also discusses the integration of RPA with AI and other tools, which can improve the efficiency of systems like password management and reminders.
Link: ResearchGate

"Automation with Artificial Intelligence in Business Process Management"
Authors: N. Parveen and N. Singh.
Published in: International Journal of Advanced Research in Computer Science and Software Engineering (2016).
This paper explores the role of automation in business processes, particularly how RPA combined with AI can streamline administrative tasks like password updates and reminders. It highlights AI's potential to optimize workflow and security in business operations.
Link: IJARCSSE Journal

Thank You