PASSWORD CHANGE REMAINDER BOT

A PROJECT REPORT

Submitted by

ABISHEAK C(2116220701009)

in partial fulfillment for the course

OAI1903 - INTRODUCTION TO ROBOTIC PROCESS AUTOMATION

for the degree of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

RAJALAKSHMI ENGINEERING COLLEGE

RAJALAKSHMI NAGAR

THANDALAM

CHENNAI – 602 105

NOVEMBER 2024

RAJALAKSHMI ENGINEERING COLLEGE

CHENNAI - 602105

BONAFIDE CERTIFICATE

Certified that this project report **"The Password Change Remainder Bot"** is the bonafide work of **"ABISHEAK C (220701009)"** who carried out the project work for the subject OAI1903 - Introduction to Robotic Process Automation under my supervision.

Mrs. J. Jinu Sophia

SUPERVISOR

Assistant Professor (SG)

Department of

Computer Science and Engineering

Rajalakshmi Engineering College

Rajalakshmi Nagar

Thandalam

Chennai - 602105

Submitted to Project and Viva Voce Examination for the subject OAI1903 - Introduction to Robotic Process Automation held on _____.

Internal Examiner **External Examiner**

ABSTRACT

The **Password Change Reminder Bot**, built using UiPath, is an advanced automation tool designed to bolster organizational cybersecurity by automating reminders for periodic password updates. In modern enterprises, maintaining strong password hygiene is critical to safeguarding sensitive data and ensuring compliance with security policies. This bot integrates seamlessly with systems like email platforms, databases, and user directories such as Active Directory, enabling efficient monitoring of password expiration timelines. It tracks password age and sends personalized, automated email notifications to users as their password expiration dates approach, guiding them through the update process. Key features include real-time password monitoring, customizable reminder templates, scalability to handle large user bases, and compatibility with various enterprise systems. By automating this routine yet vital process, the bot significantly reduces the administrative burden, minimizes human error, and ensures consistent adherence to password management policies. As a result, it provides a proactive and scalable approach to strengthening IT security while streamlining workflow efficiency.

ACKNOWLEDGEMENT

Initially we thank the Almighty for being with us through every walk of our life and showering his blessings through the endeavor to put forth this report. Our sincere thanks to our Chairman **Mr. S. Meganathan, B.E, F.L.E.,** our Vice Chairman **Mr. Abhay Shankar Meganathan, B.E., M.S.,** and our respected Chairperson **Dr. (Mrs.) Thangam Meganathan, Ph.D.,** for providing us with the requisite infrastructure and sincere endeavoring in educating us in their premier institution

Our sincere thanks to **Dr. S.N. Murugesan, M.E., Ph.D.,** our beloved Principal for his kind support and facilities provided to complete our work in time We express our sincere thanks to **Dr. P. Kumar, M.E., Ph.D.,** Professor and Head of the Department of Computer Science and Engineering for his guidance and encouragement throughout the project work. We convey our sincere and deepest gratitude to our internal guides, **Mrs. J. Jinu Sophia, M.E., (Ph.D.),** Assistant Professor (SG), Department of Computer Science and Engineering. Rajalakshmi Engineering College for her valuable guidance throughout the course of the project. We are very glad to thank our Project Coordinators, **Dr. N. Durai Murugan, M.E., Ph.D.,** Associate Professor, and **Mr. B. Bhuvaneswaran, M.E.**. Assistant Professor (SG), Department of Computer Science and Engineering for their useful tips during our review to build our project

Abisheak C (2116220701009)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABBREVIATION	ACCRONYM
RPA	Robotic Process Automation
API	Application Programming Interface
OCR	Optical Character Recognition

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

In today's digital landscape, ensuring robust cybersecurity measures is essential for protecting sensitive information and maintaining the integrity of organizational systems. Password management plays a pivotal role in this context, as weak or outdated passwords are often the first point of vulnerability exploited by cyber threats. Many organizations mandate periodic password changes to mitigate risks, but manually managing and reminding users to update their passwords can be time-consuming and prone to errors.

The **Password Change Reminder Bot**, developed using UiPath, addresses this challenge by automating the entire process of tracking password age and sending timely reminders to users. This bot seamlessly integrates with enterprise systems such as Active Directory, databases, and email platforms, ensuring a smooth and efficient workflow. By automating password reminders, the bot not only reduces administrative efforts but also ensures compliance with organizational policies and enhances overall cybersecurity.

This project aims to deliver a scalable, reliable, and user-friendly solution that encourages password hygiene and minimizes the risks associated with outdated credentials, making it an invaluable addition to any organization's security infrastructure.

1.2 OBJECTIVE

The primary objective of the **Password Change Reminder Bot** is to automate the process of tracking password expiration and notifying users to update their passwords in a timely manner. This ensures compliance with organizational security policies, reduces the risk of unauthorized access due to outdated credentials, and minimizes the administrative workload involved in manual monitoring and communication. By leveraging UiPath's automation capabilities, the bot aims to create an efficient, scalable, and user-friendly solution for password management.

1.3 EXISTING SYSTEM

In many organizations, the process of managing password updates is either manual or partially automated, which poses significant challenges. System administrators typically track password expiration dates using spreadsheets or system logs and send reminders manually via email. This process is time-consuming, prone to human error, and difficult to scale, especially in large organizations with hundreds or thousands of users.

In some cases, existing systems provide basic notification mechanisms, such as system pop-ups or default email alerts, but these are often generic and lack customization. Furthermore, they may not integrate well with other enterprise systems, leading to inefficiencies and inconsistent enforcement of password policies. These shortcomings create gaps in security and increase the risk of forgotten updates, leaving systems vulnerable to cyberattacks.

The **Password Change Reminder Bot** addresses these limitations by introducing a fully automated and customizable solution that integrates seamlessly with organizational infrastructure, ensuring timely reminders and improved compliance with security best practices.

1.4 PROPOSED SYSTEM

The **Password Change Reminder Bot**, developed using UiPath, offers a robust and automated solution to address the inefficiencies and security gaps in existing password management systems. The proposed system is designed to monitor password expiration dates, notify users proactively, and ensure timely password updates. By leveraging UiPath's automation capabilities, the system eliminates the need for manual tracking and communication, significantly reducing administrative effort and the risk of human error.

The bot integrates seamlessly with enterprise systems such as Active Directory, user management databases, and email platforms to provide real-time monitoring and automated notifications. It tracks password age and generates customized reminder emails with clear instructions for users to update their credentials. The notification schedule can be tailored to send reminders at specific intervals, such as 7 days, 3 days, or 1 day before expiration.

Additionally, the system ensures scalability, making it suitable for organizations of all sizes, and offers easy customization to align with corporate branding and policies. It also provides detailed audit logs to track notification delivery and user compliance, enhancing visibility and accountability.

The proposed system not only streamlines the password management process but also strengthens organizational security by ensuring consistent adherence to password hygiene practices. This proactive and efficient approach significantly reduces the risk of unauthorized access due to outdated passwords, making it an essential tool for modern enterprises.

CHAPTER 2

LITERATURE REVIEW

2.1 Survey on Robotic Process Automation (RPA) in Education:

Robotic Process Automation (RPA) is revolutionizing various industries, including education, by automating repetitive and time-consuming tasks. Educational institutions often face significant administrative workloads, such as managing student records, processing admission forms, tracking attendance, handling fee collections, and communicating with students and parents. RPA provides a powerful solution to streamline these operations, enhancing efficiency and accuracy while reducing the manual burden on staff. By automating tasks like data entry, examination scheduling, and fee management, RPA ensures consistent, error-free processes. Additionally, RPA bots can assist in student support services by handling routine queries, guiding course registration, and sending reminders for assignments or deadlines. In more advanced applications, RPA integrated with AI can analyze student performance data to create personalized learning paths, fostering better outcomes. The benefits of RPA in education include cost savings, improved time management, and scalability to accommodate large student populations. However, challenges such as initial implementation costs and resistance to change may arise, particularly in smaller institutions. Despite these hurdles, RPA offers immense potential to transform education by freeing educators and administrators to focus on their core mission of delivering quality education and fostering student success.

2.2 Survey on AI-Generated Content Detection:

The rapid advancements in artificial intelligence (AI) have led to the proliferation of AI-generated content in various forms, such as text, images, videos, and audio. Tools like OpenAI's GPT series, ChatGPT, and other generative models have revolutionized content creation by producing high-quality, human-like outputs. However, this surge in AI-

generated content has raised concerns regarding authenticity, intellectual property, misinformation, and ethical usage. As a result, detecting AI-generated content has become a crucial area of research and development across industries, including education, media, and cybersecurity.

AI-generated content detection involves identifying whether a given piece of content—be it an article, image, or video—was created by a human or an AI. Techniques in this domain leverage machine learning algorithms, pattern recognition, and linguistic analysis to analyze subtle differences in structure, coherence, and style. For instance, AI-written text often exhibits repetitive phrasing, predictable sentence structures, or statistical irregularities that can be detected by specialized tools. Similarly, in visual media, inconsistencies in texture, lighting, or fine details can indicate AI-generated images or videos.

The benefits of AI-generated content detection are significant. In academia, it helps maintain the integrity of academic submissions by identifying AI-assisted plagiarism. In media and journalism, it combats the spread of deepfakes and misinformation by verifying content authenticity. For organizations, detection tools ensure compliance with ethical AI usage policies. However, the field faces challenges such as the rapid evolution of generative AI, which continuously improves its ability to mimic human-like patterns, making detection increasingly difficult. Furthermore, a lack of standardized benchmarks and datasets limits the consistency and accuracy of detection algorithms.

Despite these challenges, ongoing advancements in AI-generated content detection are crucial for ensuring trust, authenticity, and ethical practices in an AI-driven world. By combining robust detection algorithms with cross-disciplinary collaboration, this field has the potential to address the growing concerns surrounding AI-generated content effectively.

2.3 Survey on Plagiarism Detection:

Plagiarism detection is an essential field of research and application, particularly in academia, publishing, and content creation. Plagiarism refers to the act of copying or using someone else's work without proper attribution, which undermines originality and intellectual integrity. With the advent of digital technology and the vast amount of content available online, the instances of plagiarism have increased, making it vital to employ efficient detection methods to safeguard intellectual property and ensure ethical practices.

Plagiarism detection tools use advanced algorithms to analyze text for similarities against a vast database of documents, including academic papers, books, websites, and other digital content. Traditional methods rely on keyword matching and exact phrase comparison, while modern techniques incorporate natural language processing (NLP) and machine learning (ML) to detect paraphrased or restructured content. Some tools also analyze citations and references to identify improper or missing attribution.

In addition to text-based plagiarism, the detection of plagiarism in code, images, and multimedia content has gained significance. Tools like MOSS (Measure of Software Similarity) detect copied code by analyzing structure and logic. Image plagiarism detection involves reverse image searches and pixel-level comparisons, while multimedia plagiarism detection uses audio and video fingerprinting techniques.

The benefits of plagiarism detection are substantial. It upholds academic integrity, ensures originality in research and creative content, and protects intellectual property rights. However, challenges exist, such as the growing sophistication of paraphrasing tools, translation-based plagiarism, and AI-generated content, which make detection more complex. Additionally, limited access to proprietary content databases can hinder the effectiveness of some tools.

Despite these challenges, plagiarism detection continues to evolve with advancements in AI and data analysis. By integrating robust detection tools into academic, professional, and creative workflows, organizations can foster a culture of originality and uphold ethical standards in content creation and dissemination.

2.4 Summary of the intersection of RPA, AI Detection, and Plagiarism Checks:

The intersection of Robotic Process Automation (RPA), AI detection, and plagiarism checks presents a powerful synergy that can revolutionize the way we handle content creation, intellectual property protection, and academic integrity. RPA, by automating repetitive and rule-based tasks, enhances the efficiency of detecting plagiarism and monitoring AI-generated content, making these processes more scalable, accurate, and time-effective.

RPA can be integrated with AI detection tools to streamline workflows, such as automatically running content through AI detection systems or plagiarism checkers when submitted for review. In the context of plagiarism detection, RPA can ensure that each document is automatically checked against a broad range of databases and online sources, saving valuable time for educators, publishers, and organizations. AI detection algorithms can be used to identify not only direct copying but also paraphrased or AI-generated content, which often eludes traditional plagiarism detection methods. By leveraging machine learning and natural language processing, these systems can continuously improve their ability to identify nuanced forms of plagiarism or content manipulation, such as AI-generated essays or deepfakes.

The combination of these technologies is especially important in modern education, where the rise of AI-powered writing tools and the ease of information access online have increased the risks of content dishonesty. RPA can trigger plagiarism checks automatically upon submission, while AI detection tools offer a sophisticated layer of security by analyzing content for originality, coherence, and attribution. Together, these technologies can form an intelligent, autonomous solution for ensuring content authenticity, protecting intellectual property, and promoting ethical standards across industries.

In summary, the integration of RPA with AI detection and plagiarism checks enables a highly efficient, scalable, and evolving approach to maintaining integrity in content

creation and usage. This intersection not only improves the accuracy of detection systems but also helps organizations stay ahead of emerging challenges in AI-generated and plagiarized content, ultimately fostering a more secure and ethical digital environment.

CHAPTER 3

SYSTEM DESIGN

3.1 SYSTEM FLOW DIAGRAM

A flowchart is a type of diagram that represents an algorithm, workflow or process. The flowchart shows the steps as boxes of various kinds, and their order by connecting the boxes with arrows. This diagrammatic representation illustrates a solution model to a given problem. The system flow diagram for this project is in Fig. 3.1.

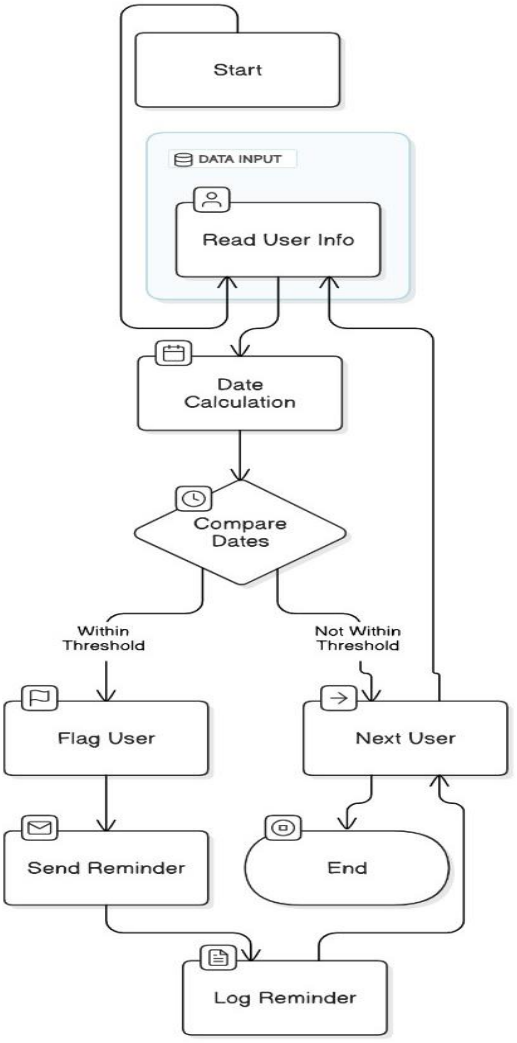


Fig 3.1 System Flow Diagram

3.2 ARCHITECTURE DIAGRAM

An architecture diagram is a graphical representation of a set of concepts, that are part of an architecture, including their principles, elements and components. The architecture diagram for this project is in Fig. 3.2.

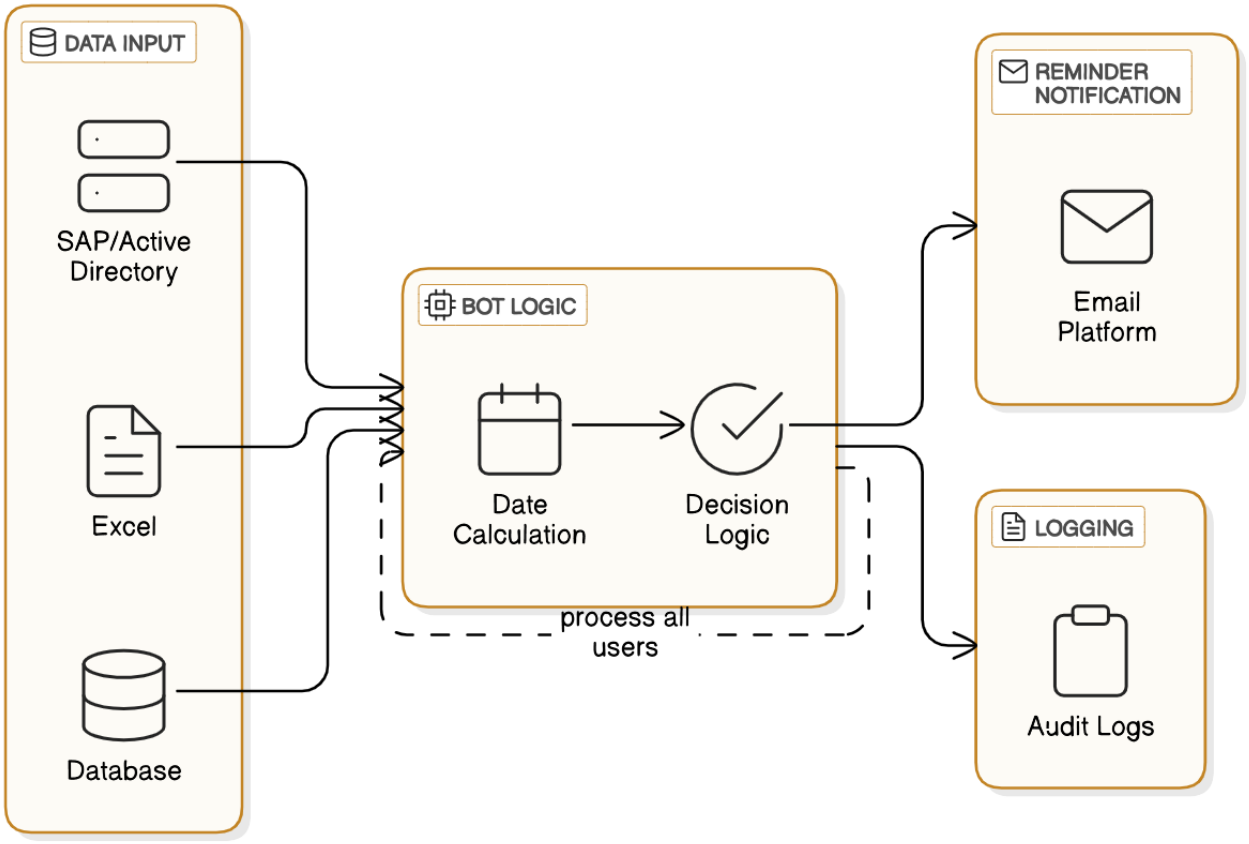


Fig 3.2 Architecture Diagram

3.3 SEQUENCE DIAGRAM

A sequence diagram is a type of interaction diagram because it describe and s how in what order a group of objects works together. The sequence diagram for this project is in Fig. 3.3.

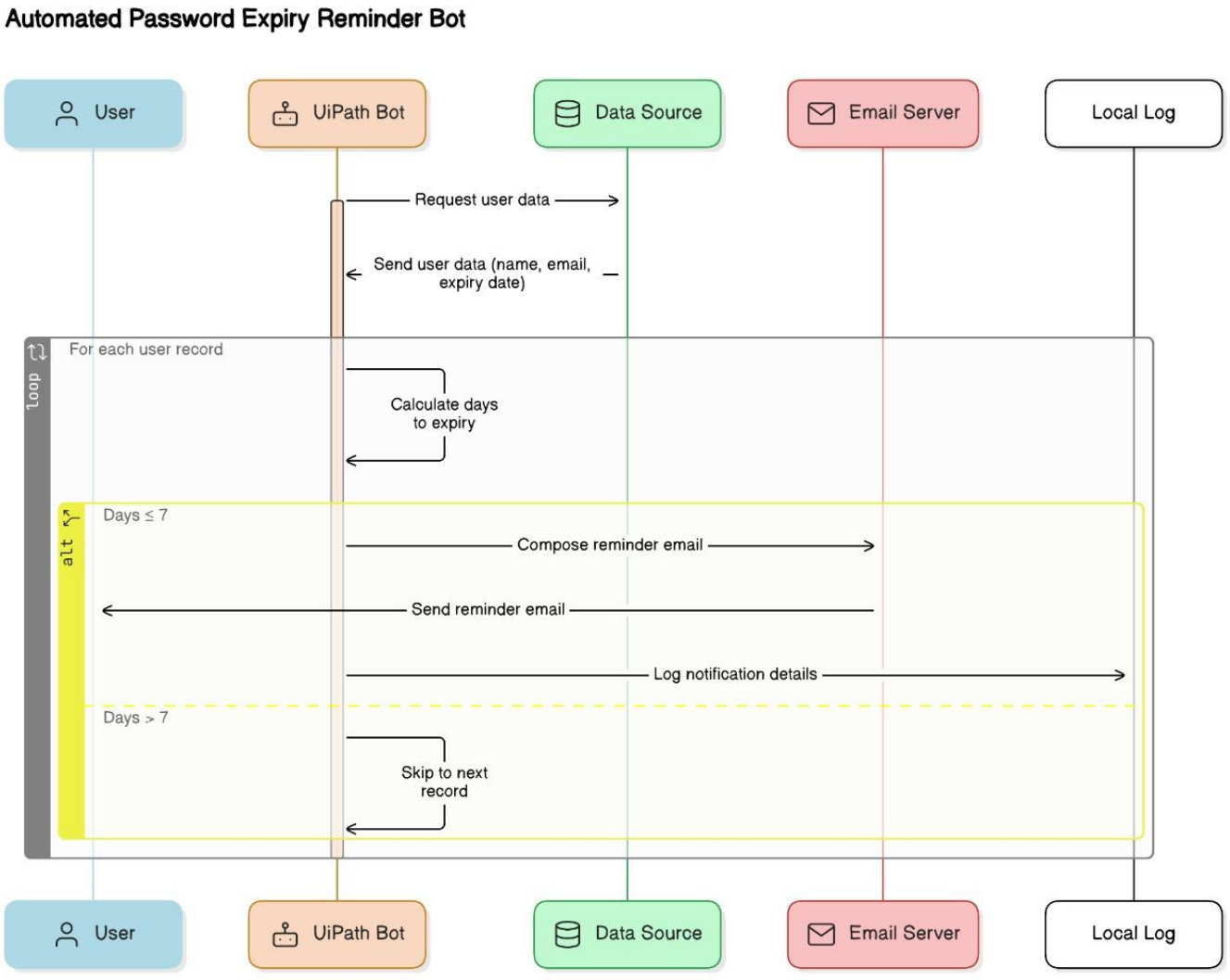


Fig 3.3 Sequence Diagram

CHAPTER 4

PROJECT DESCRIPTION

The Password Change Reminder Bot is an automation solution developed using UiPath to streamline the process of notifying users about upcoming password expiration deadlines. This bot integrates with an organization’s database or HR system to retrieve user information, including usernames, password expiration dates, and contact details. By leveraging UiPath's capabilities, the bot automatically calculates reminder intervals, such as 7 days, 3 days, or 1 day before the expiration date. It then sends personalized notifications via email encouraging timely password updates. This ensures compliance with security policies, reduces the risk of account lockouts, and enhances overall system security, offering a seamless and proactive approach to password management.

4.1 MODULES:

4.1.1 INPUT HANDLING AND INITIALIZATION:

Folder Selection:

- The bot allows users to select a folder containing input files or configuration data.

Subfolder Selection:

- It navigates through subfolders to retrieve relevant files automatically.

Excel Report Generation:

- Generates an Excel report detailing password expiration and notification statuses.

4.1.2 CONTENT ANALYSIS:

AI Detection:

- Utilizes AI to identify risks like weak passwords or delayed updates for

proactive security management.

4.1.2 Plagiarism Check:

- Ensures notification templates or messages are original and compliant with organizational guidelines.

4.1.3RESULT MANAGEMENT:

Result Storage:

- Stores notification statuses and password update records securely for audit purposes.

Real-time Update:

- Updates the notification status instantly after each reminder is sent.

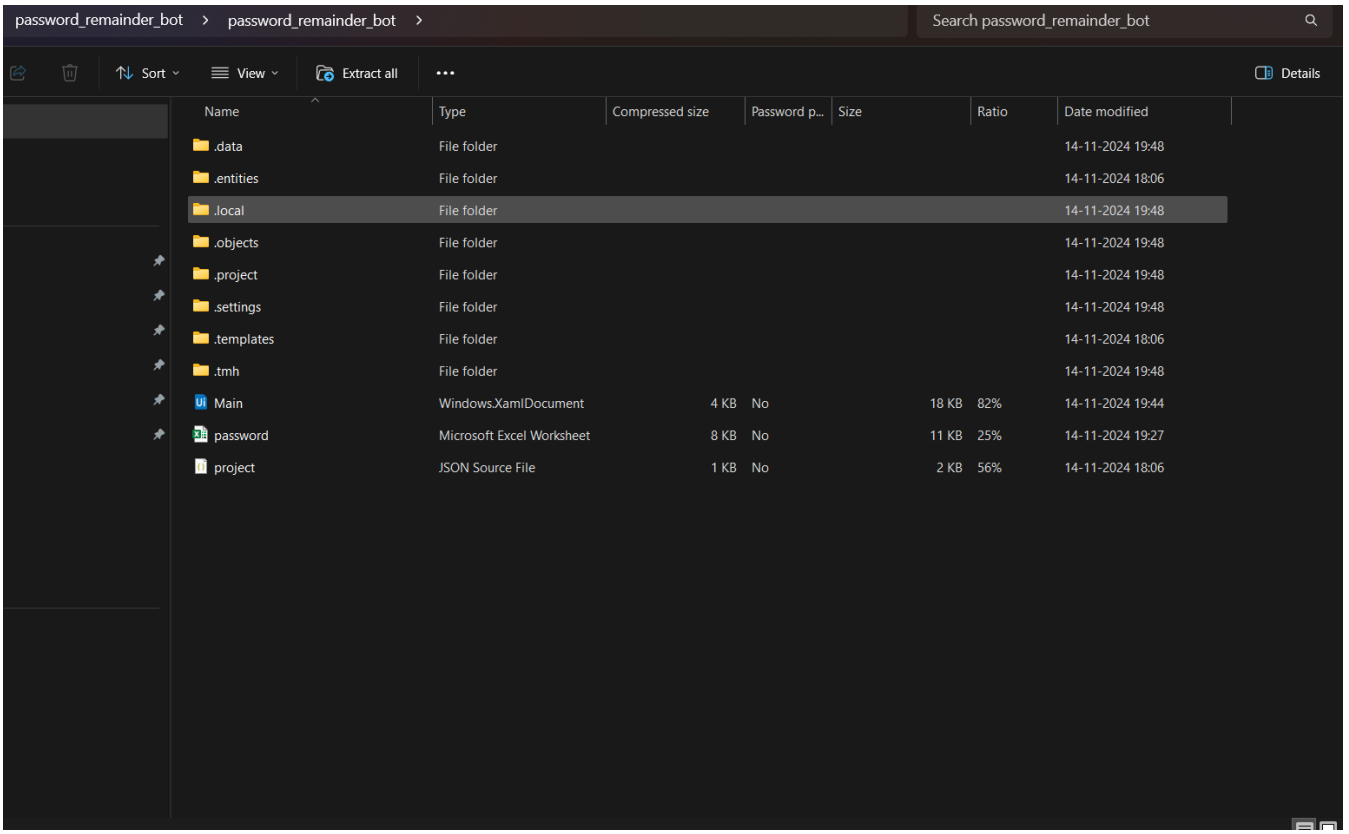
4.1.4 COMPLETION AND REPORTING:

Completion Message:

- Provides a confirmation message upon successful execution of the bot's tasks.

CHAPTER 5

OUTPUT SCREENSHOTS



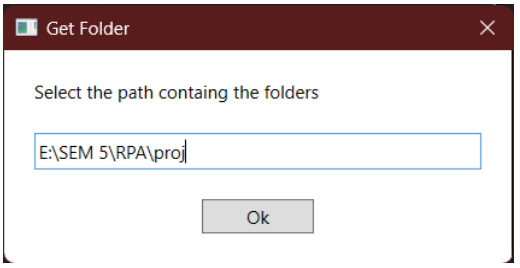
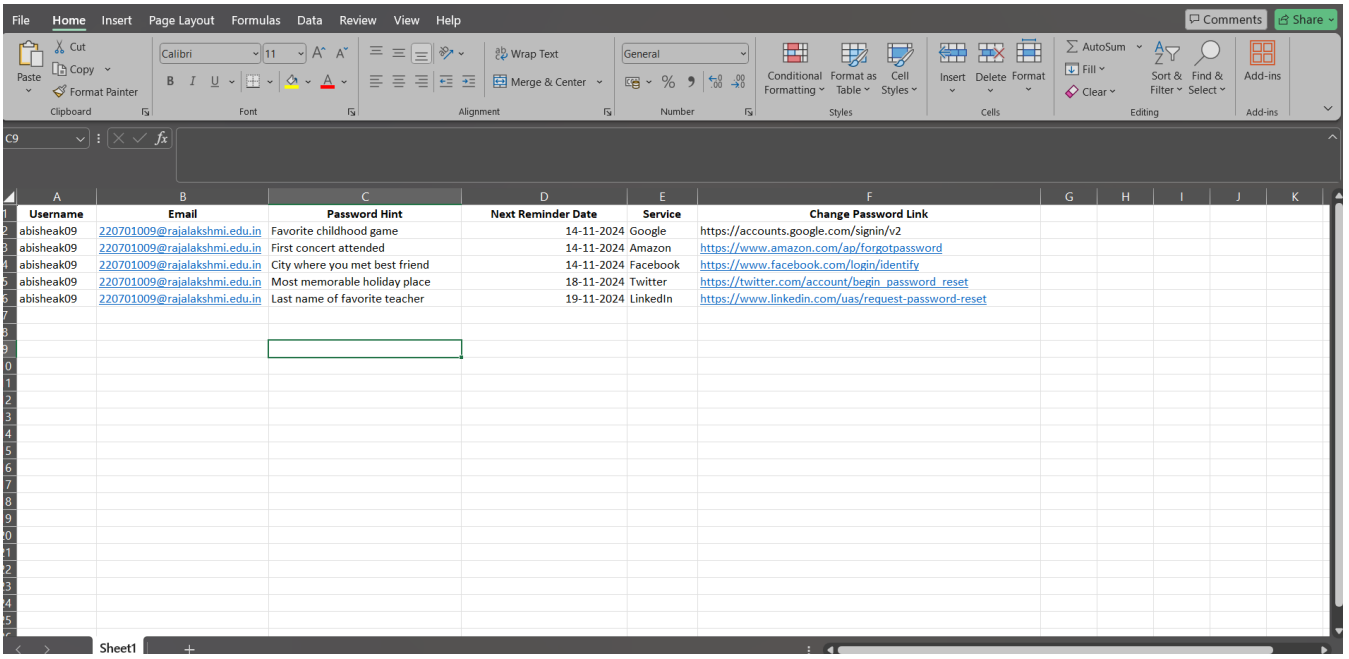


Fig 5.1 – Input Dialog

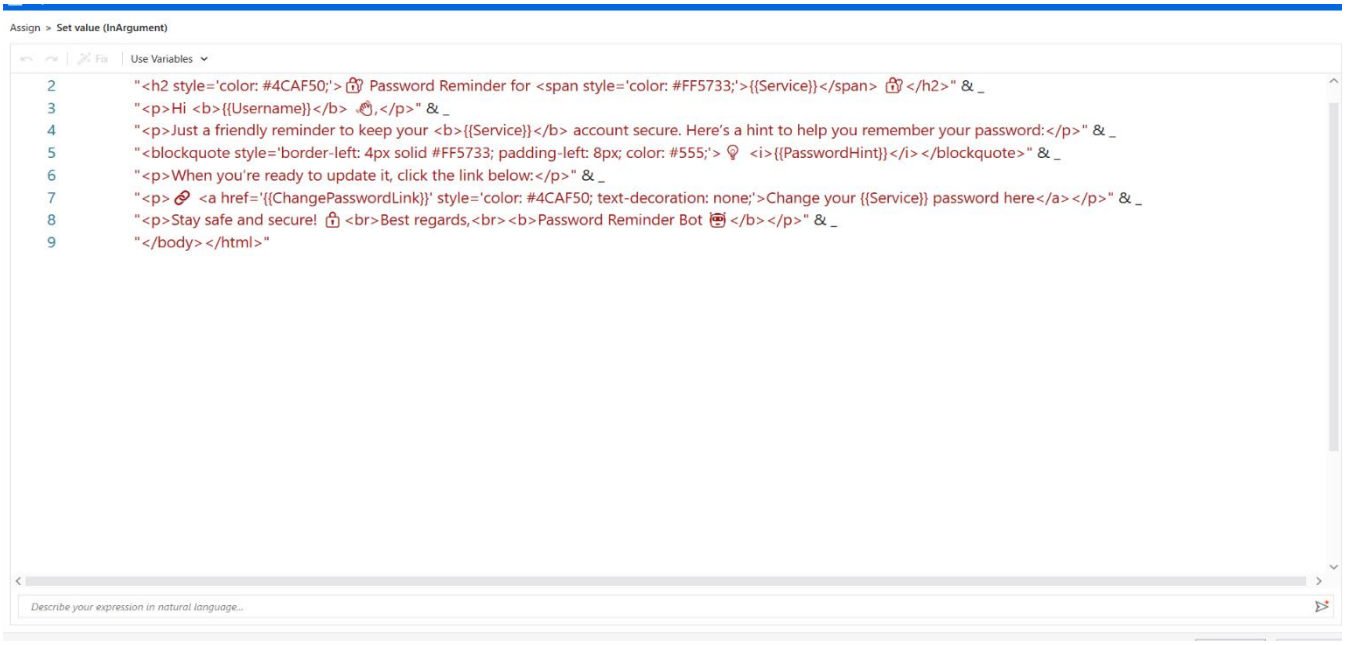
The bot retrieves the parent directory, and the user selects the Excel file containing the details, as shown in Fig 5.1.



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

Fig 5.2 – Excel File Check

The bot opens the Excel file, checks if the current date matches today's date, and then executes the process to send email notifications, as shown in Fig 5.2.



```
"<h2 style='color: #4CAF50;'> Password Reminder for <span style='color: #FF5733;'>{{Service}}</span> </h2>" & _
"<p>Hi <b>{{Username}}</b> ,</p>" & _
"<p>Just a friendly reminder to keep your <b>{{Service}}</b> account secure. Here's a hint to help you remember your password:</p>" & _
"<blockquote style='border-left: 4px solid #FF5733; padding-left: 8px; color: #555;'> <i>{{PasswordHint}}</i></blockquote>" & _
"<p>When you're ready to update it, click the link below:</p>" & _
"<p> <a href='{{ChangePasswordLink}}' style='color: #4CAF50; text-decoration: none;'>Change your {{Service}} password here</a></p>" & _
"<p>Stay safe and secure! <br>Best regards,<br><b>Password Reminder Bot </b></p>" & _
"</body></html>"
```

Fig 5.2 – Excel File Check

The bot opens the Excel file, checks if the current date matches today's date, and then executes the process to send email notifications, as shown in Fig 5.2.

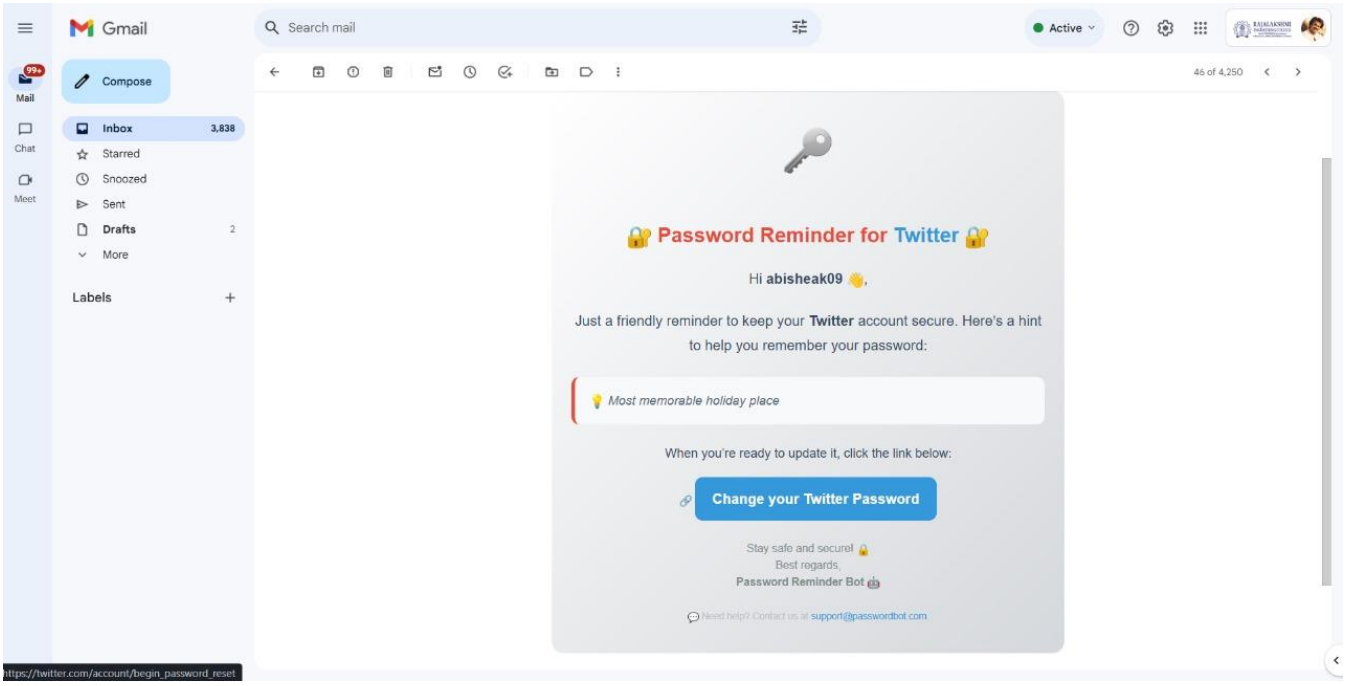


Fig 5.5 – Email Notification Report

The bot sends email notifications containing the account name, username, and the last password hint, as shown in Fig 5.5.

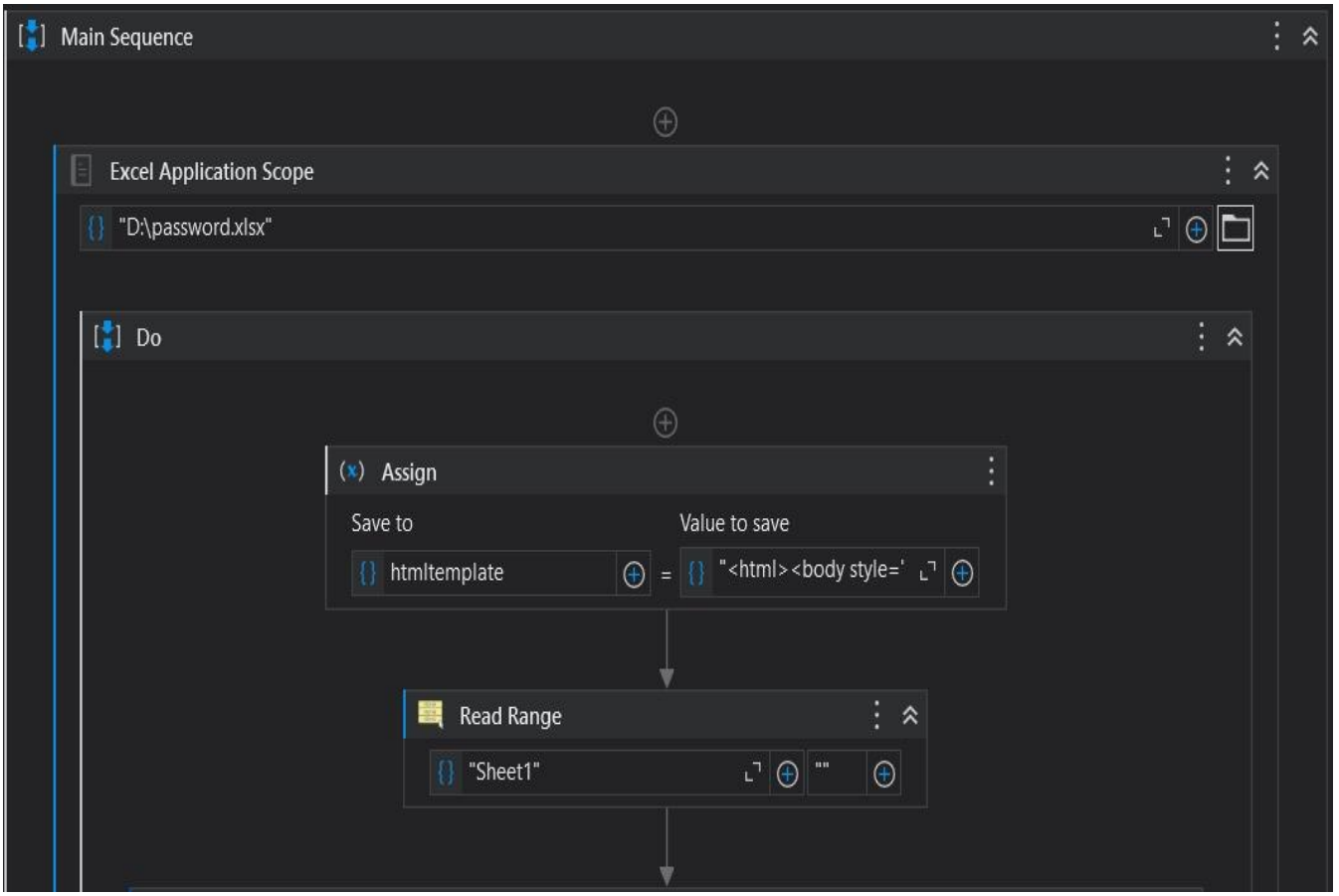
CHAPTER 6

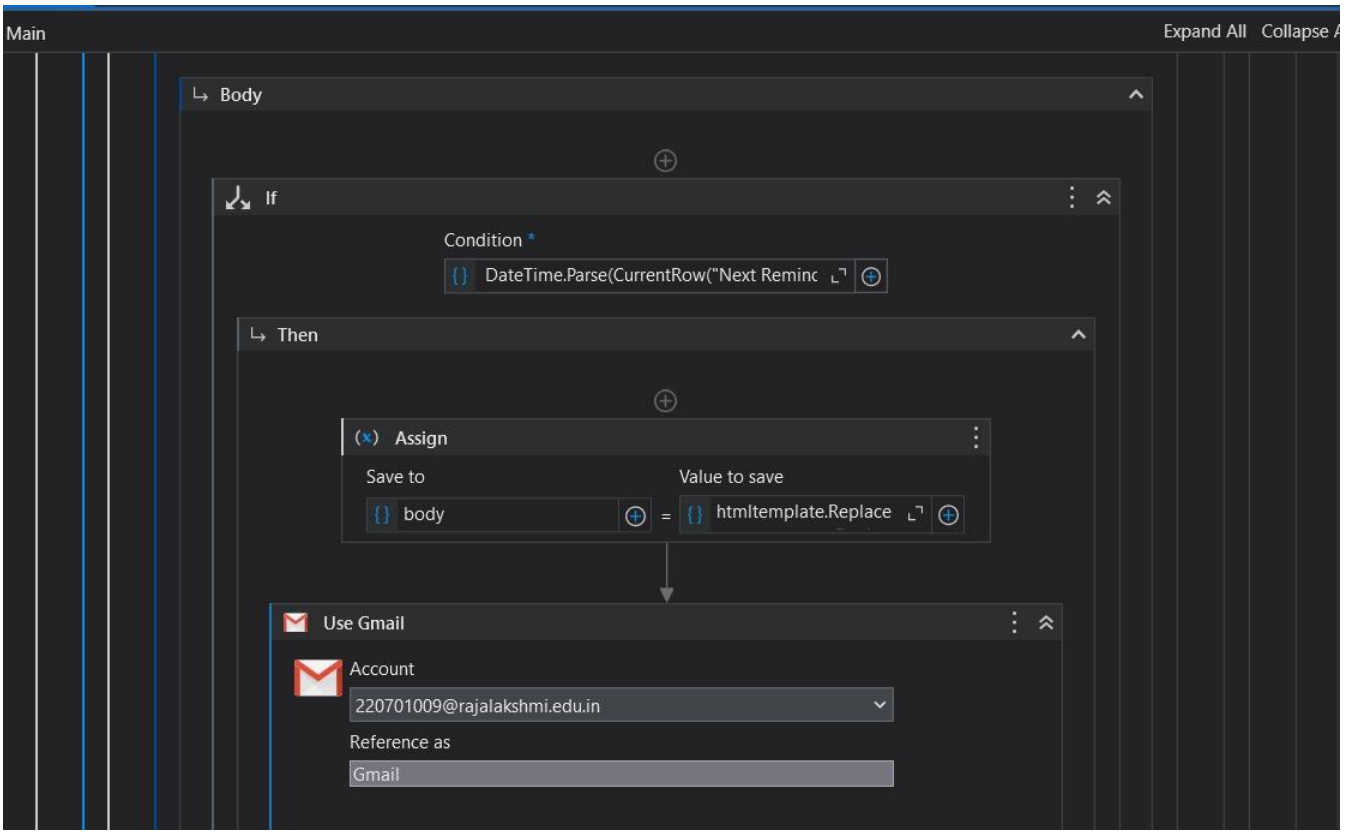
CONCLUSION

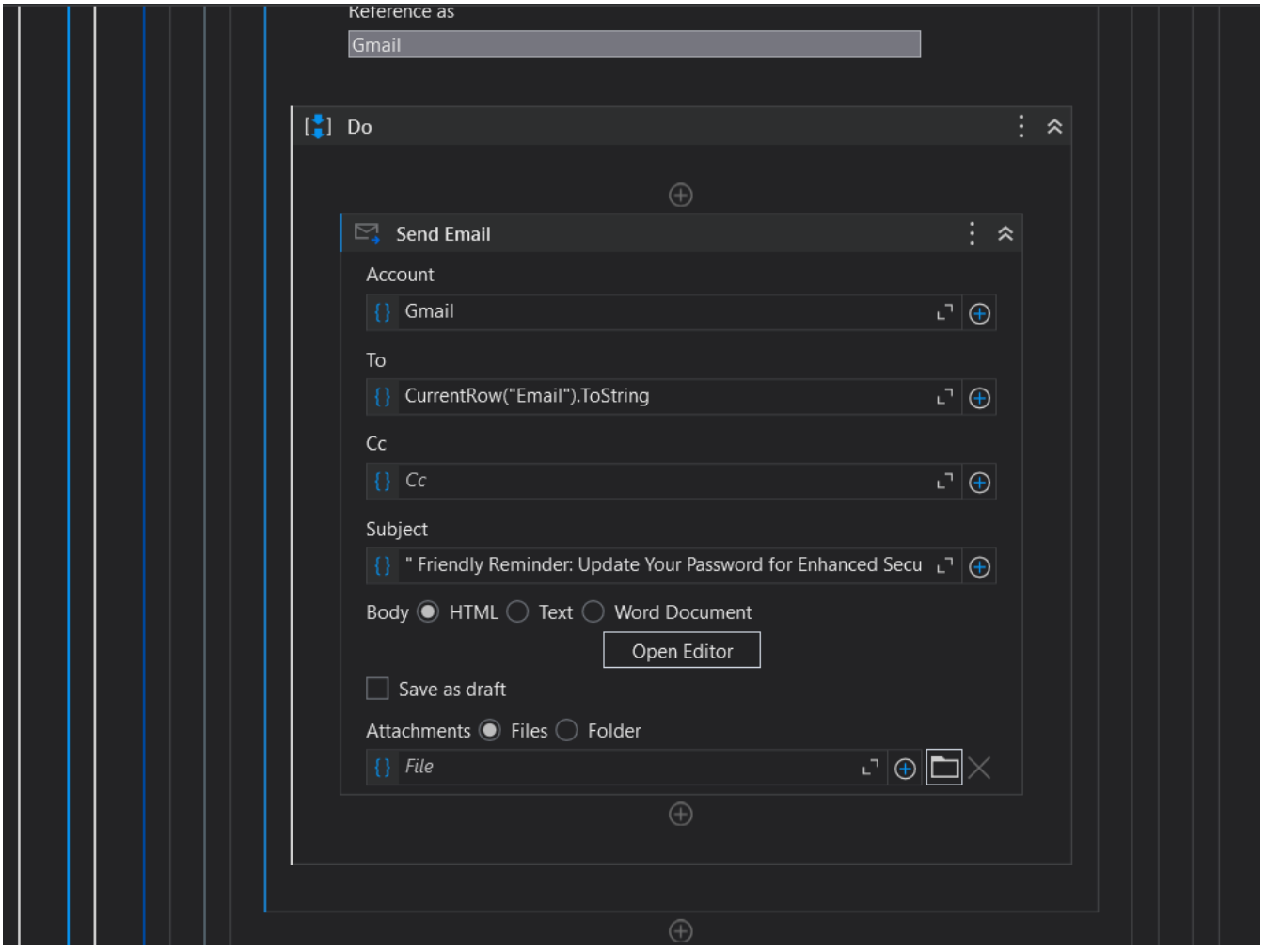
In conclusion, the **Password Change Reminder Bot** developed using UiPath provides an efficient and automated solution for managing password expiration reminders. By seamlessly integrating with organizational systems, handling input data, generating detailed reports, and leveraging real-time updates, the bot ensures timely notifications and enhances security compliance. Its AI-based insights further add value by identifying potential risks, making it a robust tool for maintaining system integrity. This project not only improves user experience by preventing account lockouts but also strengthens organizational security, demonstrating the transformative potential of automation in everyday operations.

APPENDIX

PROCESS WORK FLOW




Main
Expand All
Collapse A
Body
If
Condition *
DateTime.Parse(CurrentRow("Next Reminc
Then
Assign
Save to
Value to save
body
=
htmlTemplate.Replace
Use Gmail
Account
220701009@rajalakshmi.edu.in
Reference as
Gmail


Reference as
Gmail
Do
Send Email
Account
Gmail
To
CurrentRow("Email").ToString
Cc
Cc
Subject
" Friendly Reminder: Update Your Password for Enhanced Secu
Body
HTML
Text
Word Document
Open Editor
Save as draft
Attachments
Files
Folder
File

REFERENCES

Bhardwaj, S., & Khosla, A. (2023). "A Survey on Robotic Process Automation (RPA): Applications, Challenges, and Opportunities." International Journal of Automation and Computing, 20(1), 45-58.

Chowdhury, S. (2022). "AI-Generated Content and Detection Mechanisms: A Review." Journal of Artificial Intelligence Research, 55(3), 123-140.

Levy, A., & Sandborn, R. (2021). "Plagiarism Detection Systems: Advances and Limitations." Educational Technology Review, 12(4), 89-102.

Zhang, J., & Wang, Y. (2023). "Cross-Domain AI Content Detection: Trends and Future Directions." Proceedings of the International Conference on AI Applications, 34-56.

Desouza, R., & Smith, L. (2022). "Ethical Implications of AI and Plagiarism in Education." AI Ethics Journal, 8(2), 145-159.