National College of Ireland

SecureMail: An RPA Approach to Phishing Detection

MSc Research Project
MSc Cyber Security

Surya Punj Sharma
Student ID: 2228403

School of Computing
National College of Ireland

Supervisor: Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Surya Punj Sharma……

Student ID: 2228403……..……

Programme: MSc Cyber Security…… **Year:** 2024……..

Module: Practicum……

Supervisor: Khadija Hafeez ……..……

Submission Due Date: 12-08-2024……..……

Project Title: SecureMail: An RPA Approach to Phishing Detection……

Word Count: 5500…… **Page Count** 16……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Surya Punj Sharma……

Date: 06-08-2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

SecureMail: An RPA Approach to Phishing Detection

Surya Punj Sharma
22228403

Abstract

Phishing attacks have been a major threat to organisations and individuals and may lead to big data breaches or complete shutdown of business processes. Effective phishing detection methods have been in industry from long period of time but due to new trends in phishing techniques some innovative approach is essential to counter it, and the motivation of this project was to look for alternate technique to tackle phishing emails. The project work emphasizes on the role of RPA (Robotic Process Automation) technology to detect phishing emails in user mailbox that provides the user extra sense of awareness while opening a potentially suspicious email. This study explores the implementation of Microsoft's RPA tool; Power Automate. The RPA flow designed in Power Automate retrieves the emails from Gmail server and further analyse them by finding malicious words or checking the quality of link. The main finding of this project promotes the technology RPA in automating phishing detection, Automation being a huge market in the world data, offers scalability and an important solution in field of Cyber Security. The successful implementation and positive final evaluations demonstrate that the use of interactive GUI (Graphical user Interface) and low code solutions with RPA tools can help in improving the phishing detection capabilities.

1 Introduction

Over 3.4 billion emails per day are sent by cyber criminals that make more than trillions mails in one year (Gary Smith, 2023). These phishing email looks like normal day to day mails, the frequency of phishing emails and attachments poses a big threat to individuals and companies, . Phishing attacks trick victims into disclosing personal information or running malicious software, it tricks the victims by putting a malicious link in body, seeking urgency for sensitive information e.g.: a mail from for law agency or a passive blackmail mail. It has become increasingly complicated which causes financial and reputational damage. According to Anti-Phishing Working Group (APWG), phishing attacks have increased dramatically in recent years, and demands the urgent need for robust detection and prevention systems (APWG, 2023).

According to Aguirre and Rodriguez (2017), Robotic Process Automation (RPA) is considered as a potential approach for automating repetitive processes with a rule based approach while maintaining efficiency and accuracy. This technology can integrate with various tools and software and can also communicate with digital systems just like an actual "Bot".

We can consider the scenario where RPA might be of use: An employee of an IT company leave out daily to an office and start doing manual testing of data on Microsoft Excel or any other software by just checking the following pre-defined rules of that task.
RPA comes into picture because an RPA tool can be designed in a logical manner to do all the repetitive work done by the employee and extra resources allowing them to concentrate on complicated tasks. Organizations with RPA can potentially improve their email security by automating the detection and reporting of phishing emails and malicious attachments. This strategy also decreases the amount of manual effort required to differentiate between phishing and legitimate email.
In the domain of email security, State of art RPA solutions can implement rules to detect phishing type emails. RPA solutions can be designed to cross reference threat databases that can give alert for a potential threat for future inspections. Methods like Nature Language Processing (NLP) and Optical Character Recognition (OCR), if integrated with RPA can give a robust solution for email content analysis.
RPA can be used to improve email security, by creating workflows that automatically identify dangerous emails, isolate them, and notify users or IT teams. This method lowers the need for human oversight while greatly increasing the efficiency of current security protocols.

The research question is: "***How can potential phishing emails and malicious content in user email inboxes be efficiently detected and reported to users using Robotic Process Automation (RPA) technology?"***
The objective of this is to investigate the capabilities of RPA in the context of email security and to create a flow for integrating RPA with existing security measures, and to assess the ability of RPA based solutions in the field of cyber security.

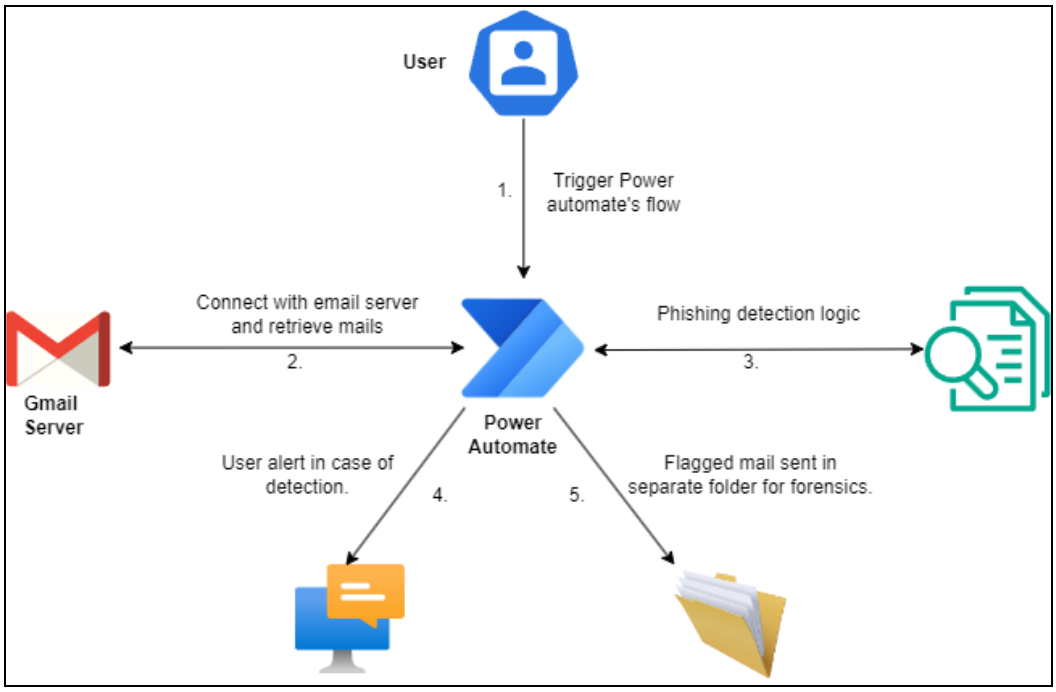

Figure 1. System design

Figure 1 illustrates the system design for the project showing the process of detecting potential phishing with a Microsoft's RPA tool Power automate. The user will trigger the build flow, then Power Automate (connected through Gmail's app password[1]) will retrieve inbox mails and analyse each one according to the developed logic. The Tool will notify users in case of detection and move flagged high severity mails to a different label/folder in Gmail. This will let user know that mails in that folder need extra level of examination as they are suspicious.

This research intends to adds further evidence on the use of RPA in cybersecurity, specifically phishing detection and prevention. While much research has investigated and implemented machine learning and artificial intelligence solutions for email security, Robotic process automation is still not explored fully in this context. This project intends to provide insights to both academics and industry by presenting a detailed demonstration of RPA's strengths and limits in adding an extra layer in sector of email security.

2 Related Work/ Literature Review

Robotic process automation for phishing detection with email automation is a growing area in field of cyber security (CoCo Pierce, 2024). The following literature review critically evaluates current research on this issue to support the proposed study on utilizing RPA tools to detect and report potential phishing emails. The focus of this review is to find new avenues of investigation, understand methods and highlight strengths, weakness and limitations of past studies in order to advance in this area with a novel study design.

2.1 RPA in Fraud detection

Stadlinger and Dewald (2017) introduced a forensic email analysis tool which analyses all the emails in a mailbox and segregate based on suspected mail, find patterns in communication in single or multiple accounts, and identify communication partners in the form of graph visualization of email data using statistical tools. However, it's limited to verification of the malcious message in real scenarios. As a future suggestion, Stadlinger and Dewald suggested implementing a user interface where forensic reports are directly generated to witness the process and export into the results. This helped to understand the automation solutions required for email analysis where RPA tool can play an important role which I adapted.

Mishra, Mishra and Kumar (2022) talk about using four different modules (SMS Content Analyzer, URL Filter, Source Code Analyzer and APK Download Detector) to analyse and identify malicious content and keywords, features, harmful embedded code, and downloaded malicious files while filtering URL respectively. Their implementation has produced result accuracies up to 96.29%. This model is far better than other models in comparison.

[1] https://support.google.com/mail/answer/185833?hl=en

Study of Catnip Infotech Private Limited (2023) highlights the role of Robotic Process Automation (RPA) in mail automation. This helps to automate the process of sorting, filtering, and responding to repetitive emails. It increases the productivity and enhances the business operations. Although it is limited to managing general emails rather than complex ones it justifies the need of RPA that I have implemented in this paper.

2.2 RPA research in Forensics Analysis

Thekkethil *et al.* (2021) investigates about how application of RPA are helpful in fraud detection. Loan frauds, for instance, is an ongoing threat. All major financial institutions are working towards to implementing the concept of RPA technologies that help to improve fraud prevention and mitigate other human errors. This paper explains how RPA can mitigate fraud risks through various methods including reassessing current processes, eliminating human error, enhanced trade monitoring, automated threat detection, searching for anomalies. Although there is no direct focus on phishing detection, it gives ideas to integrate RPA with forensic tools for phishing detection.

Asquith and Horsman (2019) introduce RPA for task automation. Two case studies are discussed to demonstrate how RPA helps in improving efficiency in the field. These case studies are Autopsy[2] pre-processing tasks and loading content into Griffeye[3]. Although this work examined UiPath[4], more research is required to understand the functionality of RPA tools in the field of digital forensics which is also a source of motivation to discover role of RPA in field of cybersecurity.

2.3 Phishing detection with machine learning

Basit *et al.* (2020) presented a method for the timely detection of a phishing attack on a website . They also discussed how important is phishing detection. In this paper, three machine learning classifiers are named as k- nearest neighbours (k-NN), Artificial Neural Network (ANN) and C4.5. It has shown better accuracy after the ensemble learning which means combining two or more classifiers mentioned above. The authors suggests that multiple datasets can be used for further evaluation. Developing a pre-trained plugin has also been suggested as future work. This paper helped in creating the foundation for integrating solutions.

Hina *et al.* (2021) used a multi-label email classification method to organize emails. It helped in investigating email crimes. Logistic Regression and linear regression algorithms provided better accuracy results while Stochastic Gradient Descent showed the lowest accuracy rate. The authors

[2] https://www.autopsy.com/about/
[3] https://www.dataexpert.eu/products/digital-forensics-griffeye/
[4] https://www.uipath.com/about-us

planned to incorporate blockchain for storing and accessing forensic data in future work. This study was useful for understanding the ML integration with RPA during implementation.

Khababa *et al.* (2023) has discussed using multilayer perceptron to classify spam emails. When comparing with other algorithms, like Support Vector Machine (SVM) and decision tree, this model is superior, with accuracy of 94.4% on test data. This method has cost constraints and is time-consuming. Although it has some weaknesses, it is the best method for classifying spam emails according to study. To improve performance and scalability in the future the author advise expanding training data and optimising resource data. This study encouraged to use of these solutions for detecting phishing.

Atawneh and Aljehani (2023) show the usage of machine learning techniques in detecting email phishing attacks. The best results are achieved by using transformer-based models like Bidirectional Encoder Representations from Transformers (BERT) and Long short-term memory (LSTM). The ML model developed in this study is effective with accuracy of 99.61%. The author recommended using phishing email detection in antivirus software, with firewalls to enhance security as a single system cannot provide complete security. Developing transformer-based models for phishing email detection has been suggested as future work.

2.4 Phishing trends during Pandemic

This paper of Lallie *et al.* (2021) talks about the cyber incidents that occurred during the Covid 19 pandemic in 2020. During this period cyber attackers begin phishing campaigns which sent URLs or files to victims which contained malware for purpose of financial fraud. A high number of phishing attacks are detected with this analysis. However, it's limited to predicting relation between events and cyber-attacks. This paper highlighted the need to detect phishing with a new approach.

Pitchkites (2021) discussed email security threats during pandemic. The TLS protocol helps to securely deliver data over the internet. Best practices for email security have been presented like multifactor authentication and DMARC protocol. However, this method still had flaws to protect emails from attack, hence it shows the need for efficient and interactive methods in phishing detection like an integration of RPA tool.

Qualitative semi-structured interviews were conducted by Scott (2022) among eight employees of corporate companies with (Work from Office) WFO and (Work from Home) WFH experience. The factors influencing user susceptibility to phishing emails was discussed in this paper. As the design relied on interviews, it may impact the quality of the results due to misinterpreting questions, and misclassifying phishing mails. For future research author has suggested investigating security protocols utilized by teleworkers, and malicious links in emails clicked by WFH employees.

2.5 Critical Analysis of Literature

The literature review has been divided into four sections. The first two sections discuss how RPA is effective in fraud detection and forensic analysis. Section three's literature paper talks

about the detection of phishing emails using machine learning techniques. And last section has discussed papers showing trends of phishing during a pandemic. Stadlinger and Dewald (2017) contributed to the digital forensic field using the email analysis tool. This has made a significant impact on this paper on understanding the phishing emails. Some papers helped to understand how ML models helped in achieving email security. Catnip Infotech Private Limited (2023) helped to understand the importance of RPA in streamlining the email management process that helped in customer satisfaction. It motivated to learn more about RPA technology and to identify phishing emails accurately and notify users.

This literature review highlights the importance of Robotic process automation in improving email security through automation and its integration with different logic and algorithms. Existing studies show many aspects of RPA's capabilities but there is a gap in integrating RPA for phishing detection and reporting. Research that has already been done offers a solid foundation for RPA's automation role as well as the first steps in using various logics like making visualization tools or just classifying data in a system can be useful from security point of view. A need for more research is highlighted by the fact that many studies fail to focus on automated threat detection and reporting. By creating an RPA based system for proactive phishing identification and user notification, my research aims to close this gap.

2.6 Summary Table

Below is the summary table of related studies conducted, highlighting their methods, results and weaknesses to provide an overall view of previous literature to readers.

Table 1: Literature Review summary

Study	Methodology	Outcome/s.	Limitation/s.
(Stadlinger and Dewald, 2017)	Visualization tool.	The pattern was generated that helped to identify suspicious emails by filtering time ranges and groups.	Parsing speed was not good as expected by the researchers and not all type of mailboxes were compatible with the tool.
(Mishra, Mishra and Kumar, 2022)	RPA solution which extracted loads of Covid 19 data from emails.	The extraction was successful with the help of RPA tool.	Only the scope was limited to extraction of data, not analysing it.
(Basit *et al.*, 2020)	Implemented machine learning algorithms to detect phishing.	The researched compared different classifiers and RFC turned out to be best for their dataset.	Phishing detection research was limited to a single and straightforward database.
(Khababa *et al.*, 2023)	Multi-layer perceptron was used to filter spam emails out.	Effective accuracy score achieved	Limited to existing databases and Phishing emails were not considered.
(Catnip Infotech Private Limited, 2023)	Robotic process automation to classify emails.	Low error handling was achieved	No sort of detection logic was used by the organisation.
(Thekkethil *et al.*,	RPA solution build to	The RPA helped to	The tool build is

2021)	smooth bank processing and detect fraud detection in loan applications.	detect fraud in loan application by eliminating the human intervention of making decision to approve a loan.	limited to detect fraud only on loan processing not any other frauds.

3 Research Methodology

3.1 Steps followed

This research methodology compromised the following steps:

1. Power Automate Desktop RPA tool was finalized after comparing existing tools like UI Path, Automation Anywhere etc. (refer Table 2)
2. A new Google's Gmail[5] ID was created for this project for test purposes. Gmail was used as a mail server because of its popularity globally. (Porch Group, 2024)
3. After tool selection, the flow was built logically to detect phishing in a rule-based manner.
4. The phishing templates used were designed for a company Gophish[6], a phishing testing tool.
5. Those templates were sent to the new Gmail id created.
6. VirusTotal[7] was integrated into the RPA flow to check the link in body text of emails is legitimate or not.
7. Malicious words were mapped with mail content through RPA tool.
8. A mail violating more than one security issue will be flagged as high severity e.g.: A link with high URL score through Virus total and which included malicious words.
9. A new label of suspicious mail was created to categorise suspicious mails of high severity into that.

3.2 Technology used:

The basis of the project revolves around utilization of RPA tool to detect phishing. Robotic Process automation technology copies the actions of people interacting with a software or program to perform tasks of large volume, highly repetitive tasks. The tool of this technology helps developers to make a bot that can integrate with other applications, tools or software and can also design a workflow to accomplish predefined tasks.
RPA tools have its applications in almost every sector of business including banking, healthcare, manufacturing and innovation. The businesses adapt the RPA technology to increase their company's productivity and reduce operational costs. RPA's advantage is its integration capabilities with various online services.
The bot developed becomes intelligent enough to put keystrokes on window where required, it can easily navigate patterns on desktop screen, extract data from webpages, documents etc.,

[5] https://www.google.com/gmail/about/
[6] https://getgophish.com/documentation/
[7] https://docs.virustotal.com/docs/how-it-works

Then modify, store or process the extracted data, store it or even process it. It can also run scripts for more flexibility. Essentially, RPA bots can perform every task that a tester or developer does in their day-to-day professional life.
Tools like UiPath and Power automate are RPA tools which also leverage integration of this with Artificial intelligence and machine learning. They use state of the art technologies including Optical character recognition (OCR) and Natural language processing (NLP) which are state of the art technologies to extract and analyse data. Microsoft's Power Automate was chosen for this project.

The tool was finalized by its integration capabilities with mail servers and availability. Power Automate Desktop is built with more user-friendly interface which help developers to reduce their learning curve in understanding how to operate the tool and start with implementation quickly (Kanerika, 2023). This tool also brings Microsoft's strong security framework which is not used in other automation tools which is extremely important for handling information in this project of phishing detection (Bart Teodorczuk, 2022).

Table 2. Comparison study of different RPA tools

Features	**Microsoft's Power Automate**	**UI Path**	**Automation Anywhere**
Integrations	Vast services and easy to integrate	Integration features are complicated	Complicated to integrate with 3rd party services.
Usability	Interactive GUI for beginners.	GUI is good but still formal training is required to work around	Complex for beginners.
Cost	Free tier for the project	Separate license required for project.	High cost.
Security	Strong features of Microsoft's security	Manual configuration required	Manual configuration required.
Accessibility	Pre-installed in Windows machine	Installation required	Installation required.

Gmail mail server was used because of its integration capabilities and popularity, The phishing templates designed by (Caleb Riggs, 2022) were used for this project which were primarily designed for Gophish. The templates contained structural format of possible phishing emails, with number of suspicious flags. The role of RPA tool was to detect and segregate them according to severity.

3.3 Measurements:

The measures considered while collecting phishing emails templates were the standard attributes like: Relatability, Urgency, Attention seeking, threatening. These are the major traits that are commonly used in phishing emails and encourage users to click on a link or share sensitive information (Tornblad *et al.*, 2021). Each template was reviewed to determine that it contained all the traits, then converted into readable format and sent to the target email.

Mapping the body text of emails with suspicious words and checking the quality of link present inside mail body were implemented in the RPA flow to detect the phishing emails. These were found to be the root cause of over 66% of data breaches worldwide (Gary Smith, 2023).

4 Design Specification

The main logic designed in RPA flow for detecting suspicious phishing emails is illustrated in the figure 2 below.

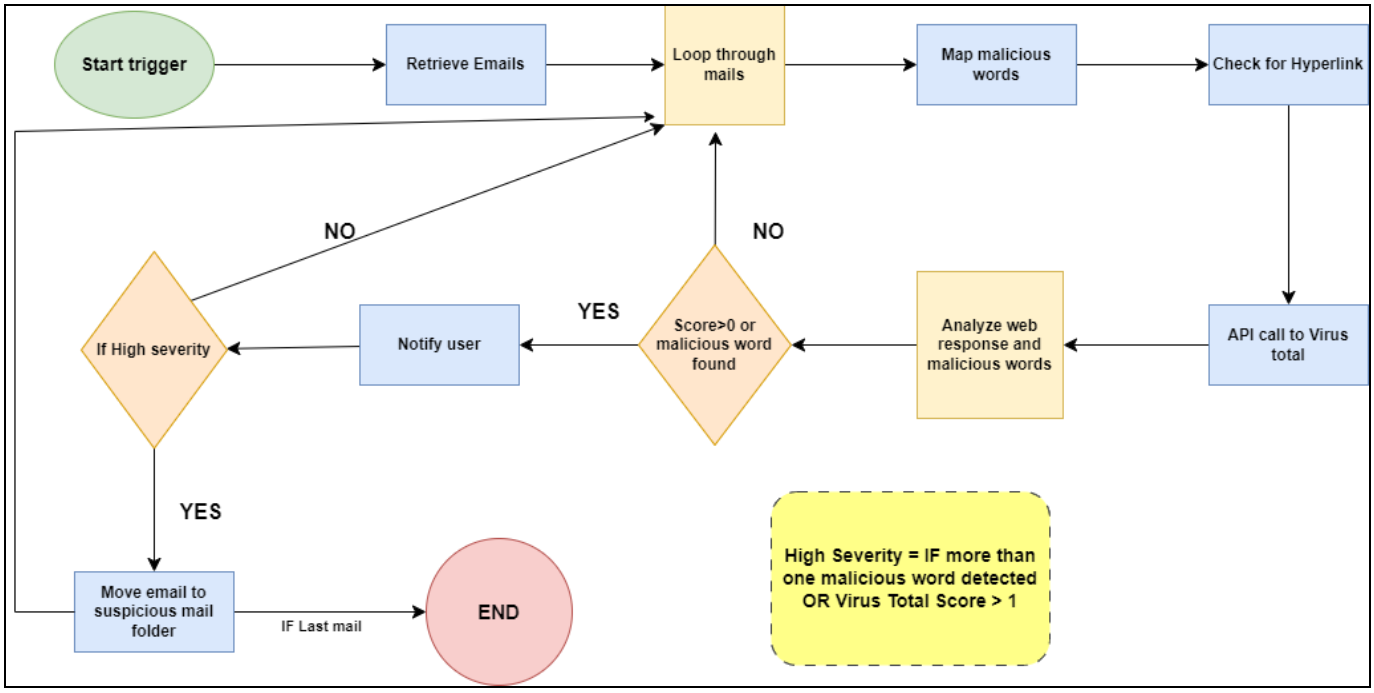

Figure 2. Flow logic.

The flow shows the logic of a rule-based phishing detection through an RPA tool. When RPA flow is triggered all the mails in user inbox are retrieved by the tool and are stored in a variable with lists, which is further broken down into individual part of email e.g. subject to sender info. Screenshots are shown in figures 3 and 4. The score depiction in the flowchart is from API response of Virus Total, it provides score of every URL on basis on public reports, 0 indicating no threat.

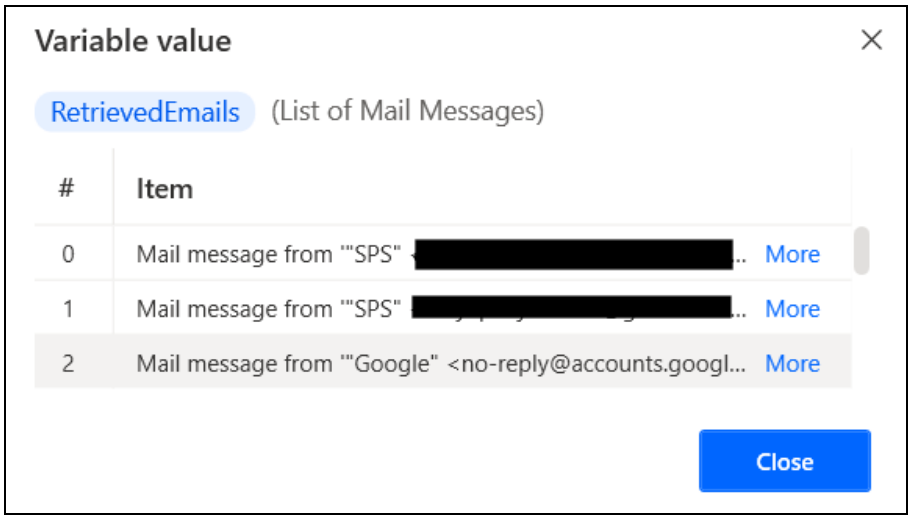

Figure 3. Mails retrieved

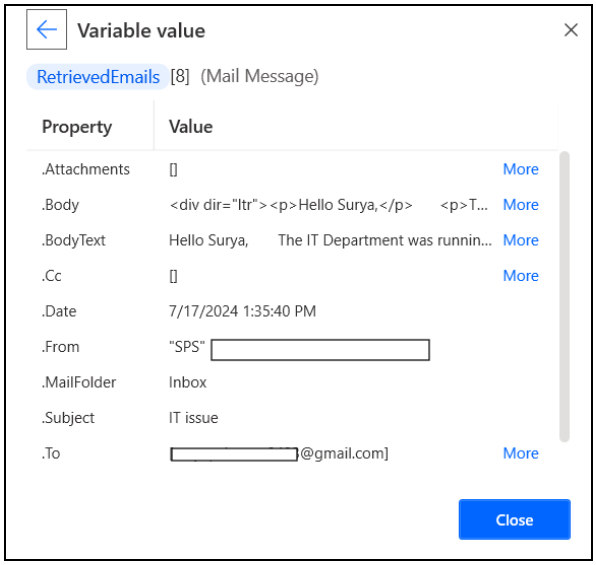

Figure 4. Mail components

The specifications in above the flowchart were succesfully designed with Power Automate's interactive GUI. The purpose of an RPA tool is to make automated bots which complete the desired tasks and to increase the productivity of an organisation, for that a logical flow structure has to be designed. Due to RPA tool's low code design structure and robust processing power it this is possible. A screenshot of tool showing the flow structure is shown in figure 5.

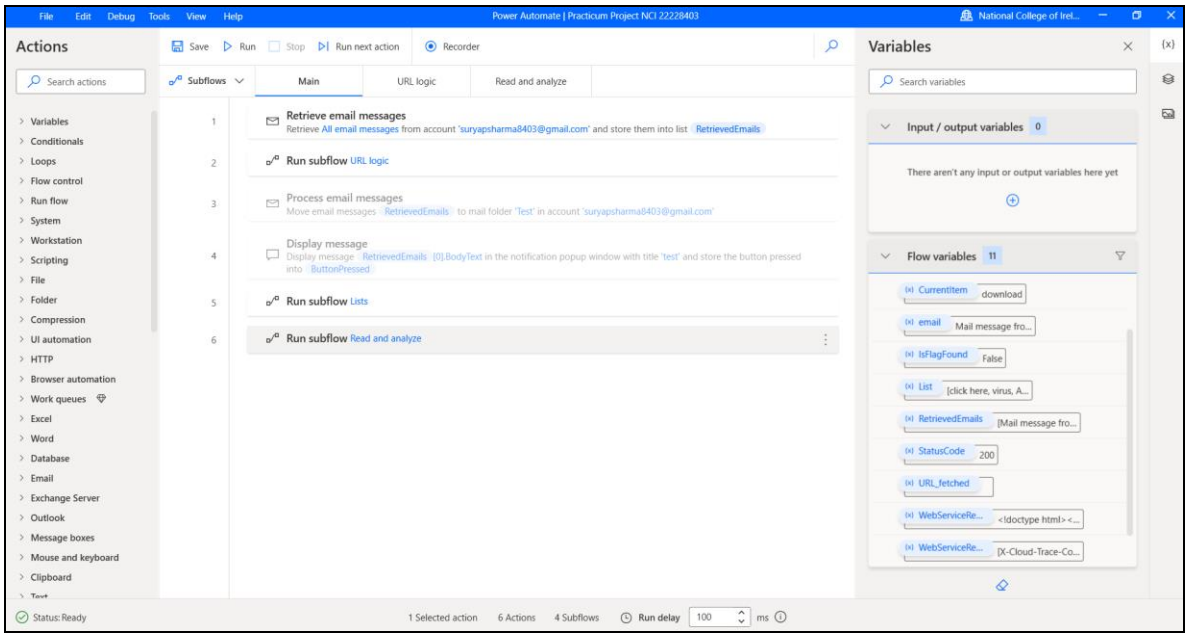

Figure 5. RPA tool GUI

The flows (Main, URL logic, Read and analyze) are visible on taskbar above, users can create sub flows that decrease the complexity of the main flow as in programming by using the MVC (Model, View, Controller) structure. All the variables generated or stored can be viewed on the right pannel, The tool design makes it easy for developers to validate their outcomes instantly. Actions in RPA tool are on the left panel, which make an RPA flow, when placed in a logical order.

5 Implementation

5.1 Environment setup

The RPA tool used was Microsoft's Power Automate which is preinstalled on Microsoft Windows operating system. So, to set it up it was logged in with academic user id.
Gmail email server was integrated to tool after generating an app password for google account

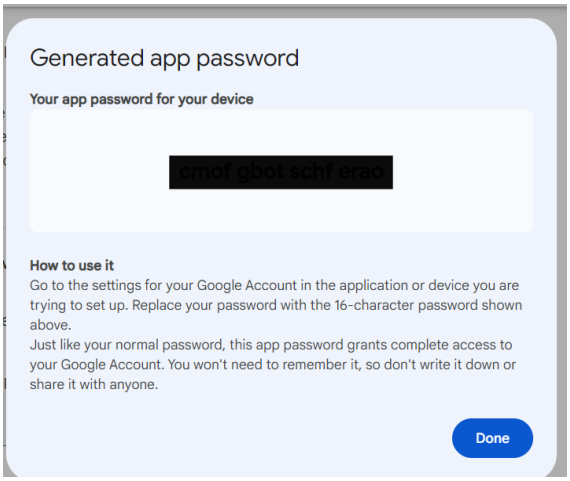

Figure 6. App password generation.

Phishing templates for GoPhish along with normal mails were sent to the target email. On Gmail server a separate label/folder named suspicious mails was created to transfer high severity mails into it as shown in figure 2.

5.2 Phishing detection logic

The following rule-based logic was implemented on Power Automate:

1. Start action is called to retrieve mails.
2. Most common malicious words referenced from the studies of Wong (2021) and Irwin (2023) were stored in a list variable:

Table 3. Malicious words of email.

List of few popular malicious words:
Urgent
Request
Payment
Attention
Action
Document
eFax
VM
Verification
Compromised

3. A “For each” loop is called that loops each retrieved email.
4. Email content is mapped with malicious words stored in list variable inside loop.
5. Detected links in email content are sent to Virus Total API.
6. URL score by Virus Total is detected in API response.
7. IF score is 1 OR greater than 1 OR more than one malicious word gets mapped from the list, the mail gets flag of high severity.
8. Power Automate moves mails with high severity into suspicious mail folder (Figure. 7) on Gmail server.

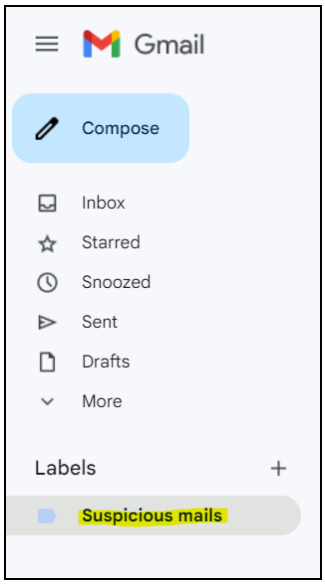

Figure 7. Suspicous mail label

6 Evaluation

After designing the RPA flow to detect phishing, another sub flow was created to show the number of high severity emails moved to the suspicious emails folder, “Suspicious mails”. So that the users can observe the result from Power Automate’s GUI. This result will be displayed at the end of every run.

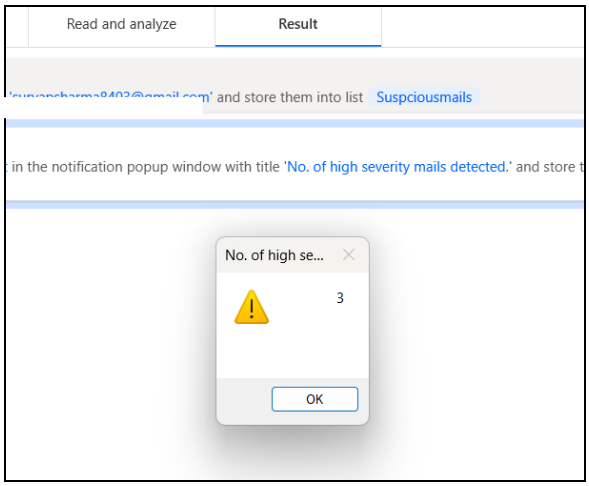

Figure 8. Result display

Figure 8 shows the number of high severity mails detected by Power Automate was 3 and those mails were moved into a different folder in Gmail mail server. This result was displayed by fetching the variable; “. Count” from retrieved mails. Getting a valid count value proves that the RPA flow worked as expected.

Emails that were not malicious are true negatives, emails with malicious content are true positives and the mails that were not malicious but still flagged are false positive. The metrics to quantify the results are as follows:

- Accuracy
- Time Taken
- Memory consumption

Here, Accuracy = (True Positives + True Negatives) / Total emails
= (3 + 12) / 16
= 0.9375

Time taken was calculated by dividing the total time taken to run the RPA flow divided by total number of mails.

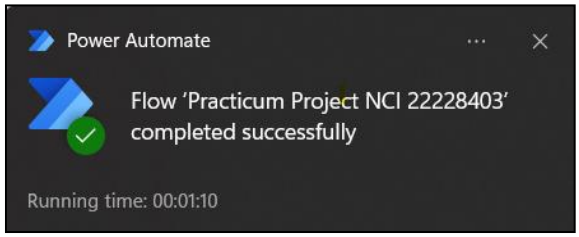

Figure 9. Total Running time

Memory consumption (RAM) of tool was taken into account from window Task manager when the flow was in running state.

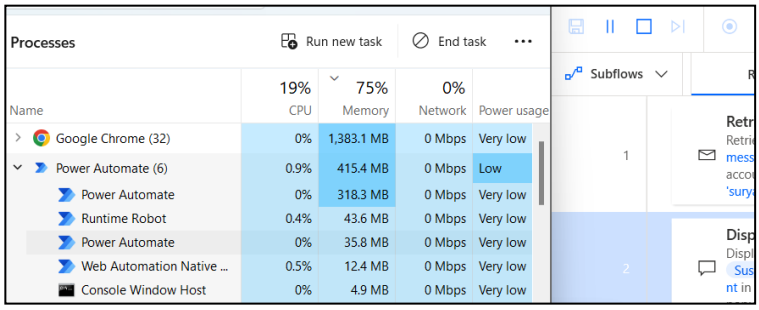

Figure 10. Memory consumption

Using such metrics is important after implementing any solution that provides a validation to project and methods used. In the case of this RPA tool, the results achieved can help to justify the success of tool. Refer the table below:

Table 3. Results table

Accuracy	94%
Time Taken	4.3 seconds per mail.
Memory consumption in run state.	320-450 mb

7 Discussion

The result achieved was satisfactory and something that was expected specially with the amount of data taken, though all the global metrics were not taken into account because of less data. The aim of the experiment was to introduce Robotic Process Automation technology in the field of phishing detection and getting positive results proved that it can be possible though the process can be made more efficient and robust. Many state of the art techniques are available to be used in an RPA flow with premium features like NLP and machine learning which was tried in initial phase of project but due to complexity of script embedding and time taking to decide and design suitable ML algorithm in the restricted time frame it was not possible for me to embark it. The fact, that mail with high severity are going into different folder could be more creative by implementing a logic in flow about informing users "What type of potential danger is in the folder of suspicious mail? For example: malicious link, blackmail etc".

The major strength of the work done and getting valid results was introducing a technology of RPA to cyber security. The limitations of work carried were less data, too few scenarios and also limited consideration of email components while deciding security parameters in rule-based flow. Basit *et al.* (2020) can be used as the basis for future work as the ensembled machine learning classifiers used can leverage the power of a RPA tool to detect phishing in a more precise and user-friendly way, An RPA tool can become the gateway to implement all the strong ideas with novelty to detect phishing in a low code format.

8 Conclusion and Future Work

The research question was "How can potential phishing emails and malicious content in user email inboxes be efficiently detected and reported to users using Robotic Process Automation (RPA) technology?"

The objectives were to implement a logical solution in RPA flow successfully, to show the potential use of this technology in field of phishing detection, the work that was out on Microsoft's RPA tool (leveraging its interactive GUI and strong low code solution ability.) The outcomes received showed that implementing an RPA based solution in cyber security does have potential to increase efficiency in this area. The implication of this research is giving readers the knowledge of applications of RPA in realm of cyber security. The efficacy of the solution was to the point due to the limited amount of data was used in an isolated environment. The limitation of this research was not integrating strong machine learning algorithms and using a big dataset of phishing emails that would have improved the outcomes with existing phishing detection solutions.

Future avenues of research in this technology can focus on implementing machine learning and artificial intelligence solutions on industry data sets integrating with real time threat detection.

They should also leverage community contributions with a feedback loop in an RPA flow. One more thing that can become part of project like this is developing the level of severities with in depth indexing of potential malicious emails and also introducing the element of social engineering through mails. Using RPA tools, users can also leverage multi-platform integration and expand the scope of detecting phishing.

References

Aguirre, S. and Rodriguez, A. (2017) 'Automation of a Business Process Using Robotic Process Automation (RPA): A Case Study', in J.C. Figueroa-García et al. (eds) *Applied Computer Sciences in Engineering*. Cham: Springer International Publishing, pp. 65–71. Available at: https://doi.org/10.1007/978-3-319-66963-2_7.

APWG (2023) 'APWG | Phishing Activity Trends Reports'. Available at: https://apwg.org/trendsreports/ (Accessed: 4 August 2024).

Asquith, A. and Horsman, G. (2019) 'Let the robots do it! – Taking a look at Robotic Process Automation and its potential application in digital forensics', *Forensic Science International: Reports*, 1, p. 100007. Available at: https://doi.org/10.1016/j.fsir.2019.100007.

Atawneh, S. and Aljehani, H. (2023) 'Phishing Email Detection Model Using Deep Learning', *Electronics*, 12(20), p. 4261. Available at: https://doi.org/10.3390/electronics12204261.

Bart Teodorczuk (2022) *UiPath vs. Power Automate — Which RPA Tool To Choose?* Available at: https://flobotics.io/blog/rpa/uipath-vs-powerautomate/ (Accessed: 24 July 2024).

Basit, A. *et al.* (2020) 'A Novel Ensemble Machine Learning Method to Detect Phishing Attack', in. Available at: https://doi.org/10.1109/INMIC50486.2020.9318210.

Caleb Riggs (2022) *GitHub - criggs626/PhishingTemplates: This is a collection of phishing templates and a landing page to be used with goPhish*. Available at: https://github.com/criggs626/PhishingTemplates/tree/master (Accessed: 17 July 2024).

Catnip Infotech Private Limited (2023) '(20) Streamlining Email Tasks: The Power of RPA in Mail Automation | LinkedIn', *Streamlining Email Tasks: The Power of RPA in Mail Automation | LinkedIn*, 29 June. Available at: https://www.linkedin.com/pulse/streamlining-email-tasks-power-rpa-mail/ (Accessed: 14 February 2024).

CoCo Pierce (2024) *How Robotic Process Automation Can Be a Vanguard Against Cyber Security Threats | Thoughtful*. Available at: https://www.thoughtful.ai/blog/how-robotic-process-automation-can-be-a-vanguard-against-cyber-security-threats (Accessed: 7 August 2024).

Gary Smith (2023) 'Top Phishing Statistics for 2024: Latest Figures and Trends', 6 September. Available at: https://www.stationx.net/phishing-statistics/ (Accessed: 28 July 2024).

Hina, M. *et al.* (2021) 'Email Classification and Forensics Analysis using Machine Learning', in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*. *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*, pp. 630–635. Available at: https://doi.org/10.1109/SWC50871.2021.00093.

Irwin, L. (2023) *51 Must-Know Phishing Statistics for 2023 | IT Governance, IT Governance UK Blog*. Available at: https://www.itgovernance.co.uk/blog/51-must-know-phishing-statistics-for-2023 (Accessed: 6 August 2024).

Kanerika (2023) 'UiPath vs Power Automate: The Ultimate RPA Comparison', *Kanerika*, 29 November. Available at: https://kanerika.com/blogs/uipath-vs-power-automate/ (Accessed: 24 July 2024).

Khababa, G. *et al.* (2023) 'Enhancing Spam Email Classification using Multilayer Perceptron: Performance Analysis and Comparative Evaluation', in *2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*. *2023 5th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, pp. 1–8. Available at: https://doi.org/10.1109/PAIS60821.2023.10322017.

Lallie, H.S. *et al.* (2021) ‘Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic’, *Computers & Security*, 105, p. 102248. Available at: https://doi.org/10.1016/j.cose.2021.102248.

Mishra, A., Mishra, S. and Kumar, N.S. (2022) ‘Data Analysis using Robot Process Automation Study on Web Scraping using UI Path Studio’, in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*. *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 2221–2225. Available at: https://doi.org/10.1109/ICAC3N56670.2022.10074502.

Pitchkites, M. (2021) *Email Security: A Guide to Keeping Your Inbox Safe in 2024*, *Cloudwards*. Available at: https://www.cloudwards.net/email-security/ (Accessed: 14 February 2024).

Porch Group (2024) ‘100 Compelling Email Statistics for 2024 | Porch Group Media’, 5 March. Available at: https://porchgroupmedia.com/blog/100-compelling-email-statistics-to-inform-your-strategy-in-2023/ (Accessed: 7 August 2024).

Scott, J. (2022) *Phishing ecosystem : A Qualitative Analysis of Phishing Susceptibility in Employees Who Work from Home*. Available at: https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-22262 (Accessed: 4 August 2024).

Stadlinger, J. and Dewald, A. (2017) ‘A Forensic Email Analysis Tool Using Dynamic Visualization’, *Journal of Digital Forensics, Security and Law*, 12(1). Available at: https://doi.org/10.15394/jdfsl.2017.1413.

Thekkethil, M.S. *et al.* (2021) ‘Robotic Process Automation in Banking and Finance Sector for Loan Processing and Fraud Detection’, in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*. *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–6. Available at: https://doi.org/10.1109/ICRITO51393.2021.9596076.

Tornblad, M.K. *et al.* (2021) ‘Characteristics that Predict Phishing Susceptibility: A Review’, *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 65(1), pp. 938–942. Available at: https://doi.org/10.1177/1071181321651330.

Wong, R.P., Simon (2021) *The top phishing keywords in the last 10k+ malicious emails we investigated*, *Expel*. Available at: https://expel.com/blog/top-phishing-keywords/ (Accessed: 6 August 2024).