

Temasek Informatics & IT School

**Diploma In Cyber & Digital Security
Security Technology and Innovation (STI)
[Subject Code – CCD3C01]**

Security Technology and Innovation

Case Study

Final Report Template

Security Technology and Innovation (CCD3C01) Report Submission

Practical Class: P02

Submitted by: Group 6

Date: 12 / 08 / 2021

“By submitting this work, we are declaring that we are the originator(s) of this work and that all other original sources used in this work has been appropriately acknowledged.

We understand that plagiarism is the act of taking and using the whole or any part of another person’s work and presenting it as our own without proper acknowledgement.

We also understand that plagiarism is an academic offence, and that disciplinary action will be taken for plagiarism.”

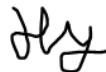
Name and Signature of student: Muhammad Aniq Syukri Bin Md Azhar



Name and Signature of student: Muhammad Mikail Bin Jasman



Name and Signature of student: So Hong Yao



Name and Signature of student: Zachary Phoon Jun Ze

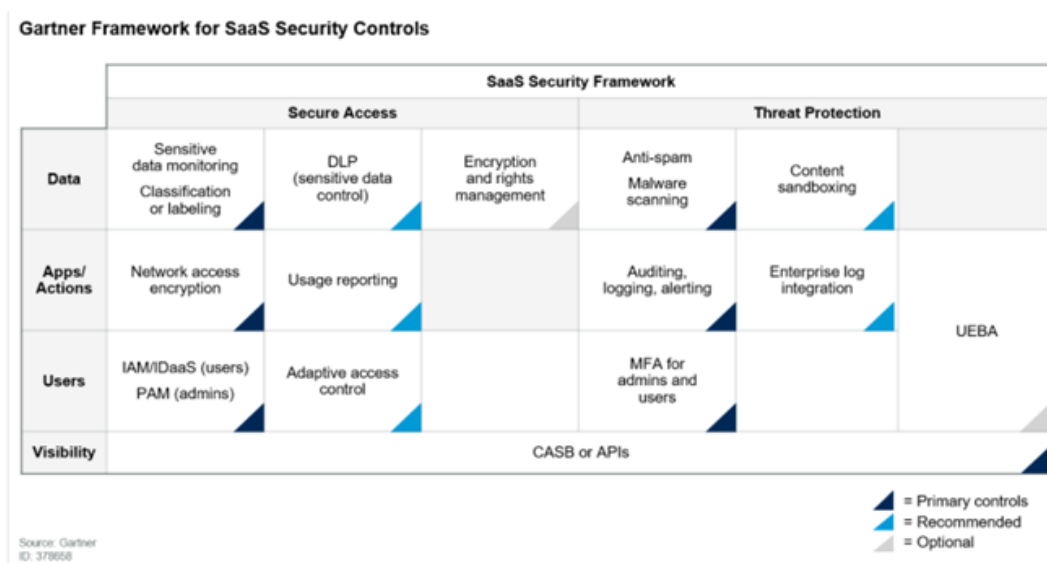


| | |
|--|-------------------------------------|
| Temasek Informatics & IT School | 1 |
| 1. Introduction | 2 |
| 2. Roles & Responsibilities | 3 |
| 3. Diagrams | Error! Bookmark not defined. |
| 3.1 Use Cases Diagram | 4 |
| 3.1.1 Google Chrome Extension & GUI Version Use Case Diagram | 4 |
| 3.1.2 Telegram Bot Version Use Case Diagram | 5 |
| 3.2 Use Case Explanation | 6 |
| 3.2.1 Use Case 1 (Google Chrome Extension) | 6 |
| 3.2.2 Use Case 2 (Koi Scanner Telegram Bot) | 6 |
| 3.2.3 Use Case 3 (Email Scanner) | 6 |
| 3.2.4 Use Case 4 (URL Scanner) | 6 |
| 3.2.5 Use Case 5 (KoiScanner Tkinter UI) | 6 |
| 3.2.6 Use Case 6 (Machine Learning) | 6 |
| 3.3 Data Classification Diagram | 7 |
| 3.4 Data Flow Diagram | 9 |
| 4. Outstanding Issues | 10 |
| 4.1 Outstanding Issues/Functions | 10 |
| 4.2 Future Enhancements | 10 |
| 5. Commercial Feasibility | 12 |
| 6. Conclusion | 13 |
| Sharing By Zachary Phoon | 13 |
| Sharing By Hong Yao | 13 |
| Sharing By Mikail | 13 |
| Sharing By Aniq Syukri | 14 |
| 7. Meeting Minutes | 15 |

1. Introduction

Phishing Emails has been one of the most popular attack vectors for cyber criminals. The emails sent may contain malicious links that once clicked will lead to a website that will steal login credentials or financial information of users.

KoiScanner is a protective aid product which allows users to scan their emails for malicious URLs. This scan can be regularly set by users or on demand via Google Chrome extension, Executable UI or via instant messaging software, Telegram. This will help separate the malicious emails (including malicious urls that are caught and blacklisted) from your regular inbox. KoiScanner provides malware and malicious links scanning and logging by using Machine Learning codes and APIs. Thus, it will provide the security and defense aspects and addresses most of the requirements of the Gartner security framework.



To solve this issue, our proposed solution is to create a google extension that will scan emails for malicious urls. Our project will scan emails on a regular basis or on demand if the user chooses to do so. By implementing our project it helps the user to prevent any loss of data by ensuring that any malicious urls are caught and blacklisted.

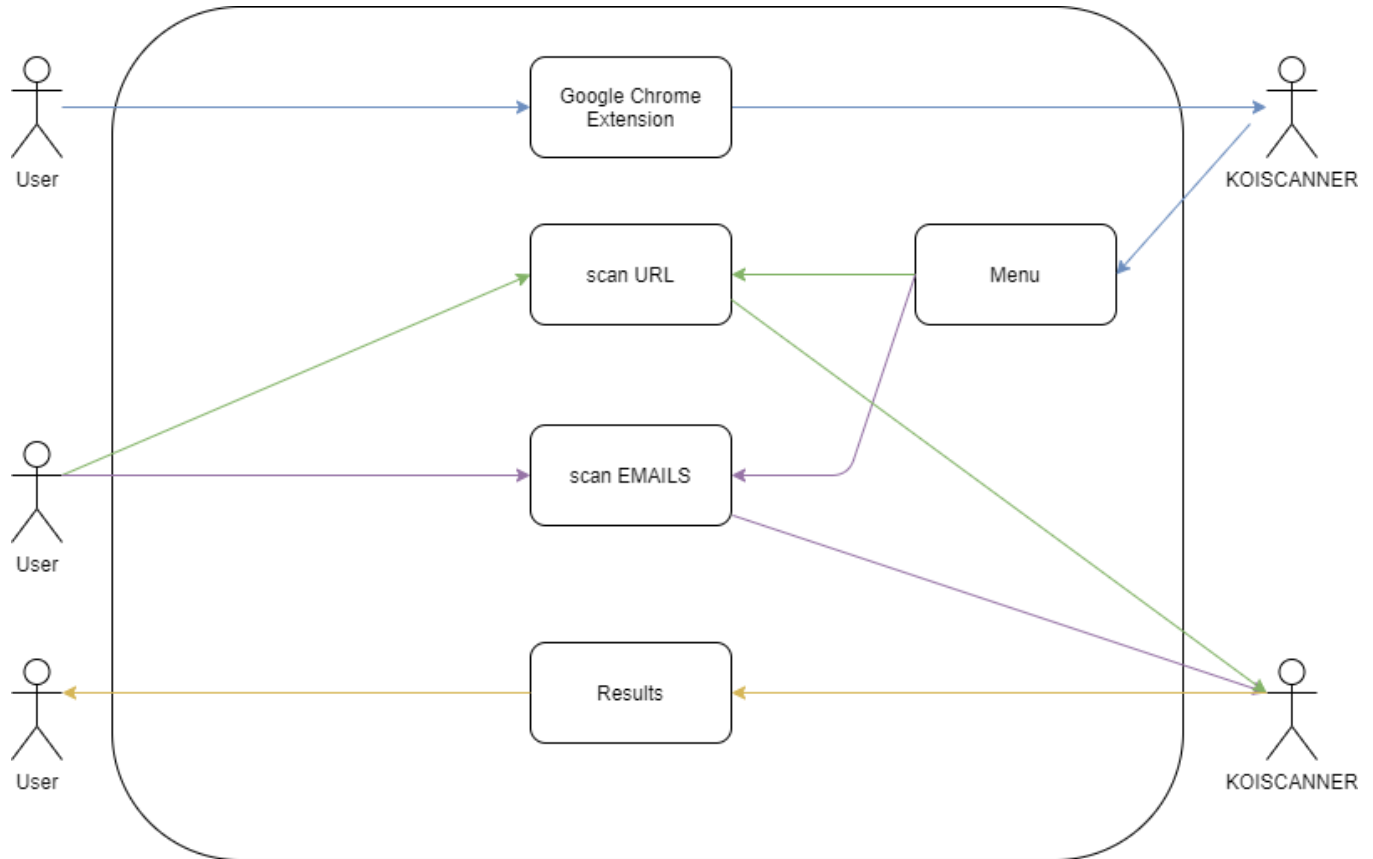
2. Roles & Responsibilities

| | |
|--------------------------------------|--|
| Zachary Phoon (Team lead) | Developer of Google Chrome Extension, Koi Scanner Telegram Bot, Email Scanner Result, URL Scanner, KoiScanner GUI Final Integrator & Tester |
| Hong Yao | Researcher of Email Scanning Developer of Use Case Email Scanner Tester of Use Case Email Scanner |
| Mikail | Researcher of Machine Learning. Developer of Machine Learning. Tester of Machine Learning Accuracy. |
| Syukri | Researcher of Machine Learning. Developer of Machine Learning. Tester of Machine Learning, Integration to the Email Scanner. |

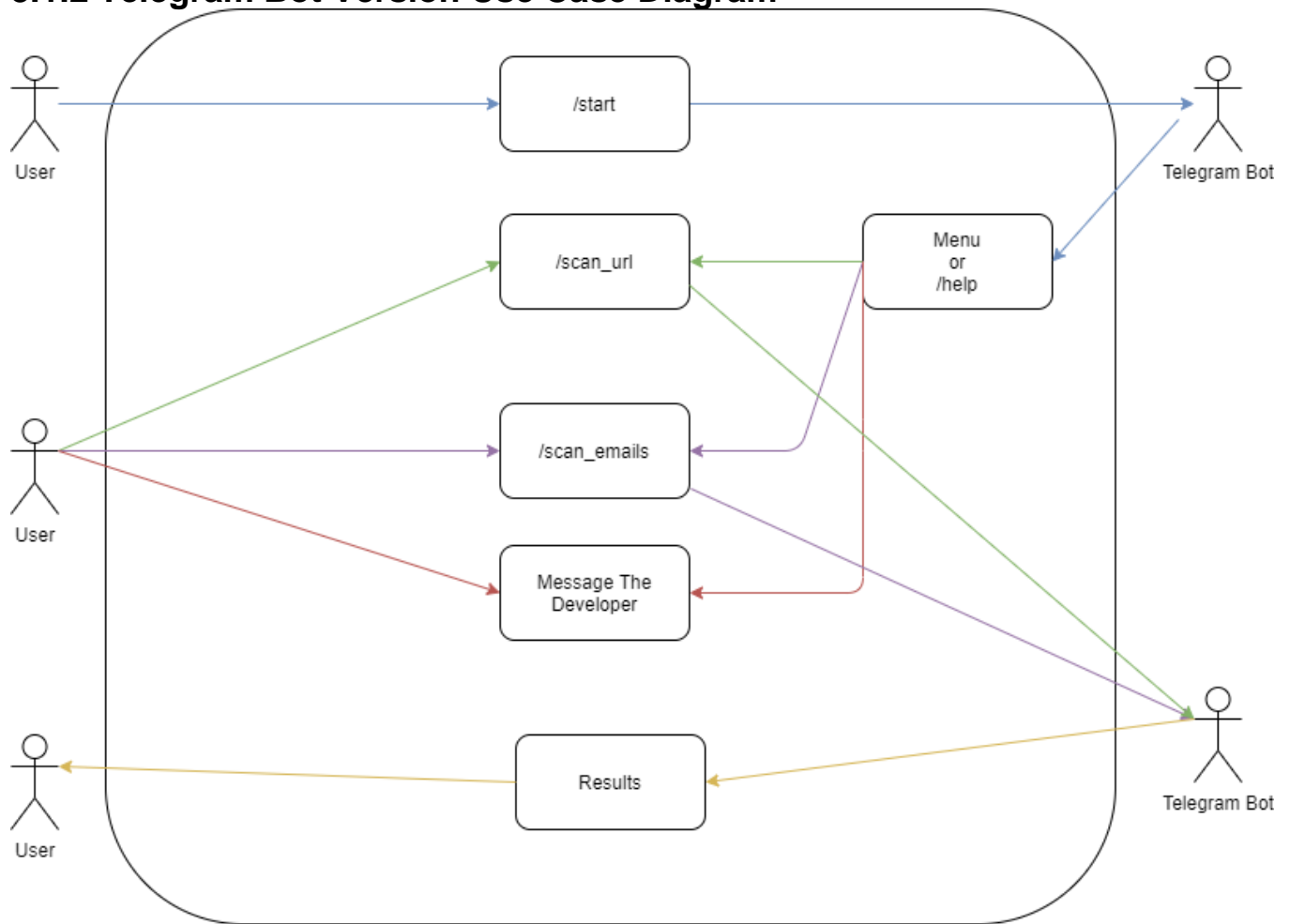
3. Diagrams

3.1 Use Cases Diagram

3.1.1 Google Chrome Extension & GUI Version Use Case Diagram



3.1.2 Telegram Bot Version Use Case Diagram



3.2 Use Case Explanation

3.2.1 Use Case 1 (Google Chrome Extension)

Google Chrome Extension to make it easier for users to use KoiScanner if they do not want to use the GUI version.

This will also give them easy access to the program without any hassle of installing the GUI executable version.

3.2.2 Use Case 2 (Koi Scanner Telegram Bot)

The Telegram Bot Is an alternative to the google extension where it is more convenient for users as it can be a click away from their smartphones. It uses the Telegram API, where it registers commands that have been preset to allow user to run the function as specified in the menu. It has two main functions like the normal KoiScanner, scanning of email for phishing links and a url scanner to detect if it is malicious or not.

This allows users to use the function on the go and if they do not trust this website, they can copy the link and do simple checks to ease their mind.

3.2.3 Use Case 3 (Email Scanner)

Uses Google IMAP to scan all the emails in Gmail. It scans the mail to find any links in the mail or the different sections of the email. They will then check this against a csv file that contains the predictions acquired by existing datasets from PhishTank and custom predictions by machine learning. Once it determines if there is anything related to a malicious link, it will then mark it as read and place it under the category of malicious. Furthermore, it uses the VirusTotal API to double confirm if the link found is indeed malicious before moving it to the malicious folder. Lastly, it uses the Cloudmersive API and IPQualityScore API to check and log the sender's IP address information, whether the attachments in the email are malicious and the malicious domain's information.

3.2.4 Use Case 4 (URL Scanner)

Similar to Email Scanner, this requires users to input a URL. With this input, it will check against existing csv datasets as well as the machine learning dataset to determine if it is malicious or not. Once it is determined as malicious it will return a pop-up to inform the user if the URL is malicious or not.

3.2.5 Use Case 5 (KoiScanner Tkinter UI)

GUI based software to display its potential. To display it for the user to understand easily.

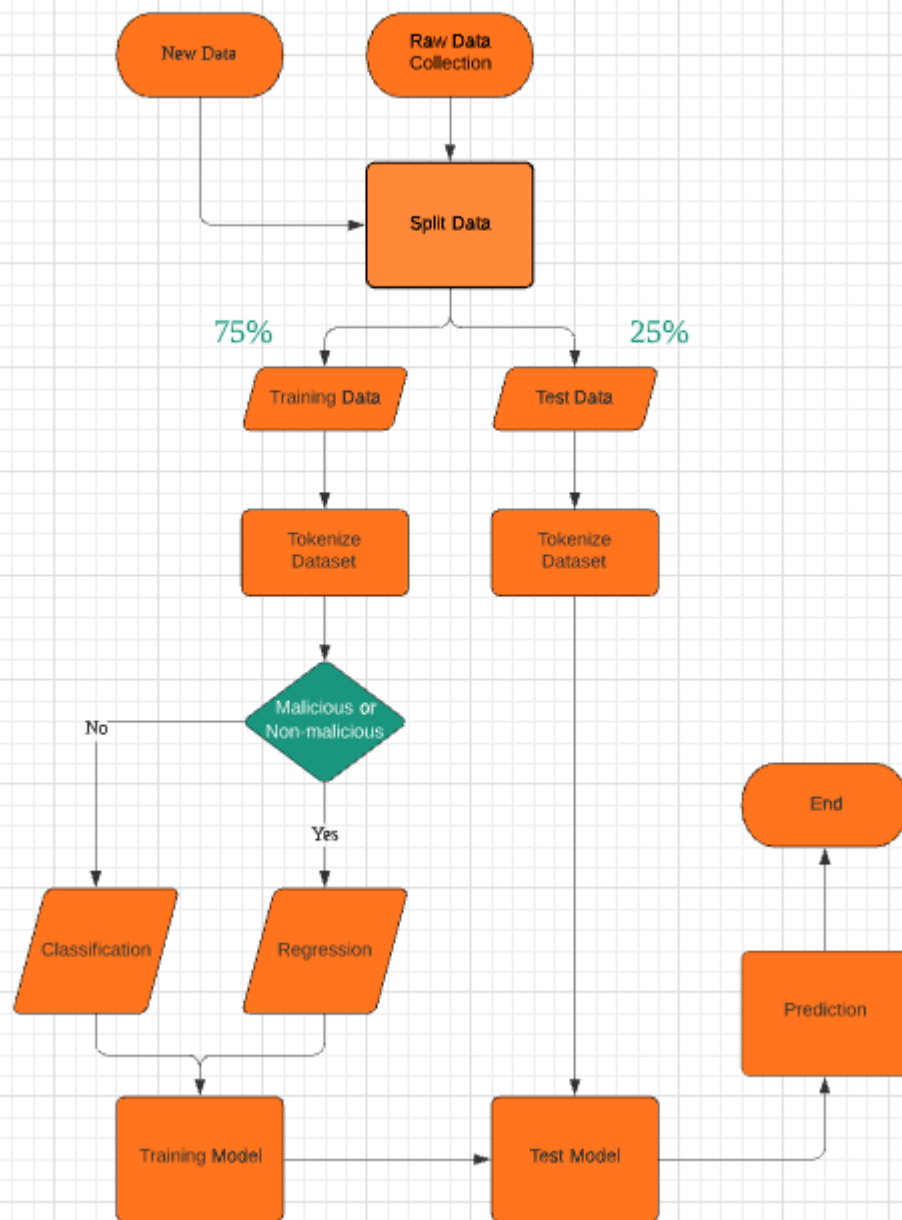
3.2.6 Use Case 6 (Machine Learning)

Machine learning is to identify the malicious URLs that are found within the Email that is sent by an attacker. There is a .csv file that contains malicious and non-malicious URL links that will be used to cross reference with the Email that will be scanned in the Gmail Inbox. Additionally, the model stores new datasets and URL links that may be new into the .csv file to keep the scanning and accuracy close to 100%.

3.3 Data Classification Diagram

Machine Learning for Email Scanner Data Classification

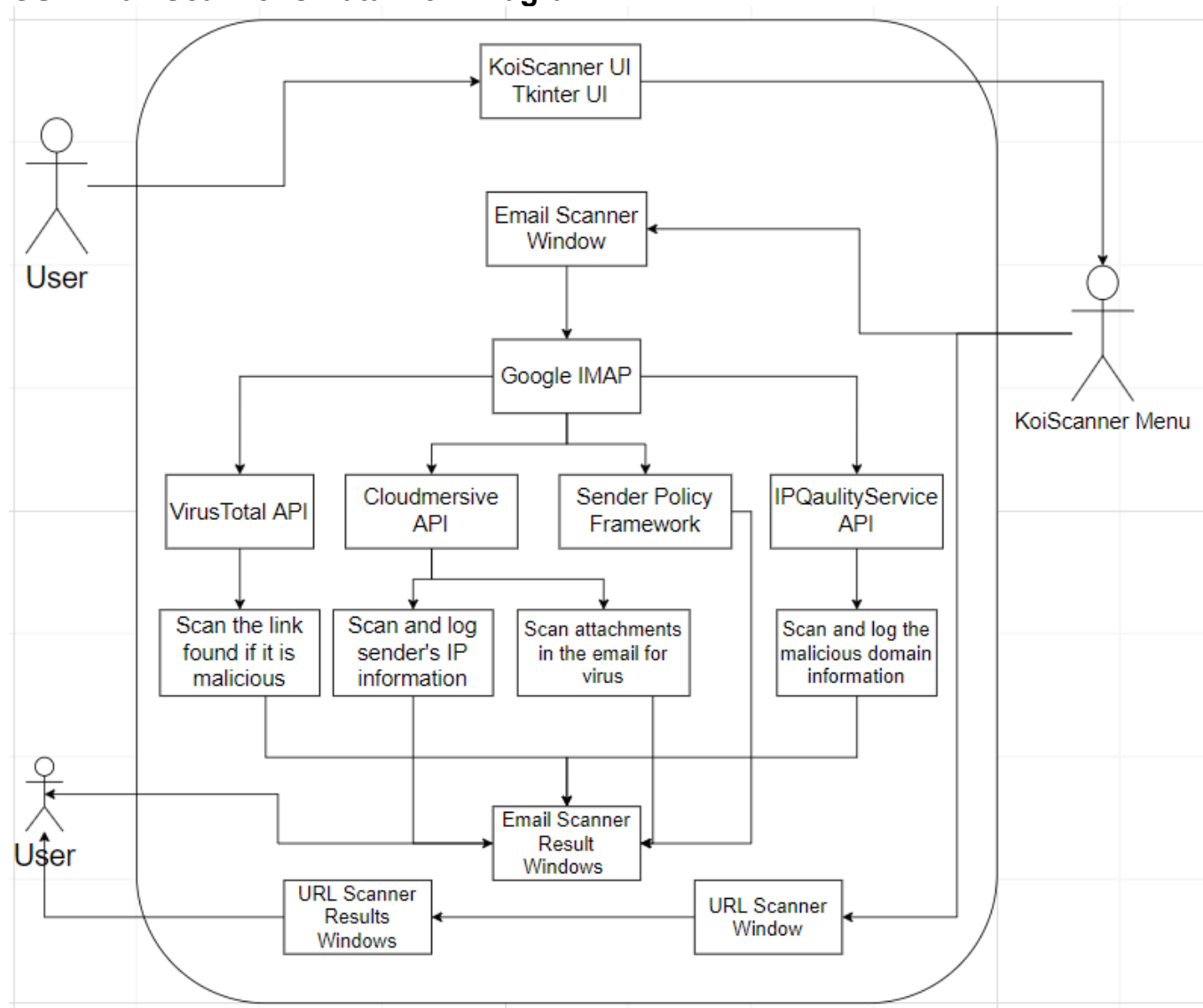
Anig Syukri | August 19, 2021



| Public (Data that may be freely disclosed to the public) | Internal Only (Not meant for public disclosure) | Confidential (Sensitive data that if compromised would affect the operations) | Restricted (Highly sensitive data that could put the organization at risk) |
|---|--|--|---|
| Pricing lists | Machine learning codes, email scanner with APIs codes, Telegram codes | Output of the email scan logs | For subscription: Credit card information Email Scanner: User's email and password |

3.4 Data Flow Diagram

GUI Email Scanner's Data Flow Diagram:



4. Outstanding Issues

4.1 Outstanding Issues/Functions

| OutStanding Issues | Description | Solution |
|-------------------------|---|--|
| Machine Learning | The code for the Machine Learning contradicts the code for the Email Scanner and due to time constraints, it has not been fully implemented yet. | Require more time to code this product out. |
| Google Chrome Extension | Google doesn't allow third party scripts, which doesn't allow us to use different modules to connect to certain IMAP functions. So this requires a longer period of time to accomplish. | Uploading the codes to a cloud based Server. This allows us to reduce time to code and allow us to simply call the functions off the server. |

4.2 Future Enhancements

| Future Enhancements | Description |
|--|---|
| Securing Telegram Bot to a full service. | It is currently running on TLS(Transport Layer Security) to make it more secure by using Telegram End to End Encryption.This requires us to ensure 100% encryption between users and Bot. As long as the API Credentials do not get leaked. |
| Allow users to login to their own Email for Email Scanner | Currently it all pre-set the credentials to check against this one Email Account. |
| Implementing a better connection between Machine Learning and the Email Scanner. | As the email scanner is relying on a API called "VirusTotal" and part of the email scanner is using Machine Learning to detect and collect data of the phishing emails, Therefore, it requires us to do more research on how the Machine Learning can be part of the Email scanner so that the application will be independent. |
| KoiScanner Mobile Application | Makes access to these functions at the user's fingertips. As smartphones are most of our everyday carry. |
| Email scanner dashboard | Gives the user an overview of the scan |

| | |
|--|---|
| | results and summary. Furthermore, users can monitor and gain insight on the type of email sent to them. |
| Email URL sandbox | If the user wants to click and check the malicious link, they would be ensured with protection as the URL will be running on a sandbox and will not penetrate their system. |
| Email scanning percentage progress bar | <p>Currently, the email scanner runs in the background after the user has clicked on 'Scan emails' or 'Scan URLs'. Users may not know how long the run will take.</p> <p>Therefore, having a percentage progress bar will allow the user to see how much longer is the email scanner going to take and have a gauge on the process.</p> |
| Save the attachments found to a cloud service like Google's cloud during scanning. | Currently, when the email scanner scanned and found an attachment, it will save to the desktop. Thus, using and save on a cloud service would be ideal to get and scan the file instead on the host laptop. |

5. Commercial Feasibility

In today's day and age, Phishing Emails that contain malicious urls and malicious urls on the Internet are rapidly increasing. Many users would want to be able to protect themselves against such attack vectors. Therefore, our product would give them the tool to protect themselves since there is a demand for such a service.

Since more than 2.65 billion internet users use Google Chrome, by making our product a Google Chrome Extension, we can make our product commercially feasible and easily accessed by users. Also by making our product available on different platforms such as Telegram and also a GUI Based version, it will give the users multiple options to make use of our products therefore generating more traffic for users to use our product. To make our product commercially feasible we can have a monthly subscription model for our services.

Monthly Subscription Model:

Basic Plan (Free)

- With the basic plan, users have free access to our services but only limited to the GUI Based Version. They would also have a limitation of 5 scans per day.

Premium Plan (\$20/month)

- With the premium plan, users will have unlimited scans on any urls or emails of their choosing. They are able to use our product on different platforms such as Google Chrome and Telegram. They are able to set the product to scan emails on a regular basis.

With this Subscription Model, it will help us to keep our services running for customers' use.

6. Conclusion

Sharing By Zachary Phoon

KoiScanner was really a wonderful project to work on. It taught me to learn more about how machine learning works from using existing data to code an interpretation to determine its prediction. As well as how a regular instant messaging application can even be used to run applications that can help us to make it more convenient for users as these are existing applications on their phones already. However functions on third-party applications will serve as a possible security risk hence function can be limited. To counter these security issues it is best to create our own application. This project really makes me think of things we use everyday and finding that small possibility to make our browsing and use of the World Wide Web safer day by day. One thing I wished I had done better is to actually implement all these projects and take user feedback and see how we can improve it and what other features they would love to see used.

Sharing By Hong Yao

The project has taught me to use the Problem Based Learning process method and the FILA chart to carry out the project through using the FILA chart to identify the problems with facts and generate ideas based on the facts found. Furthermore, what learning points can be derived and how to implement the ideas step by step. In addition, I learnt how to utilise and import the APIs like VirusTotal, Cloudmersive and IPQualityService to the email scanners that can help to improve the email scanner to scan for malicious links and domains. Moreover, I learnt to code the email scanner using Google's IMAP to try the email scanner on Gmail and how the codes and APIs found help to meet the Gartner's SaaS security policy framework. Lastly, I learnt how to use the PBL method to analyse and carry out the stages to execute the project better.

Sharing By Mikail

During the duration of this project I have gained new knowledge on Machine Learning. I coded out a machine learning model to determine if a url is malicious or not malicious. However, during the coding process there were some codes that were new to me and I had to do research to understand them. The most important lesson that I learnt when doing this project is that I should never give up or feel too discouraged when I am faced with a problem. Instead I try to use these feelings to motivate me further to find a solution to the problem. With the knowledge gained during the whole duration of the project, it has helped me to be more prepared to go into the industry after my studies.

Sharing By Aniq Syukri

The project KoiScanner is a great project to work with as it has expanded my knowledge about Machine Learning and how it will predict answers and results. I partially coded the integration of the Machine Learning codes and the email scanner codes. It really takes a huge amount of time to do it as I have to consider the variables that the Machine Learning will predict based on the type of URL that it is scanning. Additionally, I have been researching a lot on python and flask codes to help out with the Machine Learning codes and understand better about Machine Learning. It was a stressful and mind consuming project but I have learnt about time management is really a key factor to learn, understand and apply a new skill and knowledge. Overall, with the new knowledge gained, it will be a useful tool to have when working in the industry.

7. Meeting Minutes

Meeting Minutes for Security Technology and Innovation (2021)

| | | | |
|----------------------|----------------------|---------------------------|---------------|
| Chairperson: | Muhammad Mikail | Recorded by: | Zachary Phoon |
| Meeting Date: | 1st July 2021 | Time: | 2:10pm |
| Location: | Work From Home (WFH) | Distribution Date: | 1st July 2021 |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|-----------------|---|----------|---|---------------|
| C | Muhammad Mikail | X | Hong Yao | M | Zachary Phoon |
| X | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|-------------------------|
| 1. | Project Planning |
| 2. | Fila Chart |
| 3. | Used Case Diagram |
| 4. | Next meeting/Follow ups |

Discussion

| | | |
|----------|--|---------------|
| 1 | Review of Previous Action Items | Action |
| 1.1 | Putting down ideas into concrete project proposal for KoiScanner | Information |

| | | |
|----------|--|---------------|
| 2 | Discussion on team member write-up of project ideas | Action |
| 2.1 | Project Planning | All |
| 2.2 | Fila Chart | All |

| | | |
|----------|--|--------------------|
| 3 | Next meeting/Follow ups | Action |
| 3.1 | A meeting to be held on 7th July 2021. If deemed necessary, the next meeting will be changed. | Information |
| 3.2 | FILA Draft & Project Plan Submission | Information |
| 3.3 | Research on Machine Learning. | Mikail & Syukri |
| 3.4 | Research on Email Scanner. | Hong Yao & Zachary |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|---------------------------|---------------------------|-------------|
| Chairperson: | Muhammad Mikail | Recorded by: | Aniq Syukri |
| Meeting Date: | 14 July 2021 | Time: | 2:43 PM |
| Location: | Home Based Learning (HBL) | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|-----------------|---|----------|---|---------------|
| C | Muhammad Mikail | X | Hong Yao | X | Zachary Phoon |
| M | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|-------------------|
| 1. | Project Planning |
| 2. | Research |
| 3. | Next Meeting Date |

Discussion

| 1 | Review of Previous Action Items | Action |
|-----|---------------------------------|-------------|
| 1.1 | Completed Used Case Diagram | Information |

| 2 | Discussion on team member write-up of project ideas | Action |
|-----|---|--------|
| 2.1 | Use Adobe XD to make a prototype due to the lack of time to code the Machine Learning feature | All |
| 2.2 | Research on Machine Learning. | All |
| 2.3 | Research on Email Scanner. | All |

| 3 | Next meeting/Follow ups | Action |
|-----|--|-------------|
| 3.1 | Research on AI/ML codes on the features of the Email scanner | Information |
| 3.2 | Prototype design/codes of the email scanner | Information |
| 3.3 | Next Meeting Date 19 July 2021 2PM | Information |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|-----------------|---------------------------|-------------|
| Chairperson: | Muhammad Mikail | Recorded by: | Aniq Syukri |
| Meeting Date: | 19 July 2021 | Time: | 2 Pm |
| Location: | HBL | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|-----------------|---|----------|---|---------------|
| C | Muhammad Mikail | X | Hong Yao | X | Zachary Phoon |
| M | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|--|
| 1 | Research on AI/ML codes on the features of the Email scanner |
| 2 | Prototype design/codes of the email scanner |

Discussion

| 1 | Review of Previous Action Items | Action |
|-----|--------------------------------------|-------------|
| 1.1 | Creation and Review of Email Scanner | Information |
| 1.2 | Creation of URL Scanner | Information |
| 1.3 | Machine Learning Implementation | Information |

| 2 | Discussion on team member write-up of project ideas | Action |
|-----|---|-------------------------------|
| 2.1 | Creation and Review of Email Scanner | Hong Yao |
| 2.2 | Creation of URL Scanner | Zachary Phoon |
| 2.3 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |

| 3 | Next meeting/Follow ups | Action |
|-----|--------------------------------------|-------------|
| 3.1 | Creation and Review of Email Scanner | Information |
| 3.2 | Creation of URL Scanner | Information |
| 3.3 | Machine Learning Implementation | Information |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|-----------------|---------------------------|----------|
| Chairperson: | Muhammad Mikail | Recorded by: | Hong Yao |
| Meeting Date: | 21 July 2021 | Time: | 2pm |
| Location: | HBL | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|-----------------|---|-------------|---|---------------|
| C | Muhammad Mikail | X | Aniq Syukri | X | Zachary Phoon |
| M | Hong Yao | | | | |

Agenda

| No | Topic |
|----|--------------------------------------|
| 1 | Creation and Review of Email Scanner |
| 2 | Creation of URL Scanner |
| 3 | Machine Learning Implementation |

Discussion

| 1 | Review of Previous Action Items | Action |
|-----|--------------------------------------|-------------|
| 1.1 | Creation and Review of Email Scanner | Information |
| 1.2 | Creation of URL Scanner | Information |
| 1.3 | Machine Learning Implementation | |

| 2 | Discussion on team member write-up of project ideas | Action |
|-----|--|-------------------------------|
| 2.1 | Google Chrome Extension Progress and make a decision | All |
| 2.2 | Telegram Bot | Zac |
| 2.3 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |
| 2.4 | PowerPoint slides for Interim Presentation | Zac |

| 3 | Next meeting/Follow ups | Action |
|-----|---------------------------------|-------------------------------|
| 3.1 | UX UI Design Ideas and Progress | Information |
| 3.2 | Telegram Bot | Zac |
| 3.3 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |
| 3.4 | Presentation For Interim Report | All |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|-----------------|---------------------------|---------------|
| Chairperson: | Muhammad Mikail | Recorded by: | Zachary Phoon |
| Meeting Date: | 4 August 2021 | Time: | 2pm |
| Location: | HBL | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|-----------------|---|----------|---|---------------|
| C | Muhammad Mikail | X | Hong Yao | X | Zachary Phoon |
| M | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|---------------------------------|
| 1 | UX UI Design Ideas and Progress |
| 2 | Telegram Bot |
| 3 | Machine Learning Implementation |
| 4 | Presentation For Interim Report |

Discussion

| 1 | Review of Previous Action Items | Action |
|-----|---------------------------------|-------------------------------|
| 1.1 | UX UI Design Ideas and Progress | Information |
| 1.2 | Telegram Bot | Zac |
| 1.3 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |

| 2 | Discussion on team member write-up of project ideas | Action |
|-----|--|-------------|
| 2.1 | Machine Learning Implementation Failure and Research | All |
| 2.2 | Telegram Bot | Zac |
| 2.3 | UX UI Design Ideas and Progress | Information |

| 3 | Next meeting/Follow ups | Action |
|-----|-----------------------------------|-------------------------------|
| 3.1 | A meeting to be set up next week. | Information |
| 3.2 | Telegram Bot ML implementation | Zac |
| 3.3 | Begin Report Progress | ALII |
| 3.4 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|----------------|---------------------------|-------------|
| Chairperson: | Zachary Phoon | Recorded by: | Aniq Syukri |
| Meeting Date: | 11 August 2021 | Time: | 2PM |
| Location: | HBL | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|---------------|---|----------|---|-----------------|
| C | Zachary Phoon | X | Hong Yao | X | Muhammad Mikail |
| M | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|---------------------------------|
| 1 | Telegram Bot ML implementation |
| 2 | Begin Report Progress |
| 3 | Machine Learning Implementation |

Discussion

| 1 | Review of Previous Action Items | Action |
|-----|---------------------------------|-------------|
| 1.1 | Telegram Bot ML implementation | Information |
| 1.2 | Begin Report Progress | All |
| 1.3 | Machine Learning Implementation | Information |

| 2 | Discussion on team member write-up of project ideas | Action |
|-----|---|-------------------------------|
| 2.1 | UI UX Update and using APIS to log the outputs | Hong Yao |
| 2.2 | Machine Learning Implementation | Muhammad Mikail & Aniq Syukri |
| 2.3 | Telegram Bot ML Implementation | Zac |

| 3 | Next meeting/Follow ups | Action |
|-----|----------------------------------|-------------|
| 3.1 | A meeting to be set up next week | Information |

Meeting Minutes for Security Technology and Innovation(2021)

| | | | |
|----------------------|----------------|---------------------------|-------------|
| Chairperson: | Zachary Phoon | Recorded by: | Aniq Syukri |
| Meeting Date: | 19 August 2021 | Time: | 2pm |
| Location: | HBL | Distribution Date: | |

Distribution and Attendee List:

(C = Chair, M = Minute, X = Present, N = No Show, A = Apologies, Dial-in = D, To Be Updated = U)

| | | | | | |
|---|---------------|---|----------|---|-----------------|
| C | Zachary Phoon | X | Hong Yao | X | Muhammad Mikail |
| M | Aniq Syukri | | | | |

Agenda

| No | Topic |
|----|---------------------------------|
| 1 | Telegram Bot ML implementation |
| 1 | Report Progress |
| 1 | Machine Learning Implementation |

Discussion

| | | |
|----------|--|---------------|
| 1 | Review of Previous Action Items | Action |
| 1.1 | Machine Learning Implementation | Information |
| 1.2 | Telegram Bot ML implementation | Information |
| 1.3 | Report Progress | |

| | | |
|----------|--|---------------|
| 2 | Discussion on team member write-up of project ideas | Action |
| 2.1 | Report | All to note |
| 2.2 | Slides | All to note |
| 2.3 | Telegram Bot | Zachary |

| | | |
|----------|----------------------------------|---------------|
| 3 | Next meeting/Follow ups | Action |
| 3 | 20 August for Final Presentation | ALL |