Progress Evaluation: Milestone 1

Project: *AI-Powered Phishing Email Detector*

Team Members:

Curtis Jones - *cjones2022@my.fit.edu*

Elton Batista - *ebatista2022@my.fit.edu*

Jordan Chesley - *jchesley2022@my.fit.edu*

Faculty Advisor: Khaled Slhoub - *kslhoub@fit.edu*

Client: Khaled Slhoub - *College of Engineering and Science: Department of Electrical Engineering and Computer Science*

Progress of current Milestone (progress matrix)

Task	*Completion*	*Jordan*	*Elton*	*Curtis*	*To do*
Compare and select Technical Tools	*100%*	*Datasets*	*Machine Learning Models*	*LLM Models*	*none*
Detection Demo	*50%*	*Web App*	*AI Model Training*	*AI Model Testing*	*Integrate selected AI model into demo*
Resolve Technical Challenges	*20%*	*Testing Different Data Sets*	*Machine Learning Testing*	*LLM Testing*	*Perform rigorous testing on 3 selected models*

Compare and select Collaboration Tools	*90%*	*Trello setup*	*Discord Setup*	*Github setup* *Jira setup*	*Integrate Jira into team workflow*
Requirement Document	*100%*	*write 33%*	*write 33%*	*write 33%*	*Append as necessary*
Design Document	*100%*	*write 33%*	*write 33%*	*write 33%*	*Append as necessary*
Test Plan	*100%*	*write 33%*	*write 33%*	*write 33%*	*Append as necessary*

-

Task Completion

Task 1: *Compare and select Technical Tools*
Description: Researched applicable datasets to be used in training and testing an AI model. We've chosen several different datasets that are extensively used by cybersecurity researchers. Researched different types of AI models and how they could fit into our requirements by evaluating the specifications of 6 different models. We've selected 3 models, all three of which are deep learning models. Two of the models chosen are Transformer models, which run locally on the client. One model is an LLM, which runs using an API call to the service's main server.
Obstacles: There is a limited availability of phishing email datasets, meaning we have to rely on a small handful of larger datasets when training and testing individual AI models. Should an issue arise in testing, it may be worth reaching out to individual researchers for privately owned datasets.
Task 2: *Detection Demo*
Description: The basic structure for a detection demo has been constructed. This allows users to individually paste emails into a text box in order to return the confidence level of the AI's evaluation of the email.
Obstacles: An AI model has yet to be integrated into the demo, therefore it is not yet functional.
Task 3: *Resolve Technical Challenges*
Description: The three models selected best fit the requirements for the project. By doing rigorous testing on these models, we will be able to judge the tradeoffs between accuracy,

performance, and security.
Obstacles: We will need to test individual models in a browser to determine if there's any degradation in performance compared to running them locally on a computer. If there is a high degradation in performance, we will have to consider either running the model on the server-side or relying solely on the LLM chosen. This will have security implications that would have to be addressed.
Task 4: *Compare and select Collaboration Tools*
Description: Collaboration tools have been set up to allow better communication between project members. This includes a Trello, Discord, and GitHub.
Obstacles: We have decided to incorporate Jira into our workflow. This allows us to meet deadlines more consistently while maintaining better collaboration between members. By using the three documents in this milestone, we will be able to outline a SCRUM framework for future collaboration in this project.
Task 5: *Requirement Document*
Description: Developed requirements using current research and goals for the project. This includes functional and nonfunctional requirements to the system, as well as external systems that will interact with our system in any way. These requirements were extensively documented in order to create a fleshed-out design document and test plan.
Obstacles: Balancing security and performance with functionality in terms of system requirements
Task 6: *Design Document*
Description: The design document follows a microservices architecture to best meet the previously defined requirements. Different services within the design document fulfill different requirements we have documented, as can be seen in the requirements matrix. By following a microservices approach, we allow ourselves to develop each microservice independently to promote low coupling. This helps with our agile development approach moving forward
Obstacles: Implementing design philosophies that follow our strict performance and security requirements. By following the test plan, the appendix may have to be updated with changes to our design approach due to performance or security concerns due to the nature of this project
Task 7: *Test Plan*
Description: We adopted a methodology to best test the performance, accuracy, and security of our system. The tests used for different aspects of our project are outlined in our design document. We also emphasized using all testing in different browsers to best simulate how the user will interact with the system.
Obstacles: API outages may have an impact on testing. We may also have to continue researching different phishing email databases, including creating our own.

Discussion (at least a paragraph) of contribution of each team member to the current Milestone:

- Curtis Jones: Created a research document to outline possible AI models. This document compares the specifications of 6 different models that could be beneficial to the project. By comparing and analyzing these specifications, I've selected 3 models to be used in testing that best fit the scope of the project. Created the SWDD for the project, designing the architecture and framework going forward.

- Elton Batista: Assisted in setting up the team's collaboration tools by creating and organizing the GitHub repository, as well as helping configure Trello and Discord for communication. Began integrating Jira into the project workflow to support a SCRUM framework in future milestones. Researched the feasibility of running the selected AI models in a browser environment and outlined possible performance challenges that will need to be addressed during testing. Created the test document to be used in the project going forward

- Jordan Chesley: Created the Requirements document for the project. Collected datasets to be used in training and testing the artificial intelligence. Researched web tools, including REST and OAuth to add to the requirements documentation. Contributed to the architecture framework in the design document, helping flesh out a microservices architecture.

Plan for the next Milestone (task Matrix)

Task	*Jordan*	*Elton*	*Curtis*
AI model testing	*Format datasets for model testing*	*Create scripts for collecting data (Accuracy and performance)*	*Test three selected models / collect and compare data / select a model for project use*

AI model training	*Select and format datasets for model training*	*Integrate the model into a web browser*	*Train the model and analyze possible degradation in performance over the browser*
Demo	*Integrate the selected model into the demo*	*Research and test approaches to increasing security through the demo*	*Test demo output / use possible adversarial prompts to test security of model*
Research Gmail integration	*Test implementation of Oauth with different email domains*	*Research gmail API tools in relation to project requirements*	*Research possible alternatives to direct gmail API integration*
Jira setup and integration	*Create additional documentation if necessary.*	*Create a backlog of epics and user stories using existing documentation.*	*Construct sprints, assign members, assign deadlines, and set up meetings*

Discussion (at least a paragraph) of each planned task for the next Milestone

- Task 1: *AI model testing*
    - Using the three models we selected, each one will undergo vigorous testing. The data we collect, including measurements of accuracy and performance, will be compared among the models to select the best one for the scope of the project.

- Task 2: *AI model training*
    - The selected model will be trained on different phishing email datasets. For each round of training, it will undergo the same tests to observe possible faults in the model.
- Task 3: *Demo*
    - A small demo will be used to test the model's web integration. With this, we can perform multiple tests on the model, including adversarial prompts that could pose a security risk.
- Task 4: *Research Gmail integration*
    - Members will research Gmail integration into our model. We will determine which features can be implemented using the Gmail API alone. We will also research alternatives to the Gmail API if it is unsatisfactory in accomplishing our goals with this project.
- Task 5: *Jira setup and integration*
    - By using our existing documentation, we plan on integrating Jira into our workflow. This is a better collaboration system than what we are currently using. Jira allows us to better meet deadlines and be more iterative in our project development.

1. Date(s) of meeting(s) with Client during the current milestone:

   9/20

   10/3

2. Client feedback on the current milestone
    - ... (if Client and Faculty Advisor are the same, write "see Faculty Advisor Feedback below")
    - ...
    - ...
3. Date(s) of meeting(s) with Faculty Advisor during the current milestone: ...
4. Faculty Advisor feedback on each task for the current Milestone
    - Task 1: ...
    - Task 2: ...

- Task 3: ...
- Task 4: ...

5. Faculty Advisor Signature: _____ Date: _____
   ------ on a separate page ---------
6. Evaluation by Faculty Advisor
   - Faculty Advisor: detach and return this page to Dr. Chan (HC 209) or email the scores to pkc@cs.fit.edu

○ Score (0-10) for each member: circle a score (or circle two adjacent scores for .25 or write down a real number between 0 and 10)

John Smith	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
Jane Doe	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10
Mark Jones	0	1	2	3	4	5	5.5	6	6.5	7	7.5	8	8.5	9	9.5	10

- Facutly Advisor Signature: _____ Date: _____