

# Sri Lanka Institute of Information Technology

Status Document 02

2024

GROUP ID: R24-102



## **Strengthening Heart Disease Prediction With CNN: Adversarial Robustness Against Multiple Attacks**

Reg No: IT21023514

Name: Karandawala D.N

Batch: Cyber Security

## Table of Contents

1.	Microsoft Teams Calls.....	3
2.	WhatsApp calls and text message communication with the supervisor. ....	6
3.	Email Communications with Supervisors .....	8
4.	Microsoft Planner.....	10
5.	Gantt Chart .....	12
6.	Work Breakdown Structure .....	12
7.	GitLab Commits.....	13

# 1. Microsoft Teams Calls

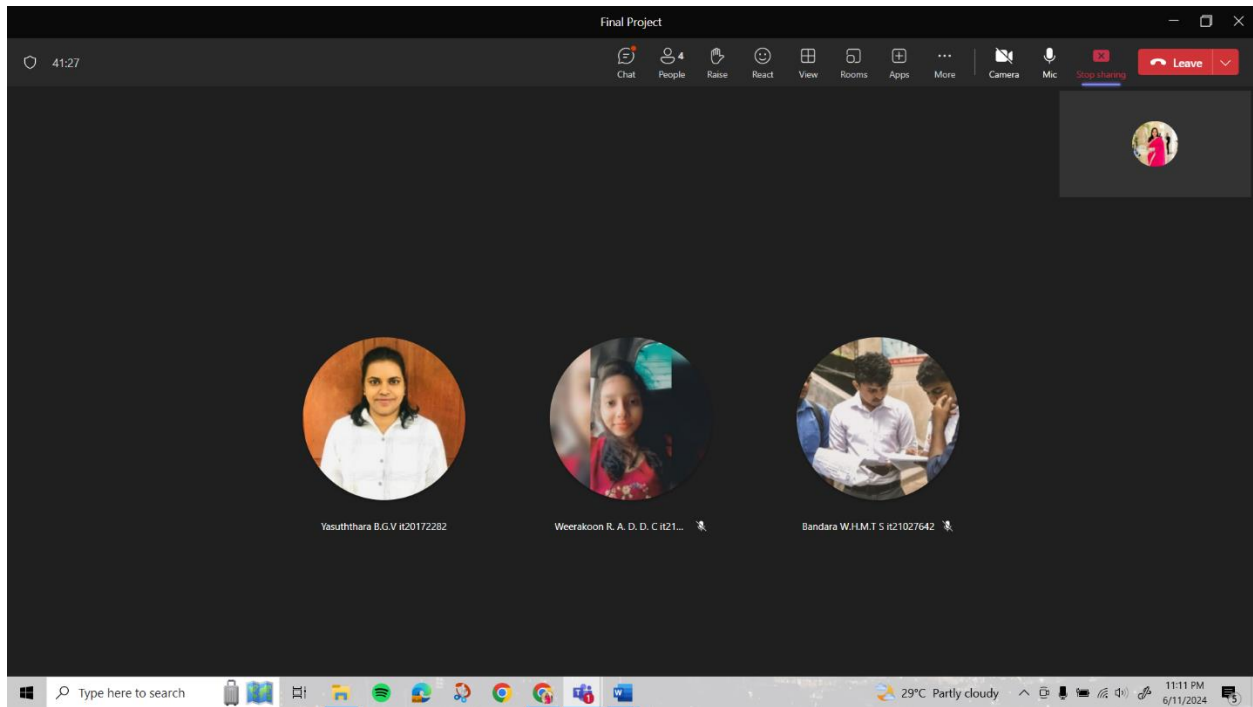


Figure 1: Teams call with team

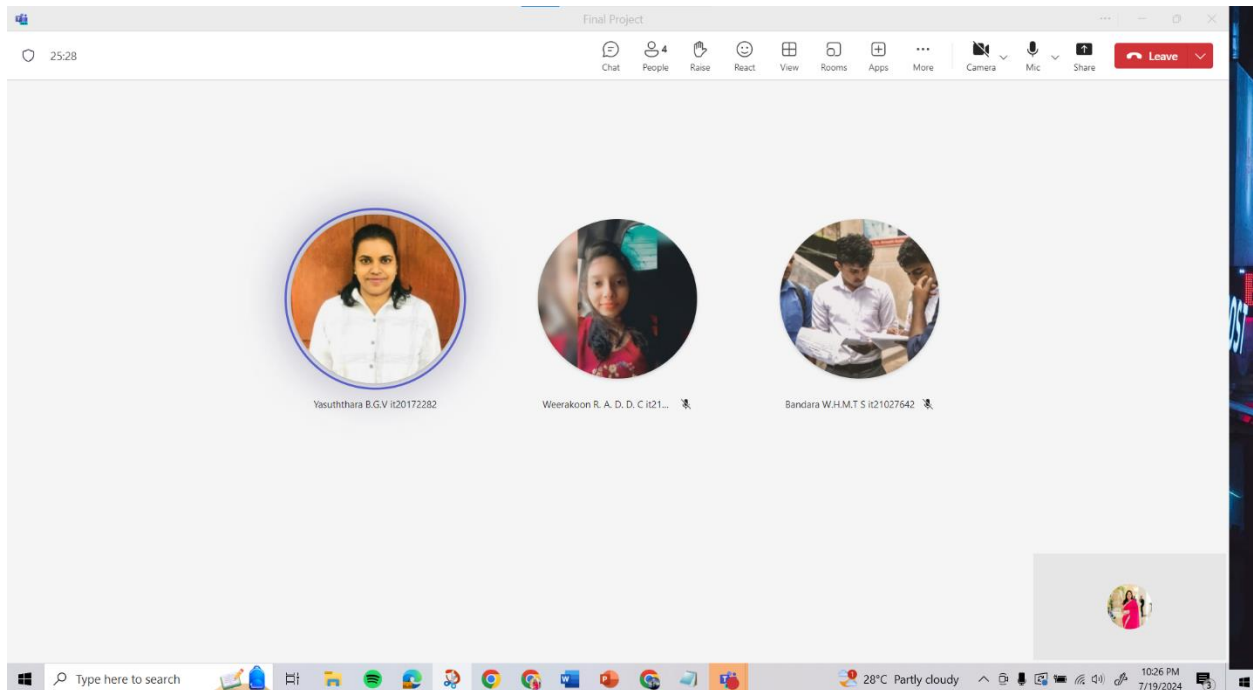


Figure 2: Teams call with team

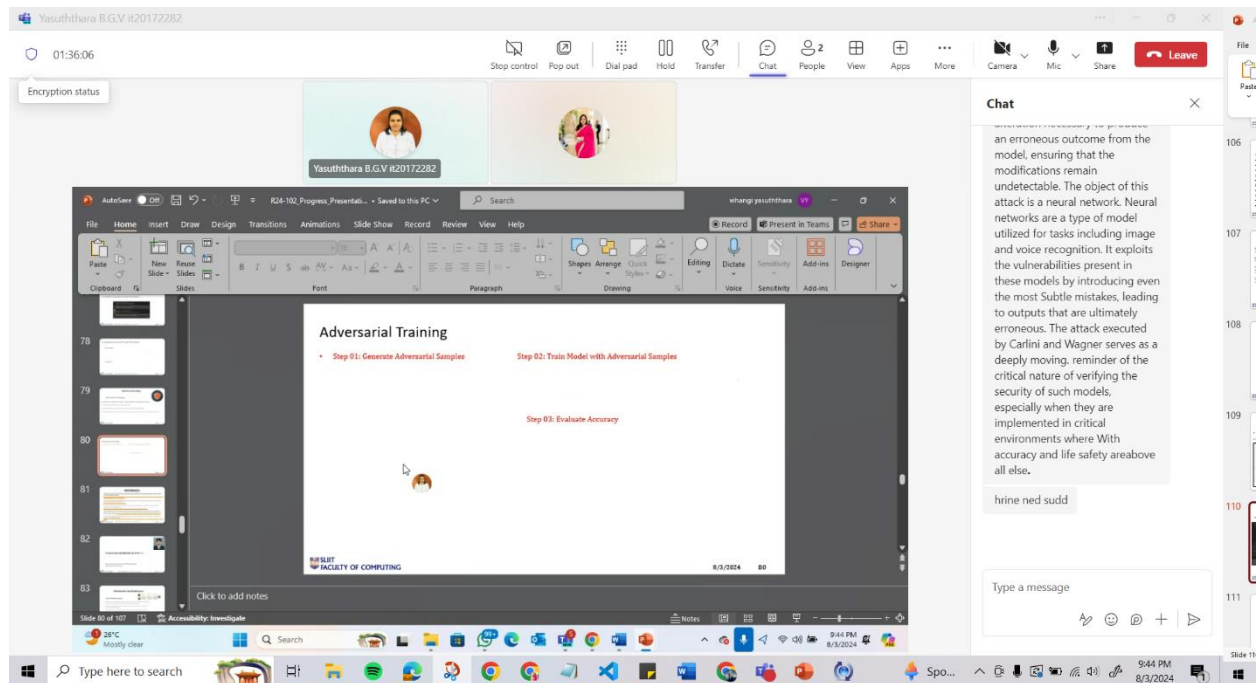


Figure 3: Teams call with team

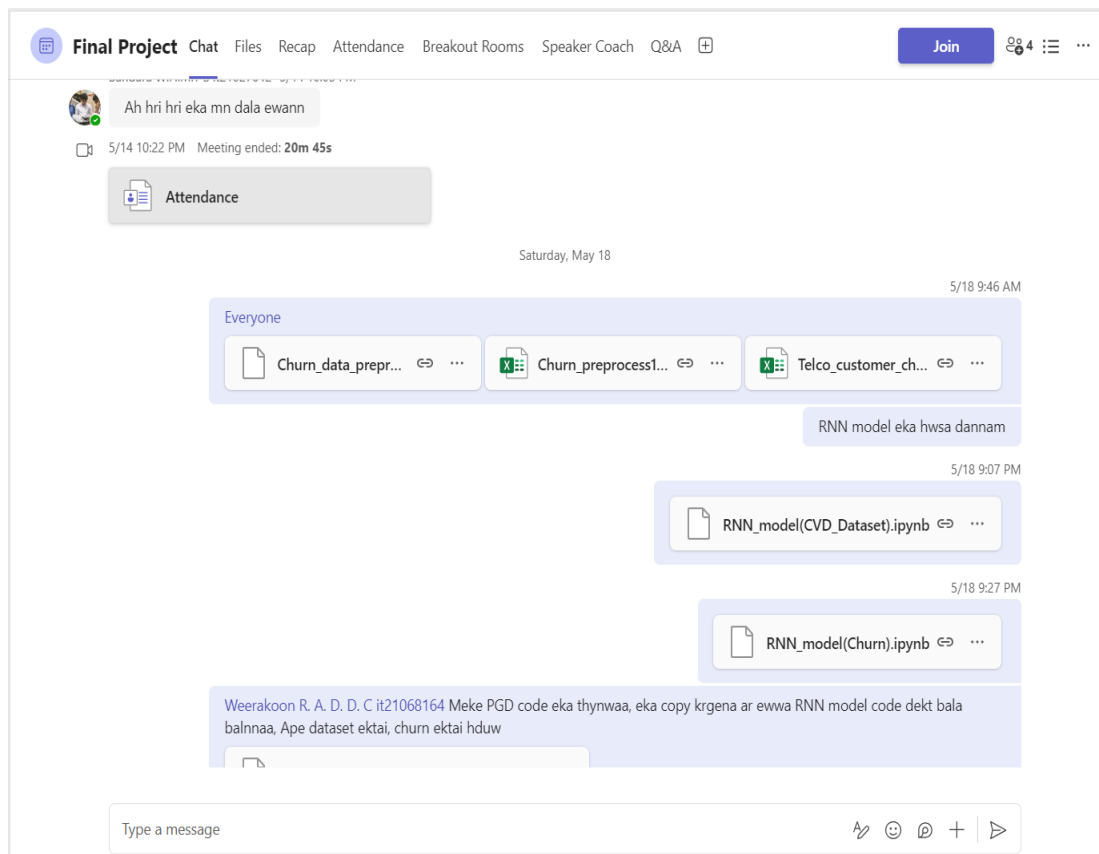


Figure 4: Teams meeting chat with the team

Final Project Chat Files Recap Attendance Breakout Rooms Speaker Coach Q&A				Join	
Upload					
		Name	Shared on	Sent by	
		Thesis Methodology - Boundary Attack.docx	Friday, July 19, 2024	Karandawala D N it21023514	
		Final_Feed-forward_model.ipynb	Saturday, May 18, 2024	Karandawala D N it21023514	
		RNN_model(Churn).ipynb	Saturday, May 18, 2024	Karandawala D N it21023514	
		RNN_model(CVD_Dataset).ipynb	Saturday, May 18, 2024	Karandawala D N it21023514	
		Churn_data_preprocessing 1.ipynb	Saturday, May 18, 2024	Karandawala D N it21023514	
		Churn_preprocess1 1.csv	Saturday, May 18, 2024	Karandawala D N it21023514	
		Telco_customer_churn 1.csv	Saturday, May 18, 2024	Karandawala D N it21023514	
		R24-102_Progress_Presentation 1 3.pptx	Tuesday, May 7, 2024	Karandawala D N it21023514	
		carlini wagner.ipynb	Monday, May 6, 2024	Yasuththara B.G.V it20172282	
		PGD 1.ipynb	Monday, May 6, 2024	Weerakoon R. A. D. D. C it21068164	
		R24-102_Progress_Presentation 1 2.pptx	Sunday, May 5, 2024	Karandawala D N it21023514	
		992507900_NP (1).jpg	Sunday, May 5, 2024	Bandara W.H.M.T S it21027642	
		with SLIIT location - GPS example.jpg	Sunday, May 5, 2024	Weerakoon R. A. D. D. C it21068164	
		R24-102_Progress_Presentation 1 1.pptx	Tuesday, April 30, 2024	Karandawala D N it21023514	
		untitled15 1 .py	Sunday, April 28, 2024	Yasuththara B.G.V it20172282	

Figure 5: Teams meeting chat with the team

## 2. WhatsApp calls and text message communication with the supervisor.

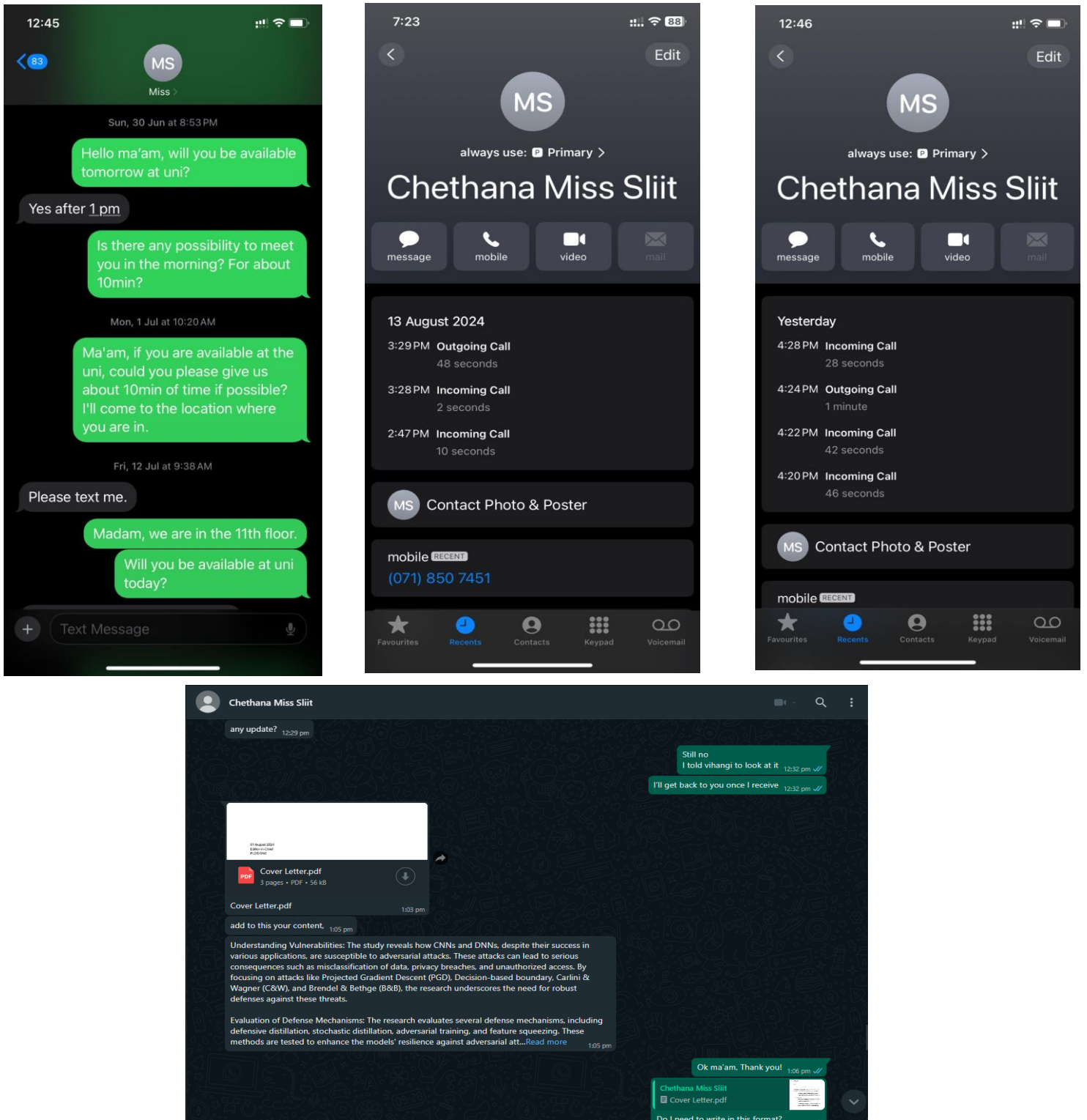


Figure 1: Meeting confirmations and feedbacks about the project from the supervisor

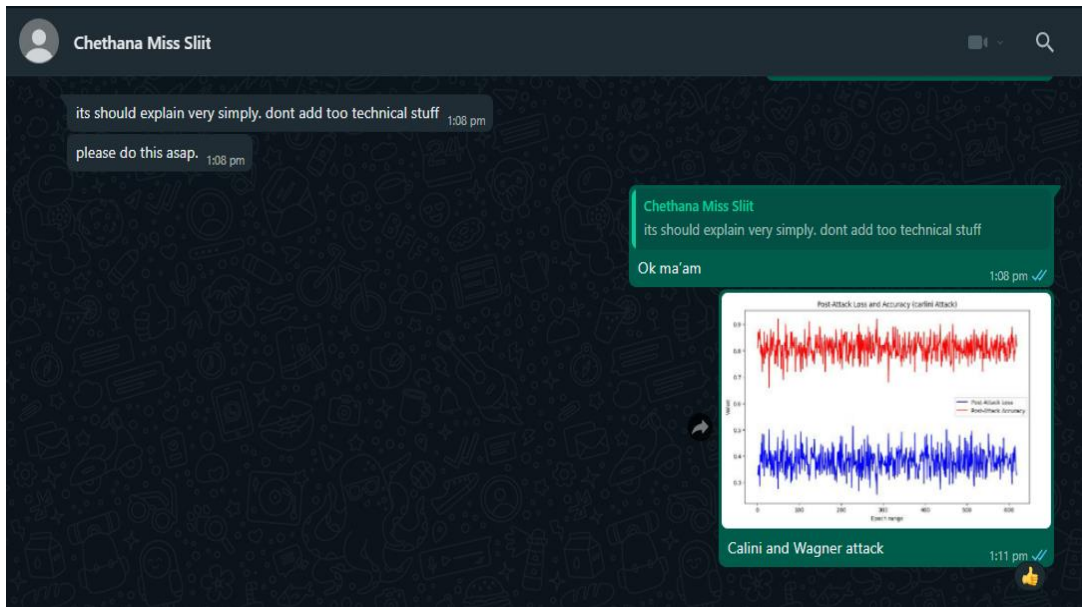


Figure 2: Supervisor's feedbacks on project work

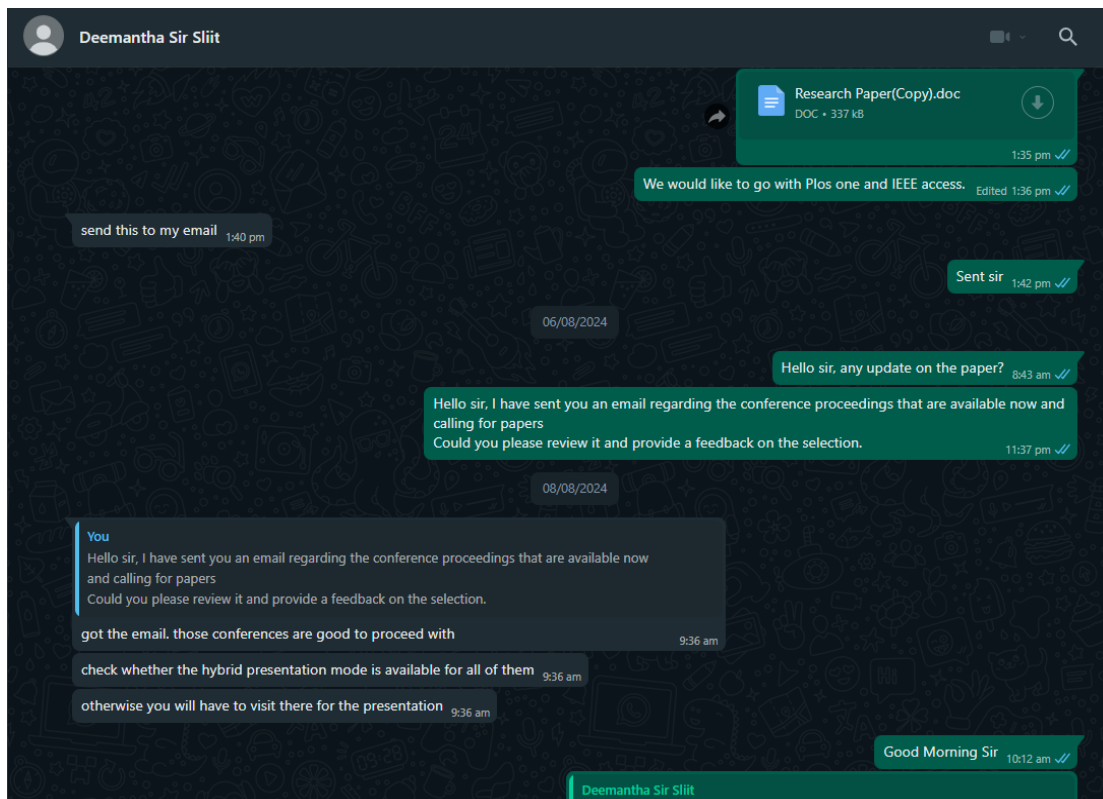



Figure 3: Communication with co-supervisor

### 3. Email Communications with Supervisors








Request for Feedback on Conference Paper Submissions




Karandawala D N it21023514

To: Chethana Liyanapathirana

Cc: Deemantha Siriwardana



Tue 06/08/2024 23:09



Conference Publication list.xlsx


12 KB

Dear Ma'am/Sir,

Attached, you will find a document listing the current conferences open for paper submissions. I have highlighted a few conferences in green that I am considering for my paper submission.

Could you please review these selections and provide your feedback on whether I can proceed with submitting my paper to these conferences?








Thanks & regards,  
Devindi Karandawala.



Deemantha Siriwardana <deemantha.s@slit.lk>

To: Chethana Liyanapathirana

Cc: Karandawala D N it21023514



Thu 08/08/2024 15:33

**[EXTERNAL EMAIL] This email has been received from an external source – please review before actioning, clicking on links, or opening attachments.**

Dear Madam


The following conference is found to be Scopus Indexed.

- IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)

Following conferences are indexed in IEEE Xplore and might have a chance of indexed in Scopus. But specific information could not be found.








- IEEE International Conference on Internet of Things and Intelligence System (IoTIS 2024):
- International Conference on System Reliability and Safety (ICSRS 2024)
- IEEE International Conference on Social Networks Analysis, Management and Security
- International Women in Engineering (WIE) Conference on Electrical and Computer Engineering

Research Paper




Karandawala D N it21023514

To: Chethana Liyanapathirana



Mon 05/08/2024 11:25




Research Paper(Copy).doc


337 KB

Dear Ma'am,

Please find the attached Research paper. We are seeking your valuable feedback on this.

Thanks & regards,  
Devindi Karandawala.

 Reply

 Forward



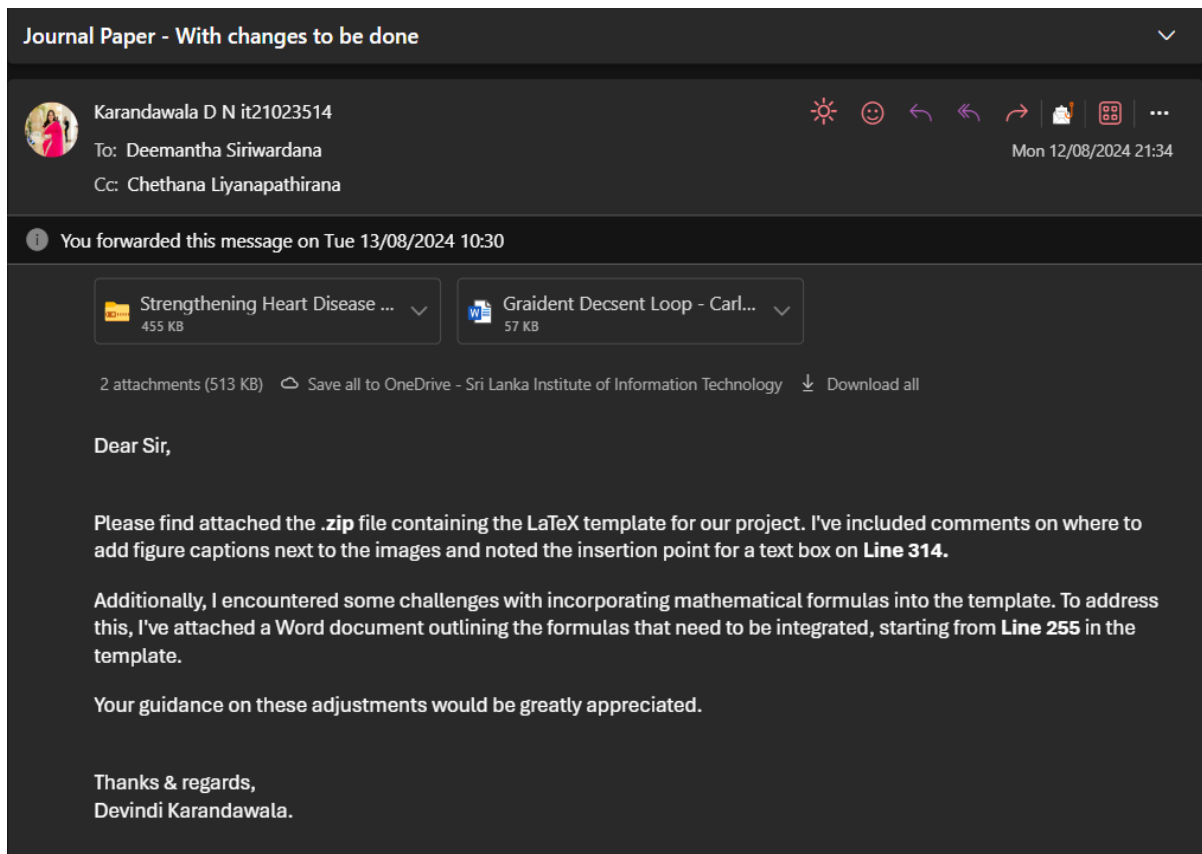
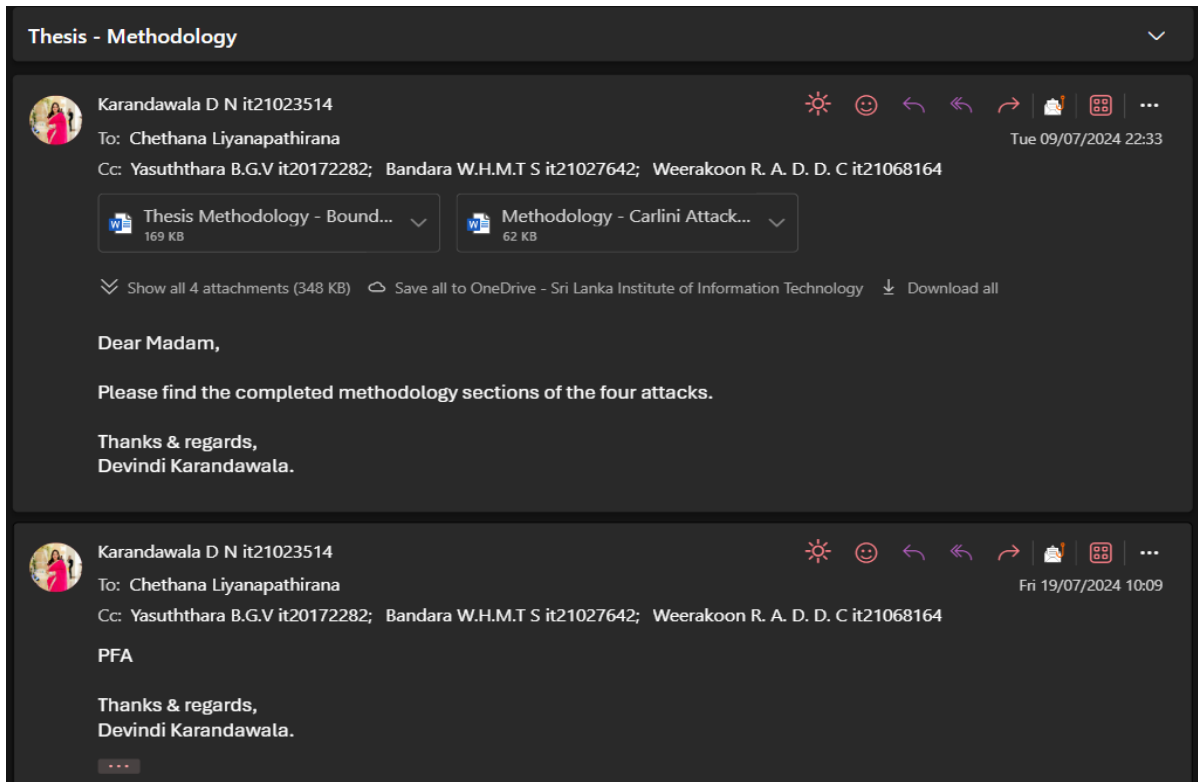


Figure 4: Email communications with supervisors

## 4. Microsoft Planner

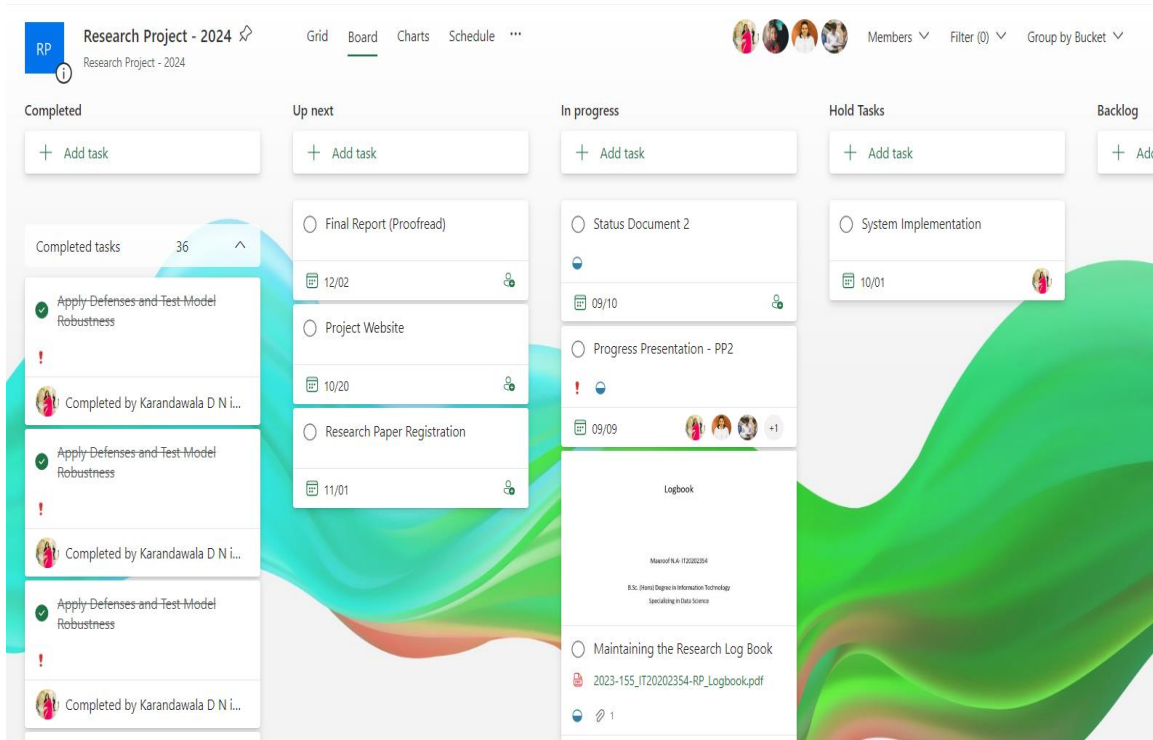


Figure 5: MS Project Planner

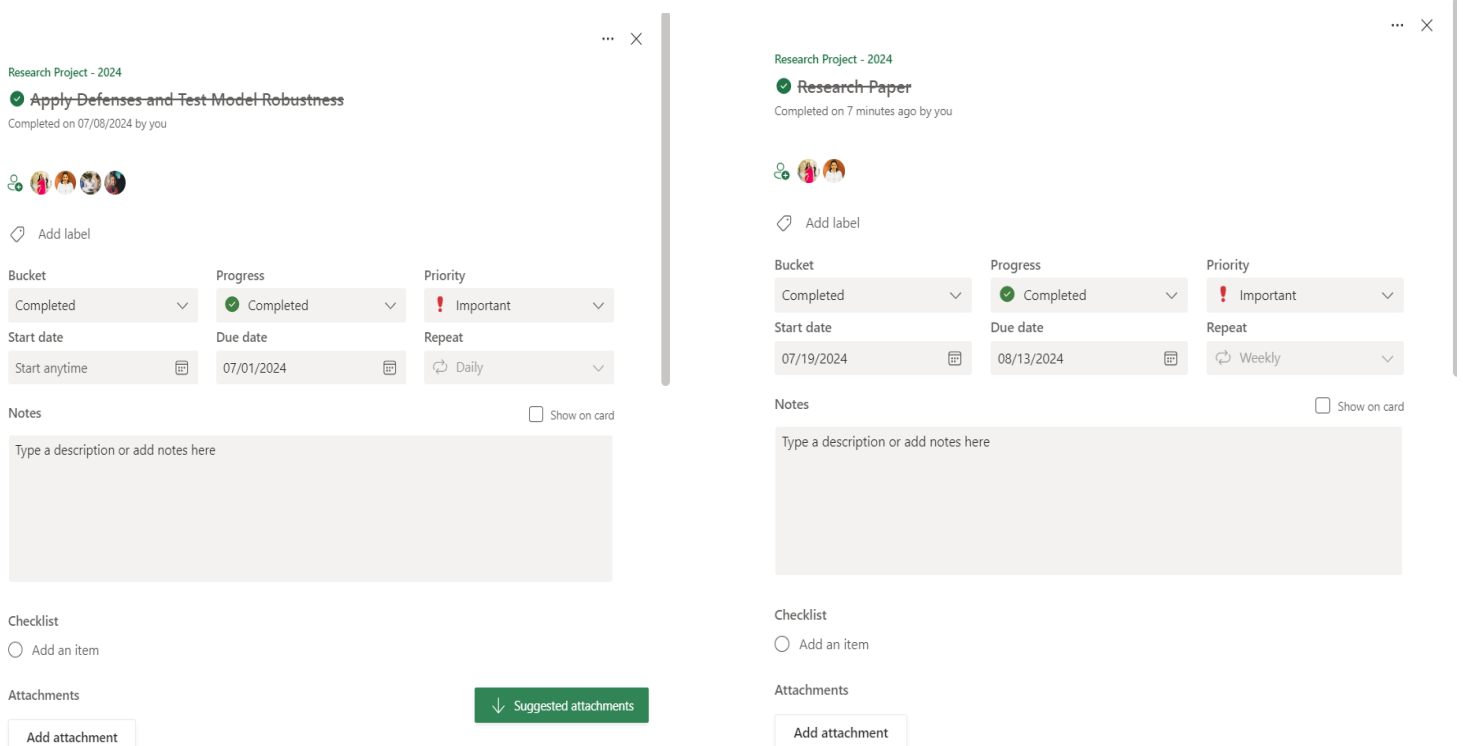


Figure 9: MS Project Planner

<div> <div> <div>RP</div> <div>Research Project - 2024</div> </div> <div> <div>Grid</div> <div>Board</div> <div>Charts</div> <div>Schedule</div> <div>...</div> </div> </div> <div> <div>Members</div> <div> <div></div> <div></div> <div></div> <div></div> </div> </div>						
Title	Assignment	Start date	Due date	Bucket	Progress	Priority
✓ Apply Defenses and Test Model Robustness	<div></div>		7/1/2024	Completed	✓ Completed	! Important
✓ Apply Defenses and Test Model Robustness	<div></div>		7/1/2024	Completed	✓ Completed	! Important
✓ Apply Defenses and Test Model Robustness	<div></div>		7/1/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/18/2024	6/30/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/19/2024	6/30/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/20/2024	7/1/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/21/2024	7/2/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/22/2024	6/30/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/23/2024	6/30/2024	Completed	✓ Completed	! Important
✓ Apply Defenses and Test Model Robustness	<div></div>		7/1/2024	Completed	✓ Completed	! Important
✓ Apply Defenses and Test Model Robustness	<div></div>		7/30/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/24/2024	7/5/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/25/2024	7/6/2024	Completed	✓ Completed	! Important
✓ Model 2 building and testing	<div></div>	5/26/2024	7/5/2024	Completed	✓ Completed	! Important
✓ Final Reports	<div></div>	7/4/2024	8/23/2024	Completed	✓ Completed	! Important
✓ Research Paper	<div></div>	7/19/2024	8/13/2024	Completed	✓ Completed	! Important
<div> <div>+</div> <div>Add new task</div> </div>						

Figure 10: Completed tasks

## 5. Gantt Chart

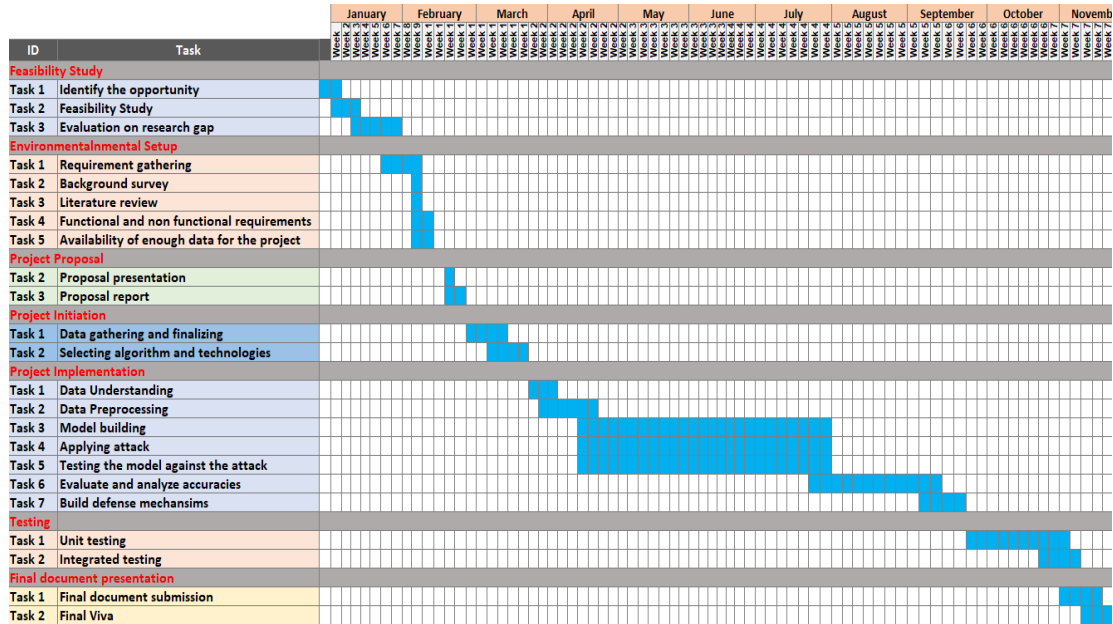


Figure 11 Gantt chart

## 6. Work Breakdown Structure

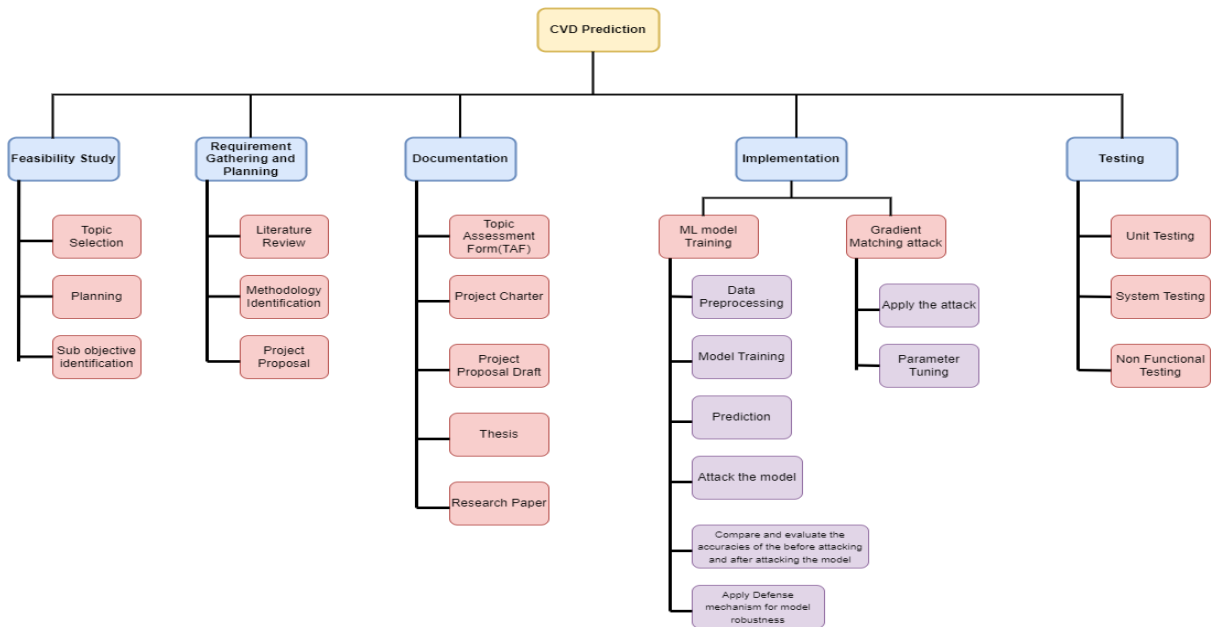


Figure 12: WBS

## 7. GitLab Commits

GitLab Projects Groups More

Search or jump to...

R24-102

Project overview

Repository

Files

Commits

Branches

Tags

Contributors

Graph

Compare

Issues 0

Merge Requests 0

CI / CD

Operations

Collapse sidebar

Brendel\_and\_bethge\_defensive\_distillation  
Savindhya Bandara authored 10 hours ago

Name	Last commit	Last update
Boundary_Attack.ipynb	Initial commit	4 months ago
Boundary_Attack_Defense_Adversarial_Trainin...	Boundary attack defense - Adversarial Training	1 day ago
Boundary_Attack_Defense_Ensemble_Model.ip...	Boundary attack defense - Ensemble Model	1 day ago
Brendel_and_Bethge_Attack.ipynb	Brendel and Bethge Attack	4 months ago
Brendel_and_bethge_defensive_distillation.py	Brendel_and_bethge_defensive_distillation	10 hours ago
Carlini_Attack.ipynb	Carlini_Attack	4 months ago
Carlini_Wagner_Attack_Defense_Adversarial_tr...	Carlini & Wagner Attack Defense Adversarial Training	22 hours ago
Final_1D_CNN_Model.ipynb	Final 1D CNN model	4 months ago
Final_Data_Preprocessing.ipynb	Initial commit	4 months ago
PGD_attack.ipynb	PGD attack code	4 months ago
README.md	Add README.md	4 months ago
Stochastic_Distillation.ipynb	PGD Attack Defense Strategy - Stochastic Distillation	10 hours ago

R24-102 > R24-102 > Commits

master r24-102 Filter by commit message

08 Sep, 2024 2 commits

Brendel\_and\_bethge\_defensive\_distillation  
Savindhya Bandara authored 10 hours ago

PGD Attack Defense Strategy - Stochastic Distillation  
Devmini Chethika Weerakoon authored 10 hours ago

07 Sep, 2024 1 commit

Carlini & Wagner Attack Defense Adversarial Training  
Vihangi Yasuthara authored 22 hours ago

06 Sep, 2024 2 commits

Boundary attack defense - Adversarial Training  
Devindi Navodya Karandawala authored 1 day ago

Boundary attack defense - Ensemble Model  
Devindi Navodya Karandawala authored 1 day ago

04 May, 2024 3 commits

Final 1D CNN model  
Devindi Navodya Karandawala authored 4 months ago

Delete 1D\_CNN\_Model - Test.ipynb  
Devindi Navodya Karandawala authored 4 months ago

Delete Final\_1D\_CNN\_Model.ipynb  
Devindi Navodya Karandawala authored 4 months ago

Figure 13 GitLab commits