

# **UNIFIED DLP SOLUTIONS FOR EMAIL SYSTEM**

**Project Id: TMP-2023-24-082**

Status Document - 02

LOGU J.J - IT20638818

B.Sc. (Hons) Degree in Information Technology

Specialization in Cyber Security

Department of Information Technology

Sri Lanka Institute of Information Technology

Sri Lanka

March 2024

## Table of Contents

1. Microsoft Teams Details .....	3
1.1 Team Members .....	3
1.2 Team Meeting with Group Members .....	3
1.3 Team meeting with Supervisor.....	5
2. Microsoft team analytics .....	6
2.2 Planner Board .....	<b>Error! Bookmark not defined.</b>
2.2 Team Planner Charts.....	7
3. WhatsApp chat with Supervisor .....	8
4. WhatsApp Call and Chat with Team.....	9
5. Email and planned Teams Events ..	<b>Error! Bookmark not defined.</b>
6. Gantt Chart .....	11
7. Work Breakdown Structure (WBS) .....	12
8. Gitlab Commits .....	12

# 1. Microsoft Teams Details

## 1.1 Team Members

The screenshot shows the Microsoft Teams interface for a team named "TMP-2023-24-082\_ Unified DLP Solutions for Email ...". The left sidebar shows the team's main channels, with "General" selected. The main area displays the "Members" tab, which lists the team's members and their roles.

+ Add member					
▼ Owners (2)					
Name	Title	Location	Tags	Role	
Keshani S.K. h20299002			Leader	Owner	
Amila Nuwan	Senior Lecturer	Malabe		Owner	
▼ Members and guests (3)					
Name	Title	Location	Tags	Role	
Logu J.J. h20638818				Member	
Ahamed R.R. h20650902				Member	
Fayaz A.C.M. h20637828				Member	

## 1.2 Team meeting with Group Members

The screenshot shows a Microsoft Teams meeting interface. The main area displays a presentation slide titled "Send Messages" with a table of email data. The right sidebar shows a list of participants in the meeting.

Recipient Email	Email Title	Email Body	Detected Points	Level	Date Time	St
fayazacm110@gmail.com	Test 3	Hi iam fayaz. This email regarding HR login credentials. username : Fayaz123 password : faq123 username,password	High		2024-03-17 22:11:25	NOT

Participants in the meeting:

- Kokila keshani
- Roshan Ahmed
- Muhammed Fayaz
- Jethushan Logu

Roshan Ahamed (Presenting)

phpMyAdmin

Showing rows 5 - 3 (4 total, Query took 0.000 seconds)

SELECT \* FROM `test\_data`

Query results operations

Print Copy to clipboard Export Display chart Create new

Bookmark this SQL query

Label

Let every user access this bookmark

	email_id	recipient_email	sender_email	sender_password	email_body	email_title	status	timestamp	timestamp2
	25	kokila.ahamed@gmail.com	Test 1	Hi			2024-03-17 21:48:57	SENT	ALL
	26	kokila.ahamed@gmail.com	Test 2	This email regarding HMI login credentials, username: 2024-03-17 21:48:57			2024-03-17 21:48:57	SENT	ALL
	27	kokila.ahamed@gmail.com	Test 3	Hi iam fayaz This email regarding HMI login creden			2024-03-17 22:13:37	SENT	ALL
	28	kokila.ahamed@gmail.com	Test 4	I am Jethushan Logu This email regarding HMI login creden			2024-03-17 22:13:37	SENT	ALL

22:22 | rpr-vghf-rol

Roshan Ahamed (Presenting)

Project

App.py

```

# Initialize variables for email parameters
sender_email = "rpr.vghf@gmail.com"
sender_password = "2024-03-17 21:48:57"
receiver_email = kokila.ahamed@gmail.com
email_subject = kokila.ahamed@gmail.com
email_body = kokila.ahamed@gmail.com

# Call the send_email function
if send_email(sender_email, sender_password, receiver_email, email_subject, email_body):
    message = {"status": "success", "text": "Email sent successfully"}
else:
    message = {"status": "error", "text": "Failed to send email"}

# Update status in the database
senddata_status = "SENT"

try:
    db.session.commit()
except Exception as e:
    db.session.rollback()
    message = {"status": "error", "text": "Failed to update status"}

release_message = {"status": "success", "text": "Email sent successfully"}

```

22:24 | rpr-vghf-rol

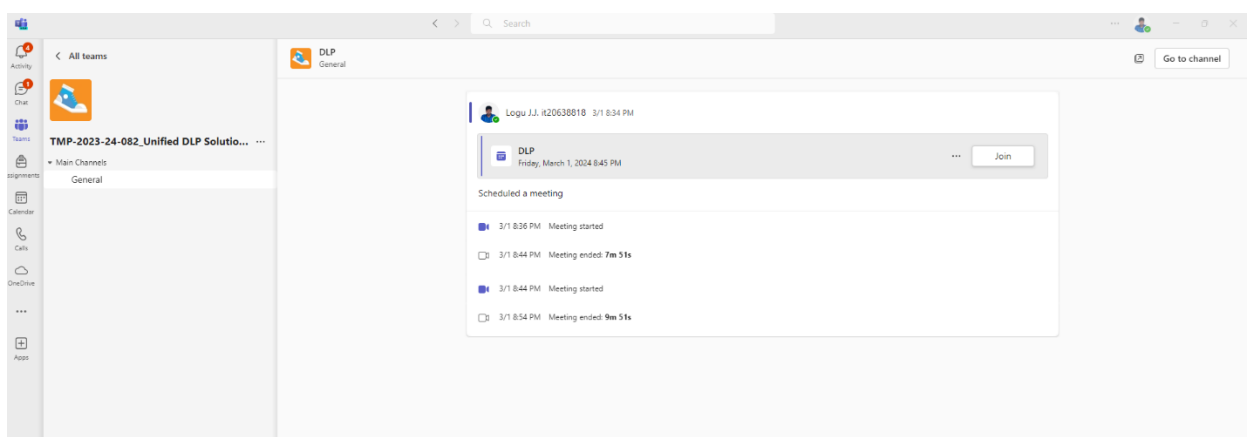
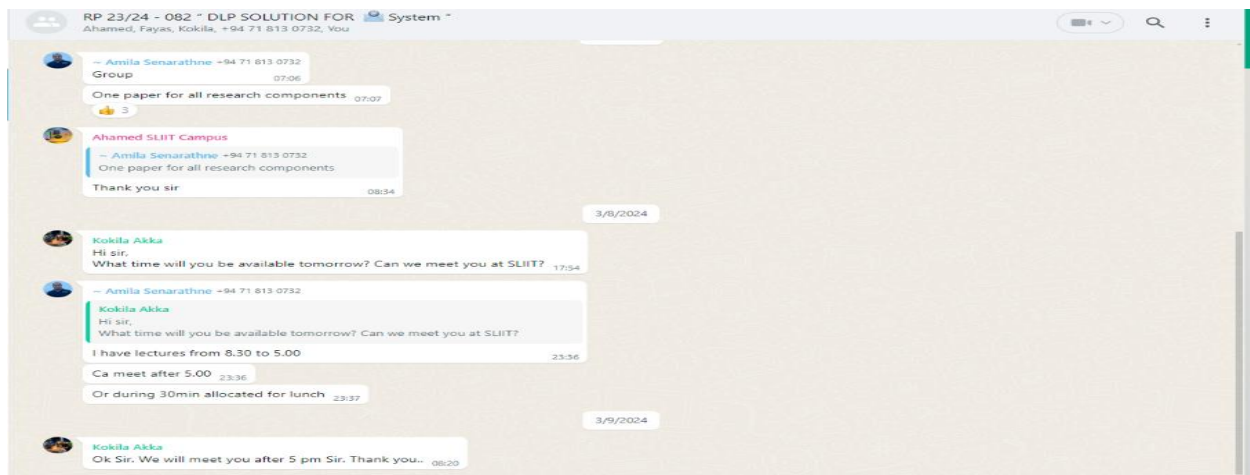
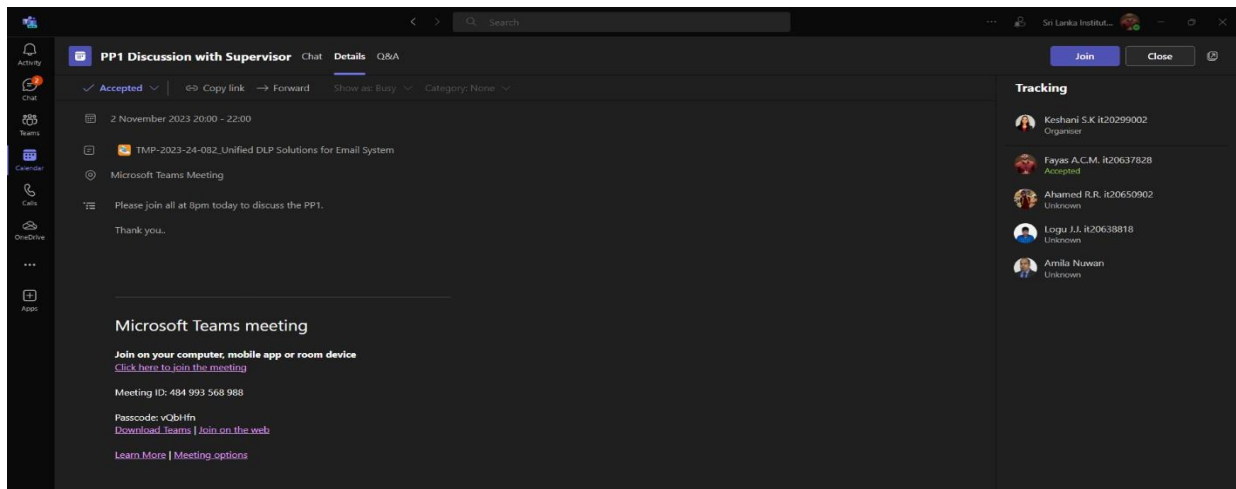
Roshan Ahamed

Jethushan Logu

Muhammed Fayaz

kokila keshani

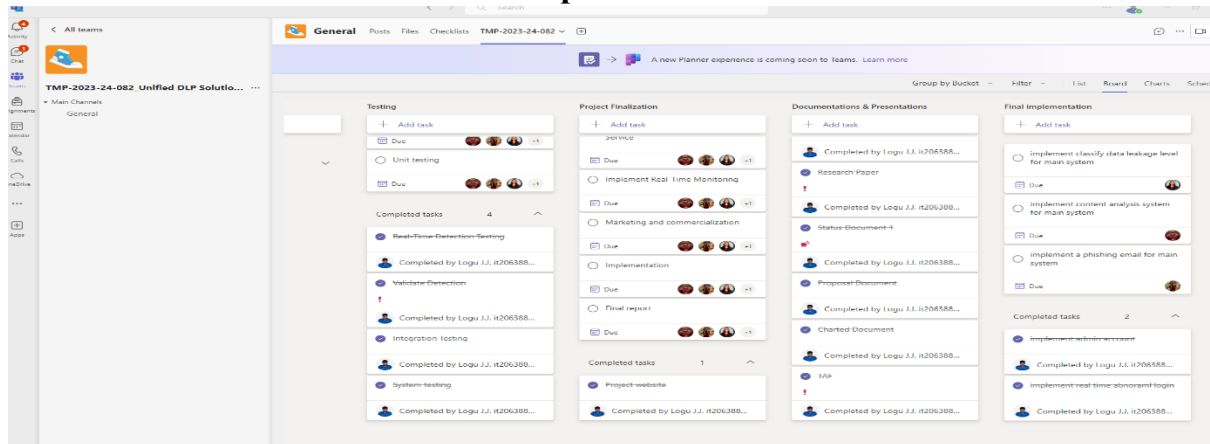
## 1.3 Team Meeting with Supervisor



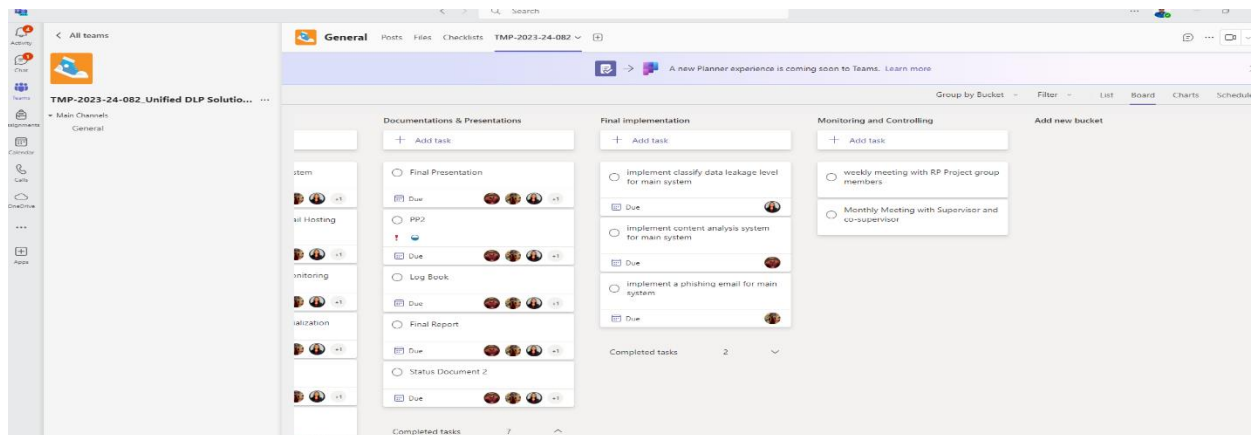


### 3. MS team's planner

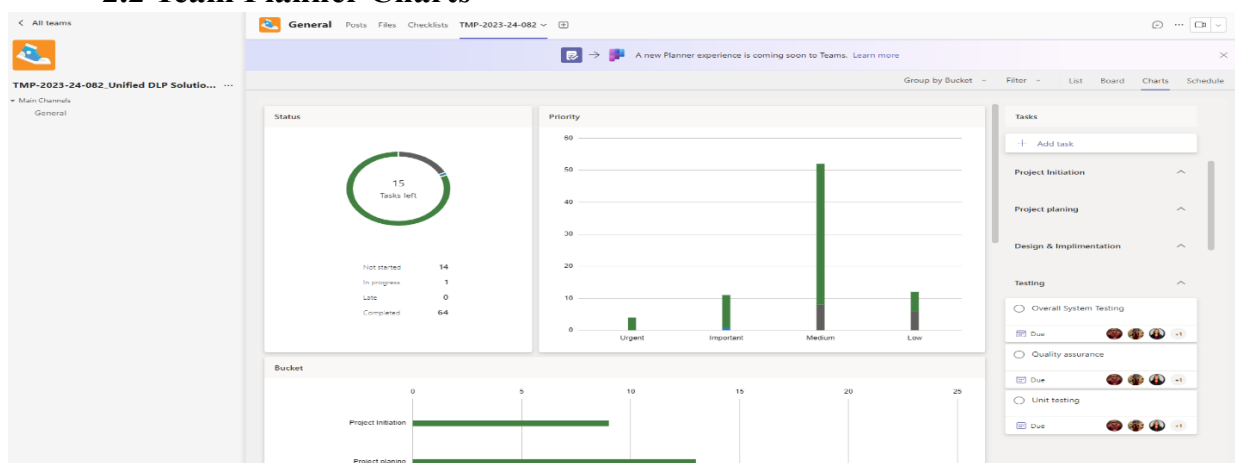
#### Completed Tasks



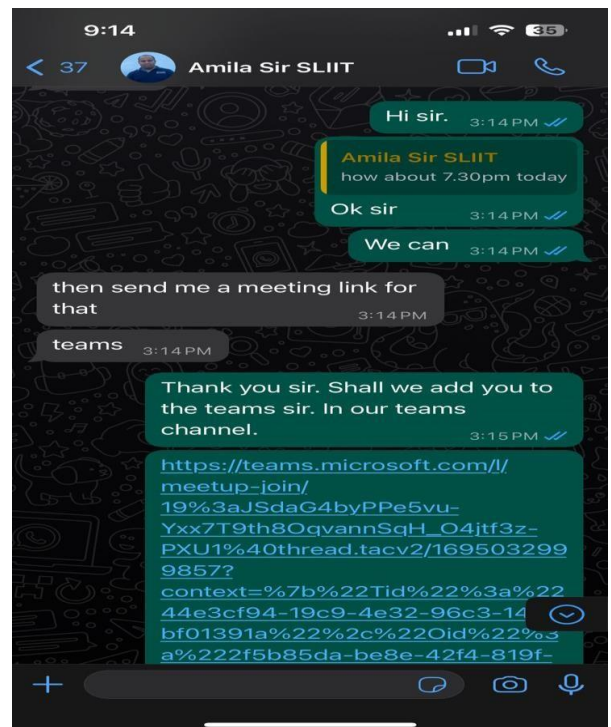
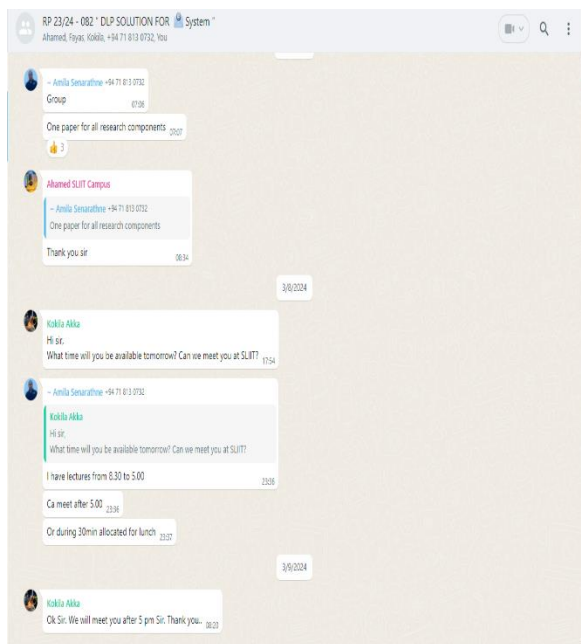
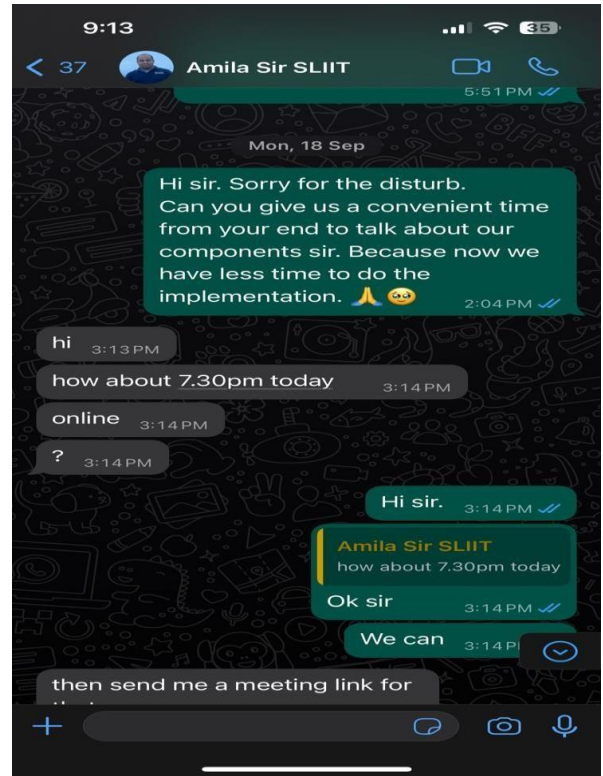
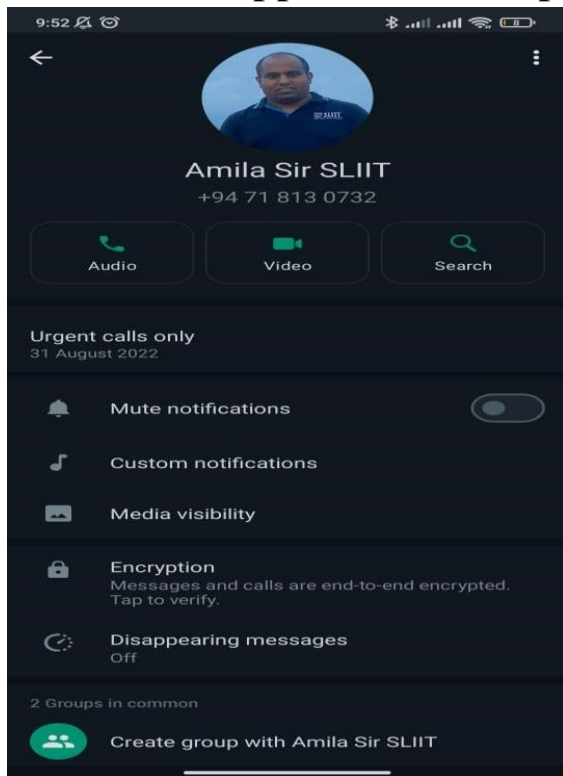
#### Pending Tasks



#### 2.2 Team Planner Charts

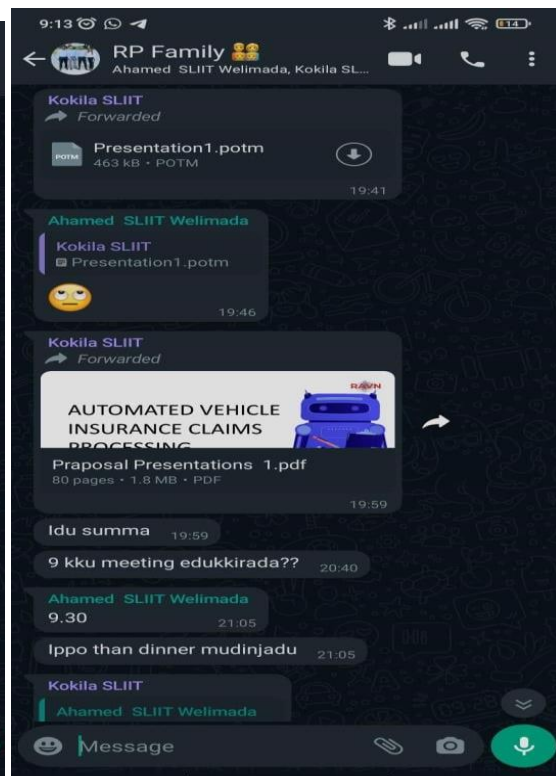
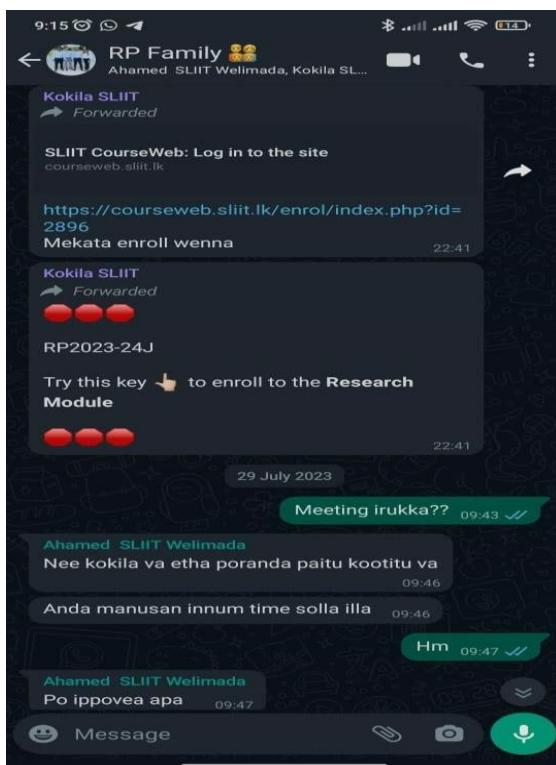
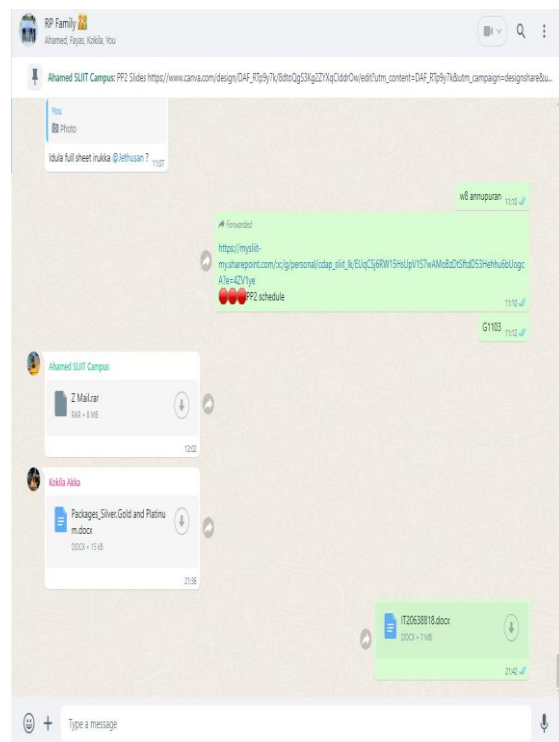
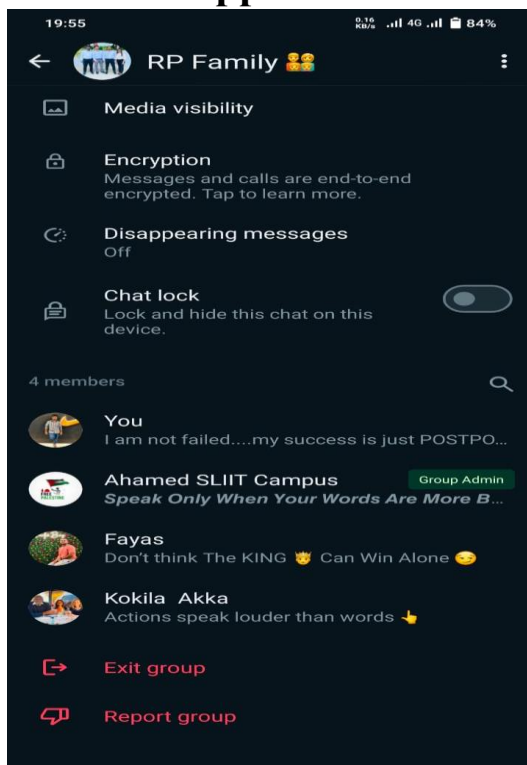


### 3. WhatsApp chat with Supervisor

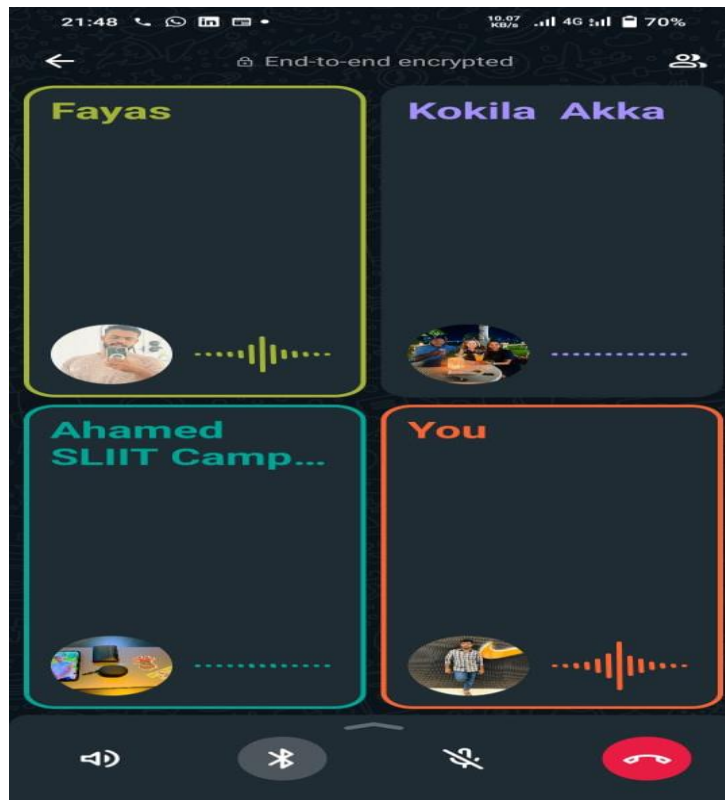




## 4. WhatsApp Call and Chat with Team

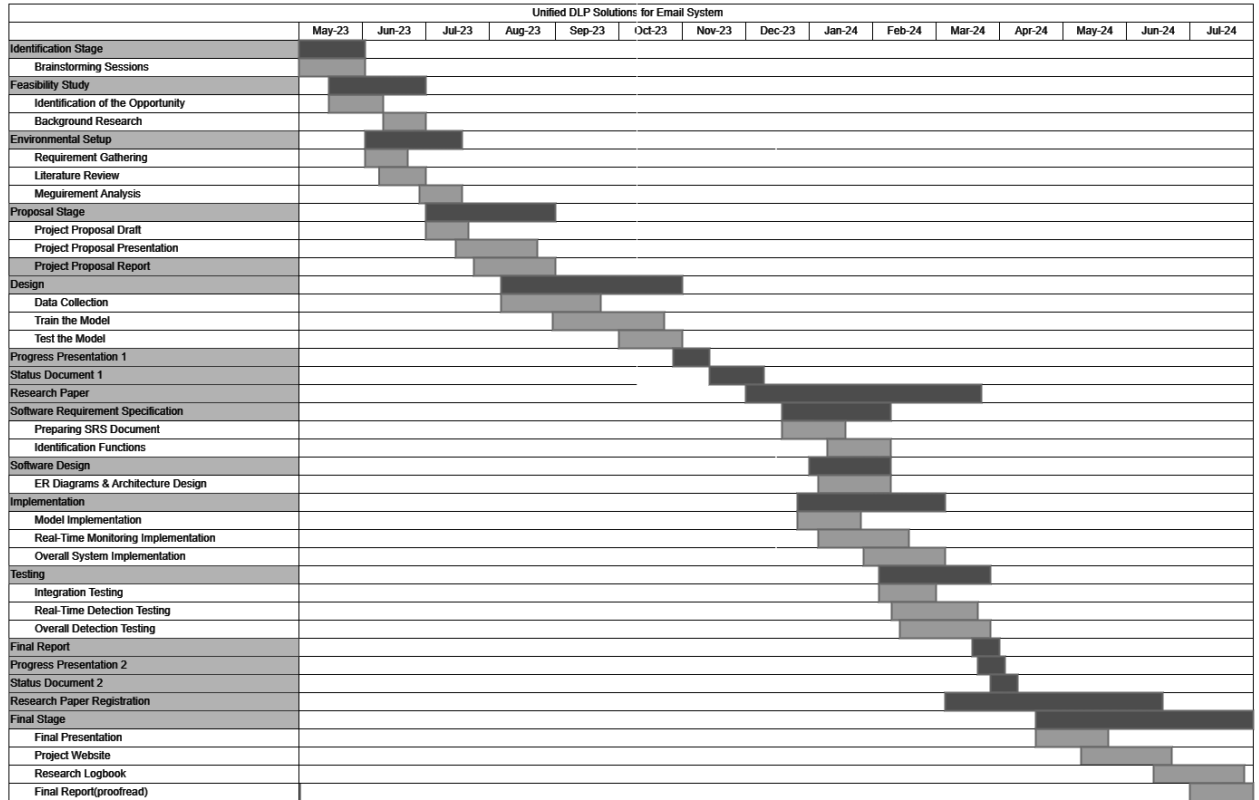


## Recent Meeting with team members WhatsApp group call discussing about PP2 Update

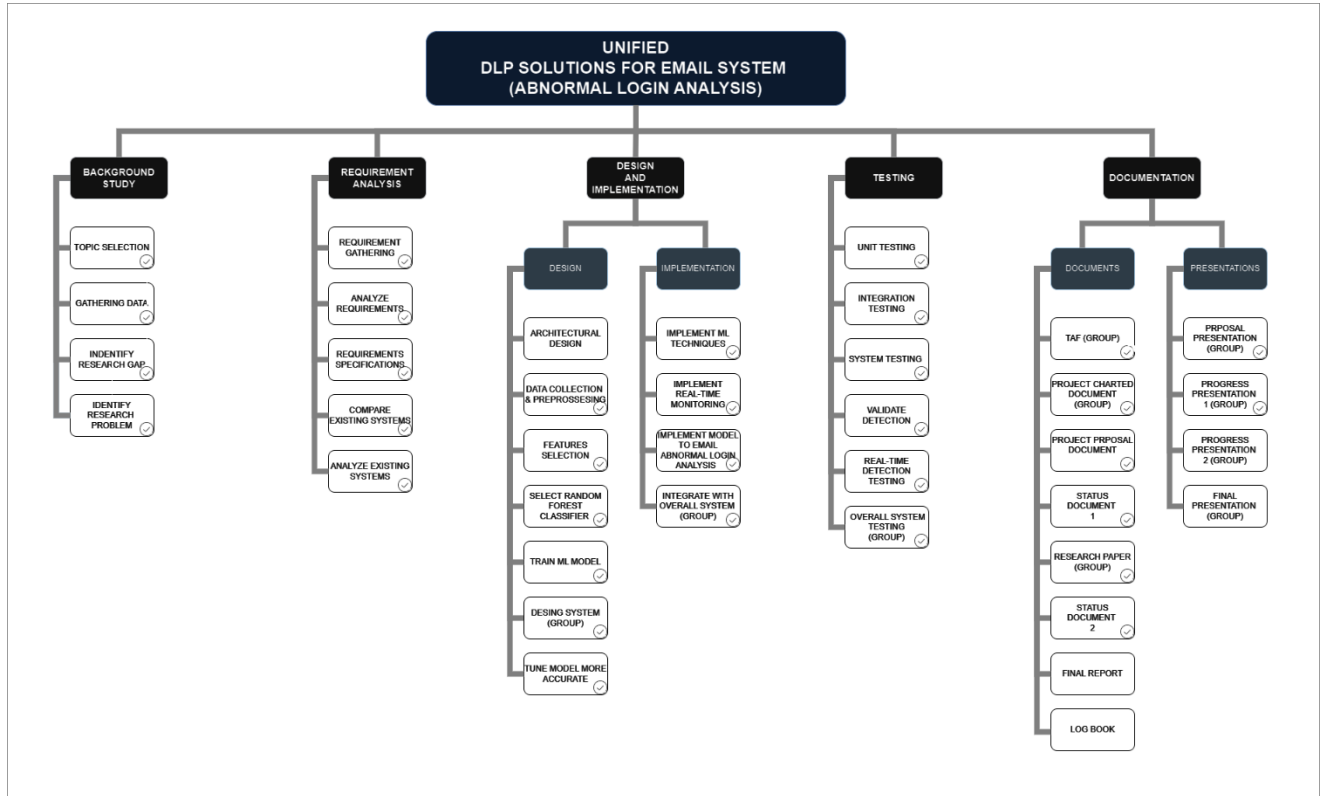


*Fig: recent whatsapp call Meeting*

## 6. Gantt Chart



## 7. Work Breakdown Structure (WBS)



## 8. Gitlab Commits

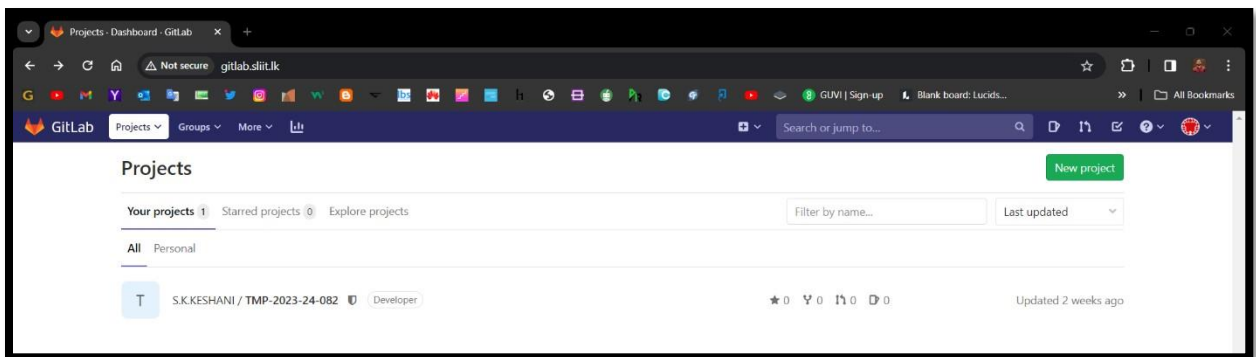


Fig: Project

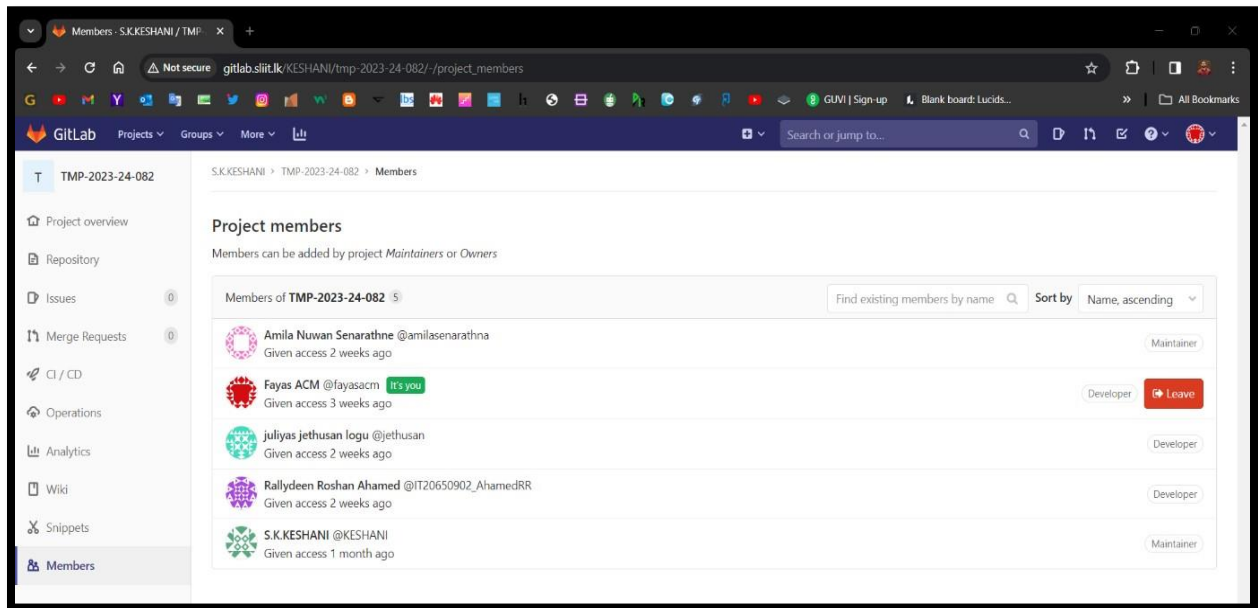


Fig: Team Members and Supervisor

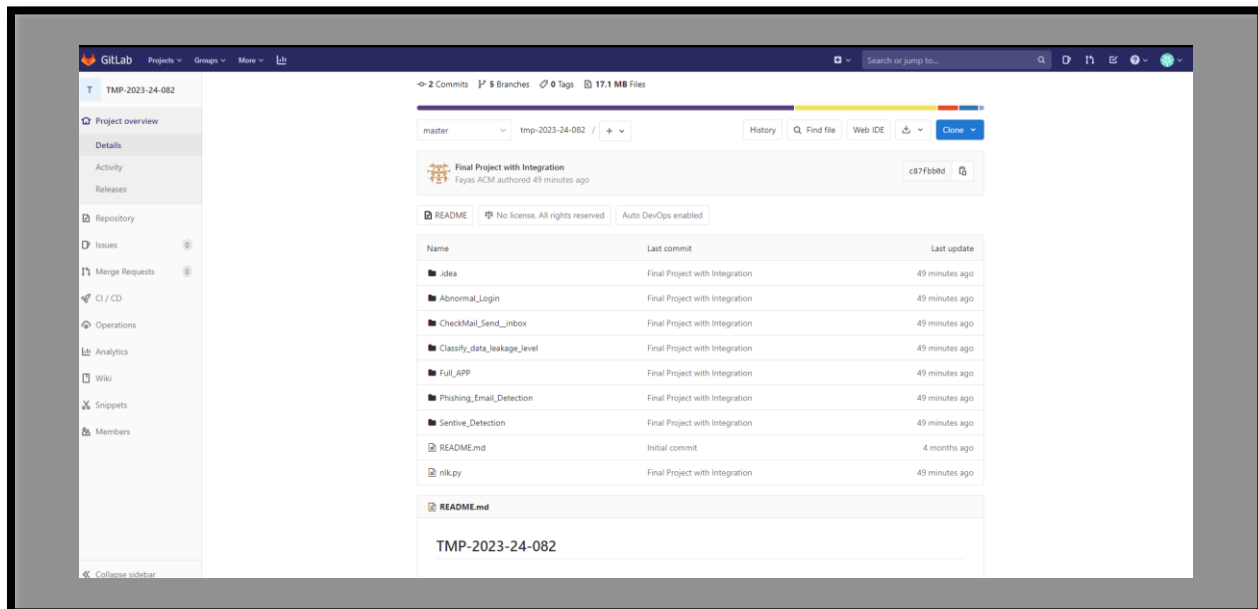
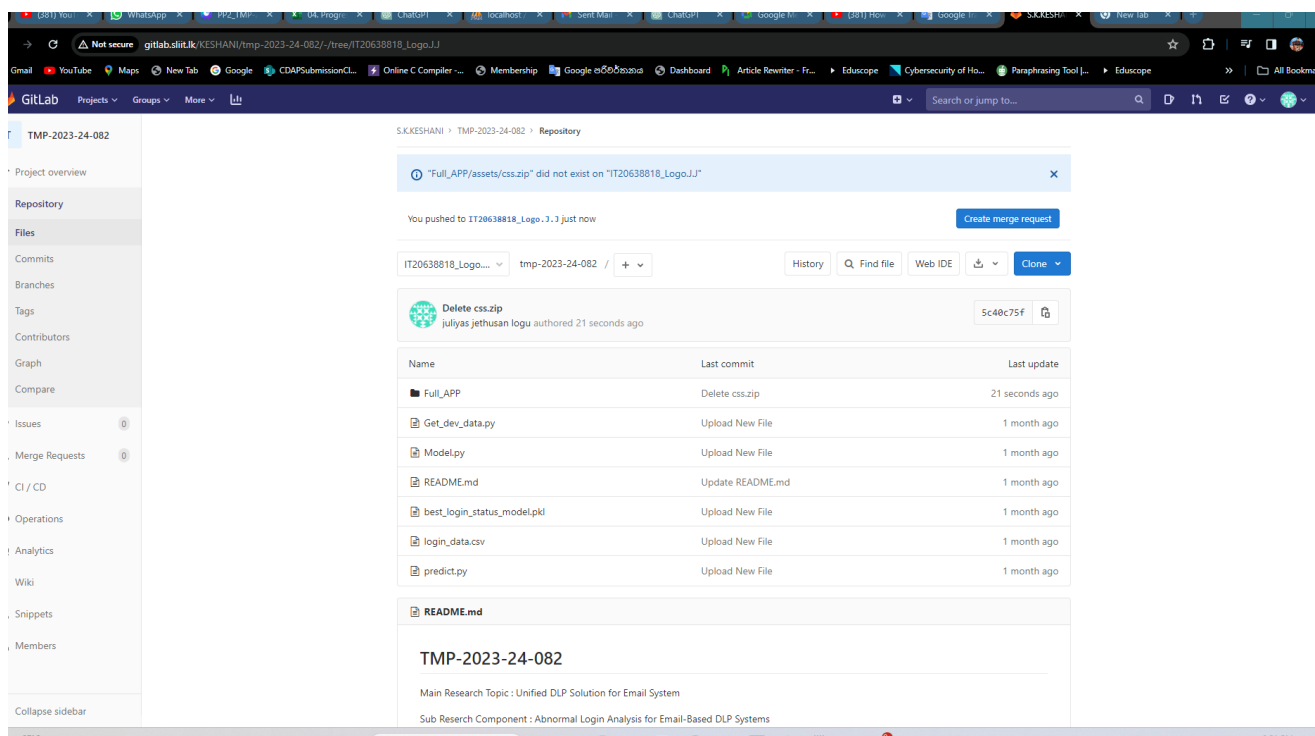


Fig: Code Repository group



*Code repository individual*

**README.md**

## TMP-2023-24-082

Main Research Topic : Unified DLP Solution for Email System

Sub Reserch Component : Abnormal Login Analysis for Email-Based DLP Systems

Develop a system that employs analytical techniques to monitor, detect, and respond to unusual or unauthorized login activities in email systems. Implement multi-factor authentication for enhanced security. Abnormal login analysis in email systems is a pivotal component of Data Leakage Prevention (DLP). When an unusual login is detected, the system can take measures such as sending alerts, locking the account, or requiring additional authentication.

Main Objective: The primary goal of Abnormal Login Analysis in DLP systems is to promptly detect and respond to unusual or unauthorized login attempts, thereby safeguarding email data and preventing potential data breaches.

Sub-Objectives: • User Behavior Profiling: Establish baselines of regular user login patterns, including times, locations, and devices, to facilitate the identification of anomalies. • Geographic Analysis: Flag login attempts from unusual or high-risk geographic locations, especially if they don't align with the user's typical patterns. • Sequential Login Analysis: Detect rapid sequences of login attempts, which might indicate brute-force attacks. • Integration with Response Protocols: Seamlessly integrate the abnormal login detection module with automated response systems, ensuring swift actions like account locks or alert notifications.

*Fig: ReadMe File*