UNIFIED DLP SOLUTIONS FOR EMAIL SYSTEM

Project Id: TMP-2023-24-082

Status Document - 01

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

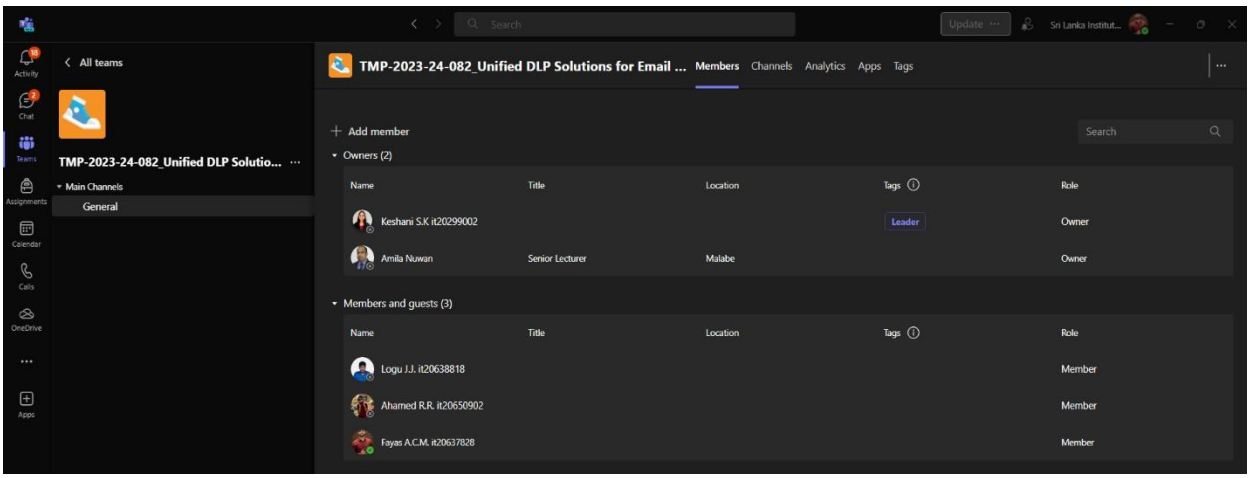
December 2023

Table of Contents

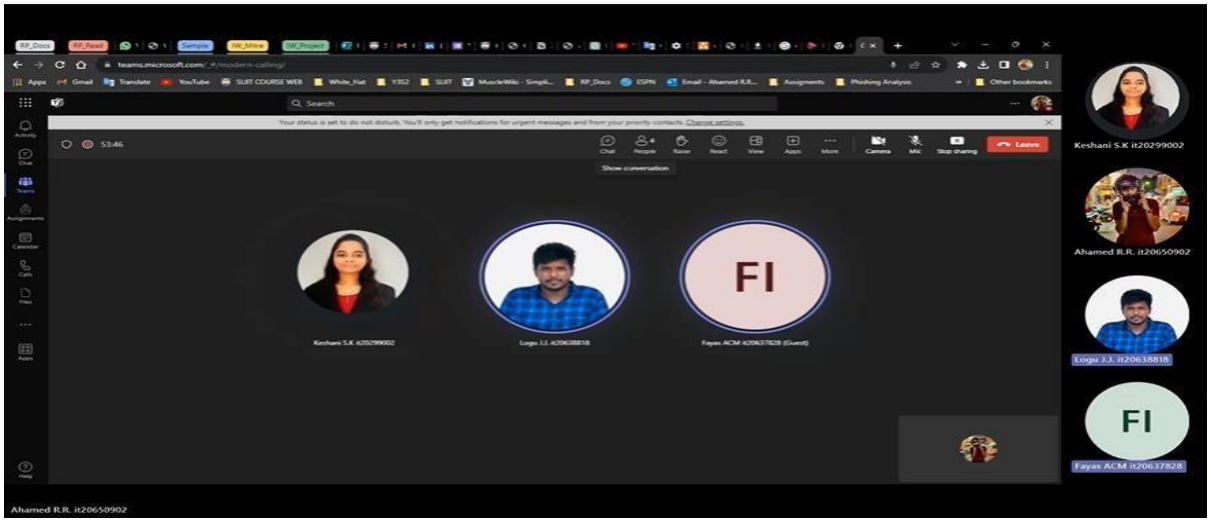
1. Microsoft Teams Details 3
1.1 Team Members 3
1.2 Team Meeting with Group Members 3
1.3 Team meeting with Supervisor.....5
2. MS Teams Planner 7
2.2 Planner Board 7
2.2 Team Planner Charts.....8
3. WhatsApp chat with Supervisor 9
4. WhatsApp Call and Chat with Team.....10
5. Email and planned Teams Events 11
6. Gannt Chart 13
7. Work Breakdown Structure (WBS) 14
8. Gitlab Commits 14

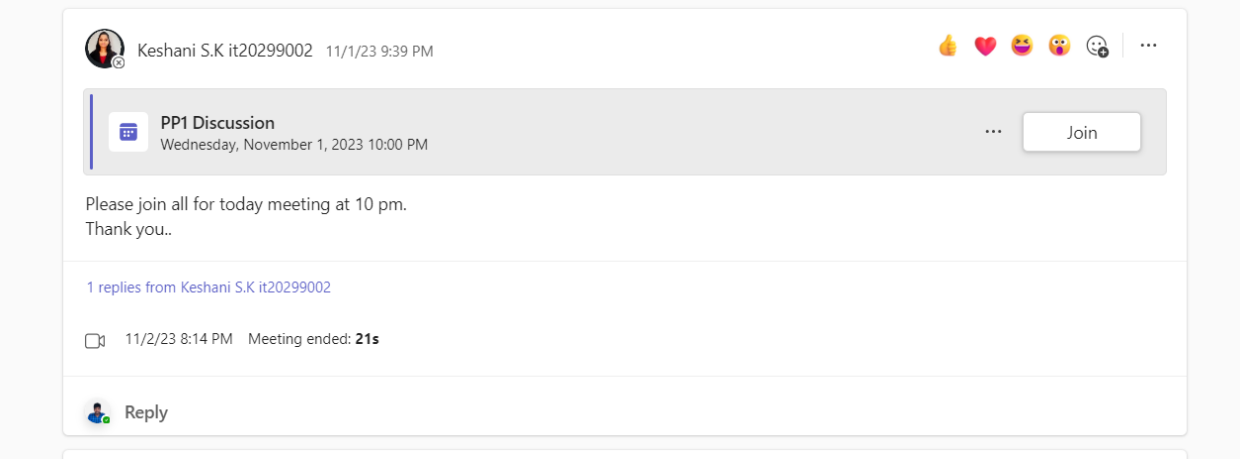
1. Microsoft Teams Details

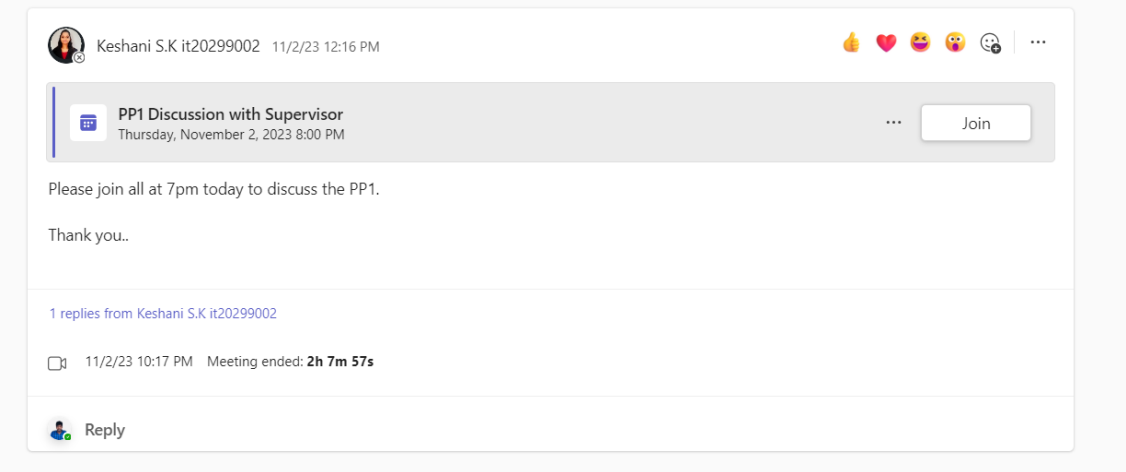
1.1 Team Members

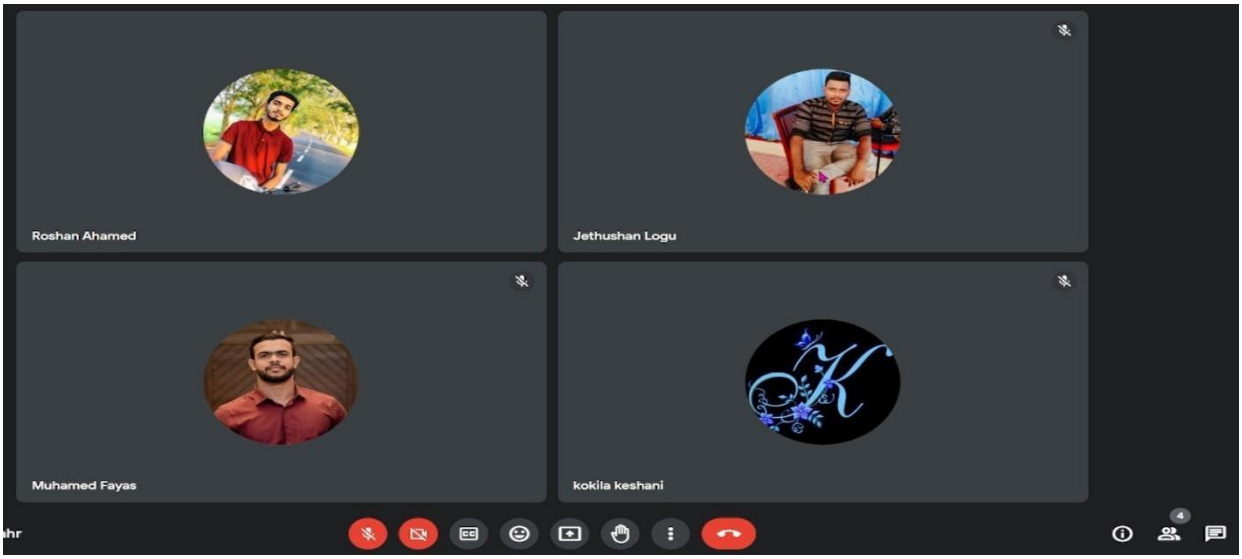


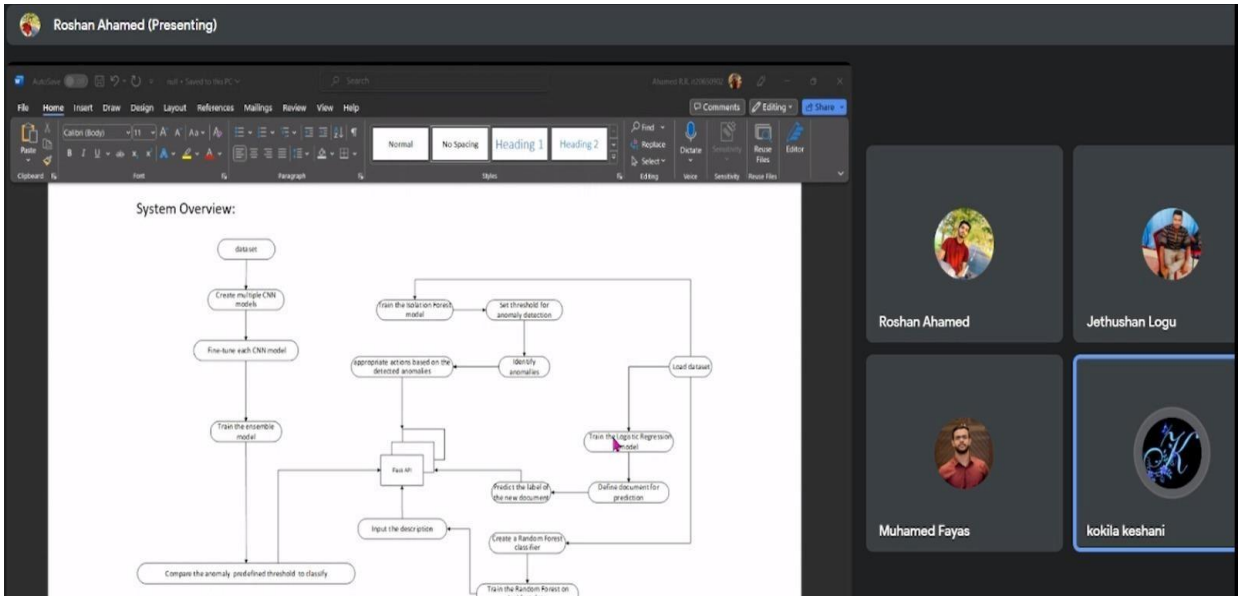
1.2 Team meeting with Group Members



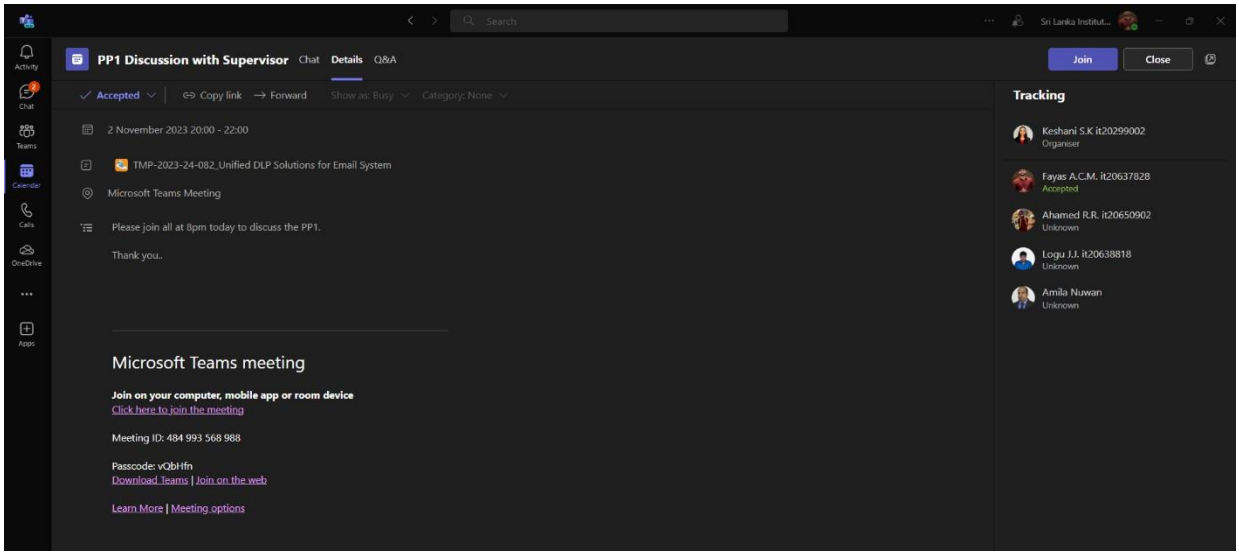

Keshani S.K it20299002 11/1/23 9:39 PM
PP1 Discussion
Wednesday, November 1, 2023 10:00 PM
Join
Please join all for today meeting at 10 pm.
Thank you..
1 replies from Keshani S.K it20299002
11/2/23 8:14 PM Meeting ended: 21s
Reply

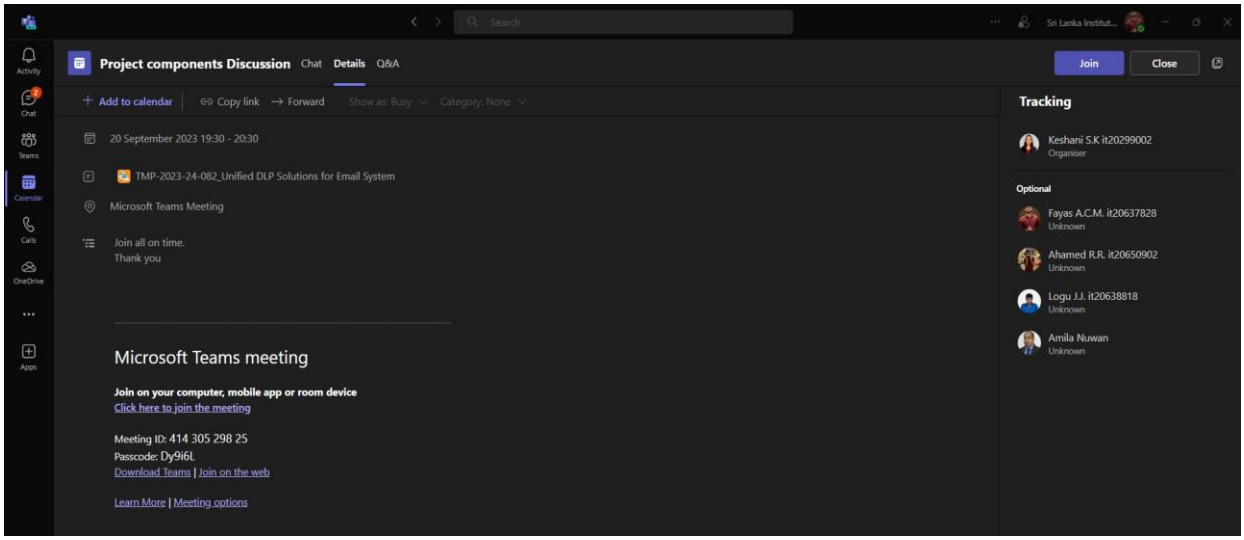

Keshani S.K it20299002 11/2/23 12:16 PM
PP1 Discussion with Supervisor
Thursday, November 2, 2023 8:00 PM
Join
Please join all at 7pm today to discuss the PP1.
Thank you..
1 replies from Keshani S.K it20299002
11/2/23 10:17 PM Meeting ended: 2h 7m 57s
Reply

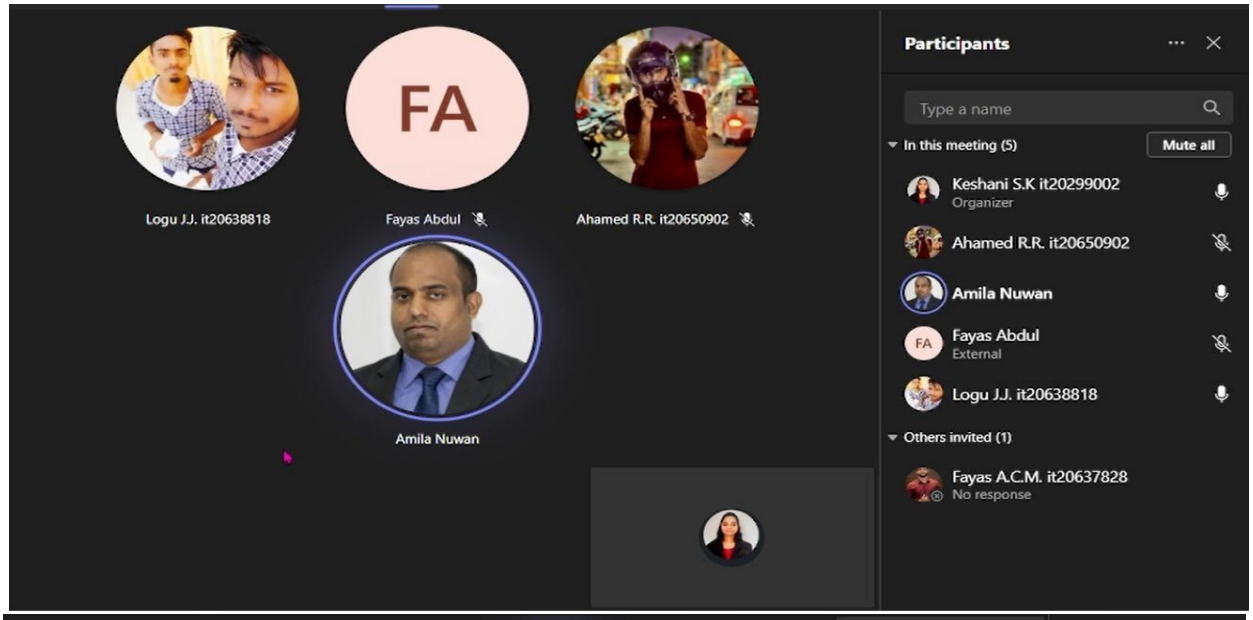

Roshan Ahamed
Jethushan Logu
Muhamed Fayas
kokila keshani

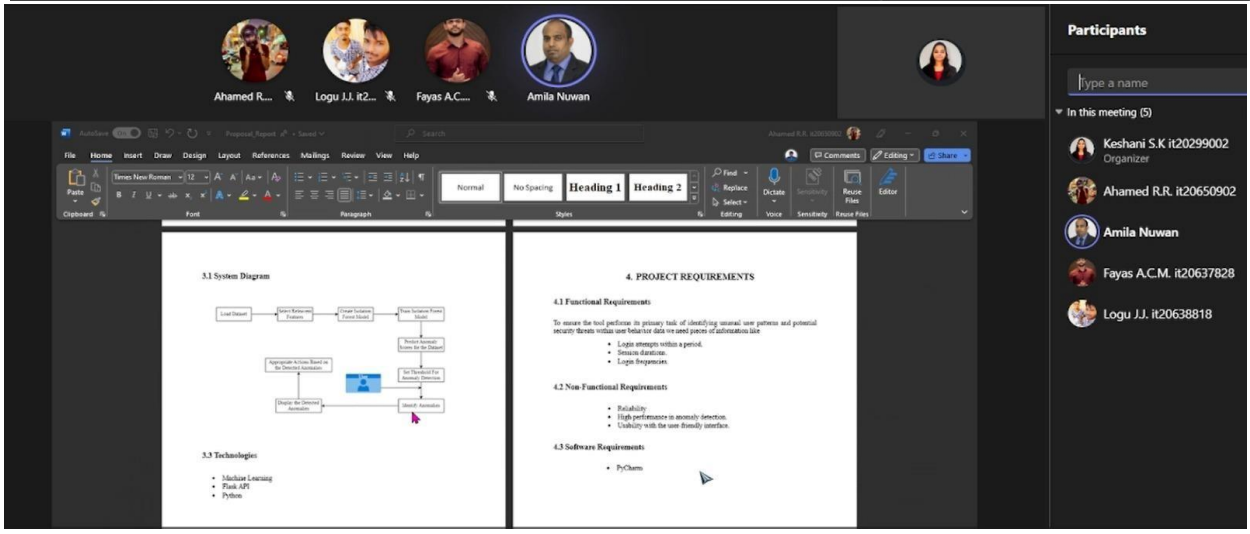


1.3 Team Meeting with Supervisor




Project components Discussion
Chat
Details
Q&A
Join
Close
Add to calendar
Copy link
Forward
20 September 2023 19:30 - 20:30
TMP-2023-24-082_Unified DLP Solutions for Email System
Microsoft Teams Meeting
Join all on time.
Thank you
Microsoft Teams meeting
Join on your computer, mobile app or room device
Click here to join the meeting
Meeting ID: 414 305 298 25
Passcode: Dy9i6L
Download Teams | Join on the web
Learn More | Meeting options
Tracking
Keshani S.K it20299002
Organiser
Optional
Fayas A.C.M. it20637828
Ahamed R.R. it20650902
Logu J.J. it20638818
Amila Nuwan
Unknown

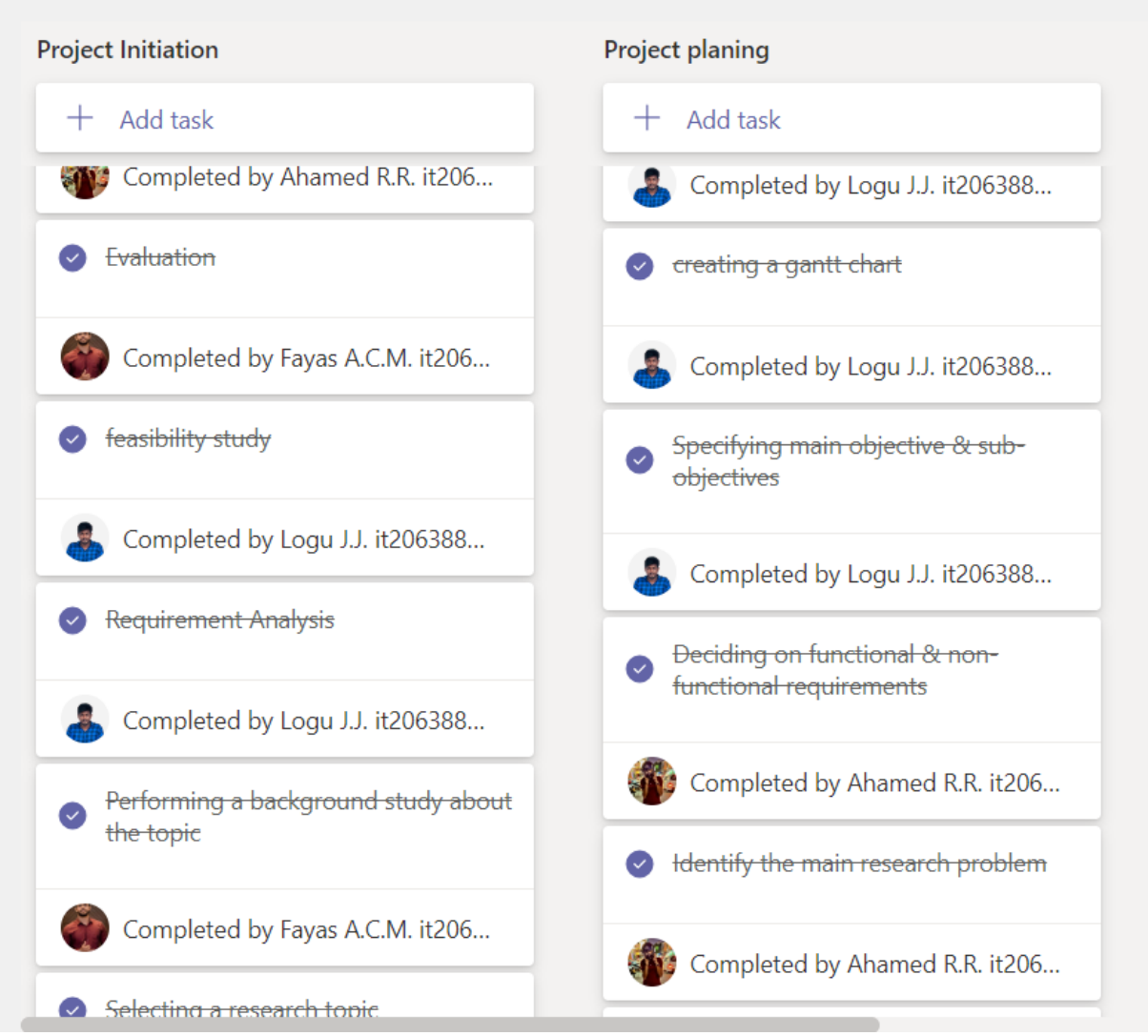

Logu J.J. it20638818
Fayas Abdul
Ahamed R.R. it20650902
Amila Nuwan
Participants
Type a name
In this meeting (5)
Mute all
Keshani S.K it20299002
Organizer
Ahamed R.R. it20650902
Amila Nuwan
Fayas Abdul
External
Logu J.J. it20638818
Others invited (1)
Fayas A.C.M. it20637828
No response


Ahamed R....
Logu J.J. it2...
Fayas A.C....
Amila Nuwan
Participants
Type a name
In this meeting (5)
Keshani S.K it20299002
Organizer
Ahamed R.R. it20650902
Amila Nuwan
Fayas A.C.M. it20637828
Logu J.J. it20638818
3.1 System Diagram
3.3 Technologies
Machine Learning
Flask API
Python
4. PROJECT REQUIREMENTS
4.1 Functional Requirements
4.2 Non-Functional Requirements
Reliability
High performance in anomaly detection.
Usability with the user-friendly interface.
4.3 Software Requirements
PyCharm

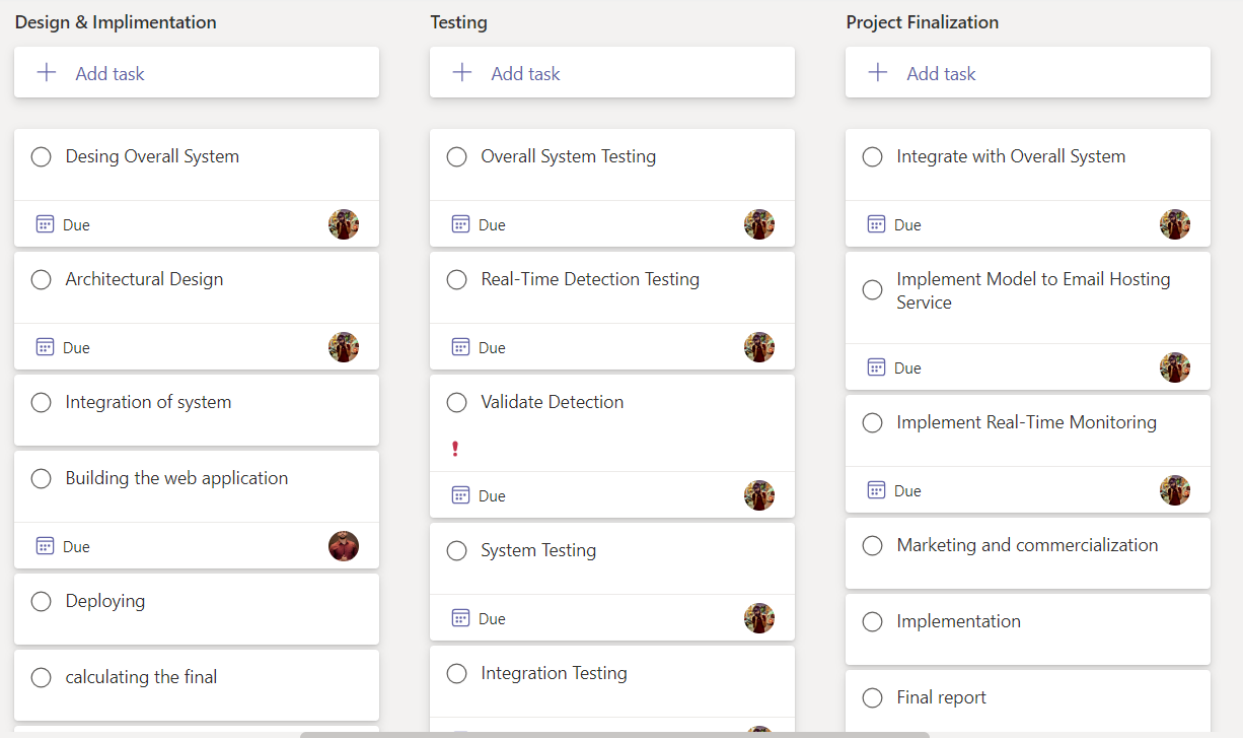
2. MS Teams Planner

2.2 Planner Board

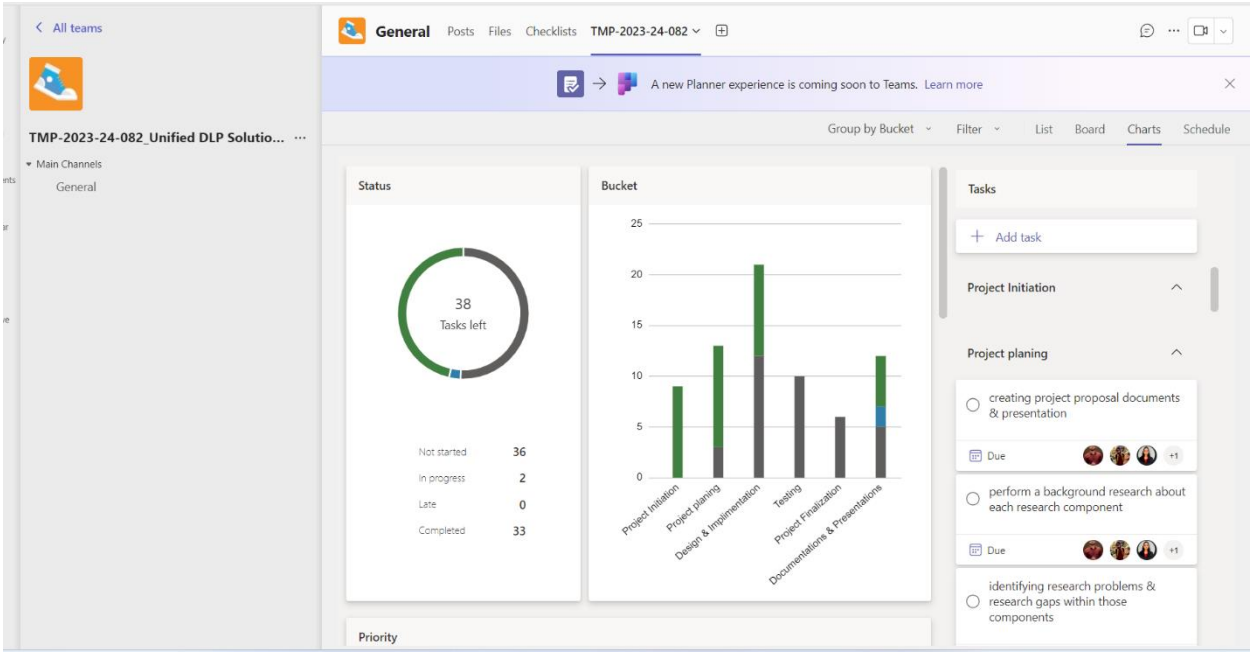
Completed Tasks



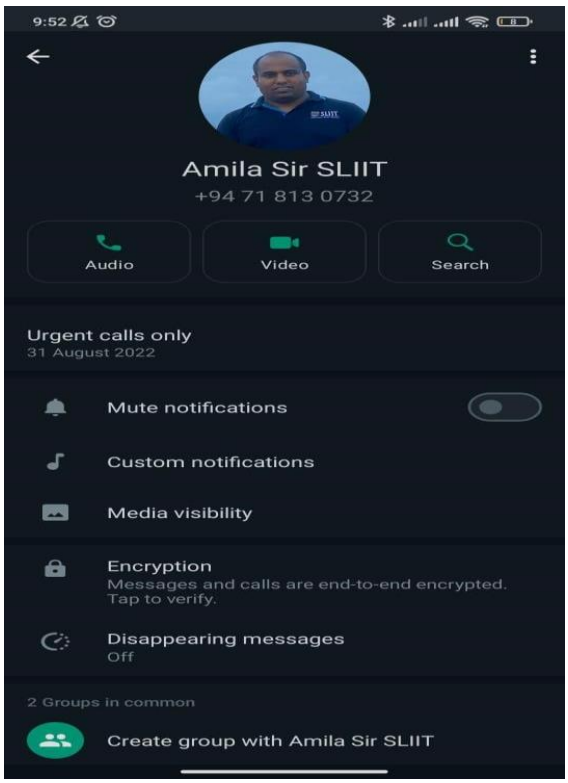
Pending Tasks

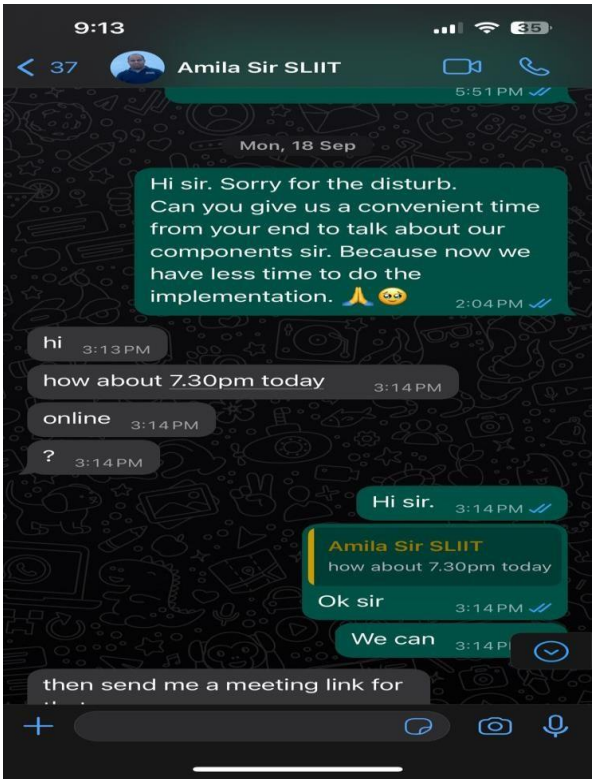


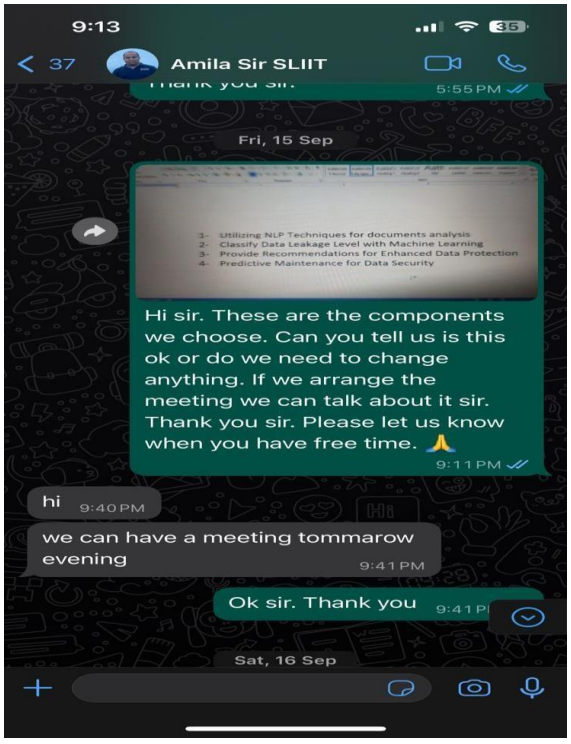
2.2 Team Planner Charts

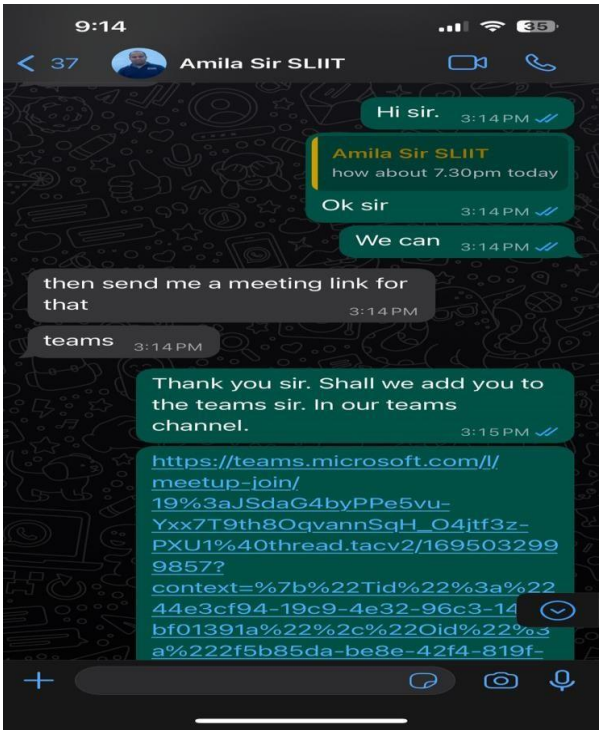


3. WhatsApp chat with Supervisor

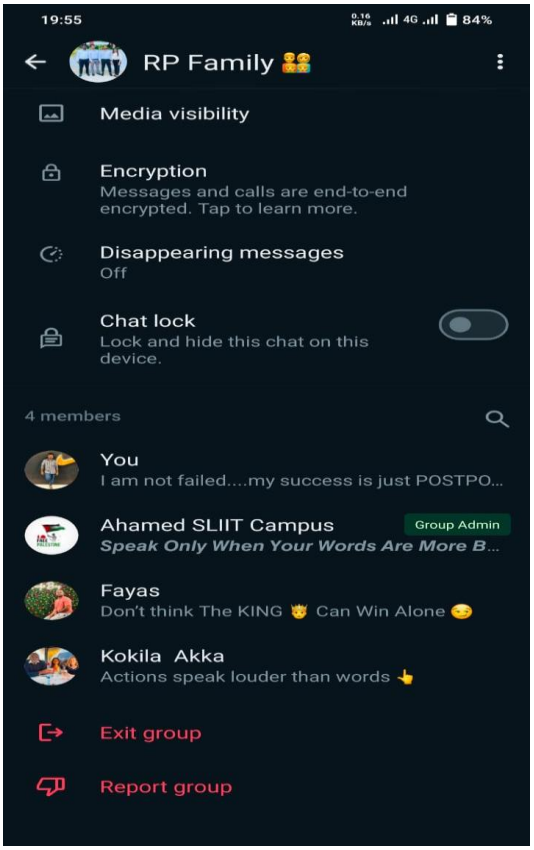


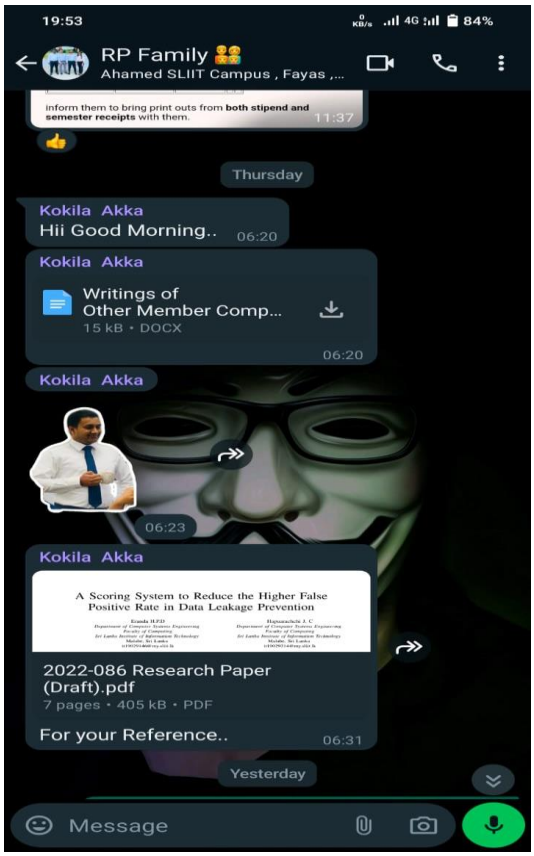


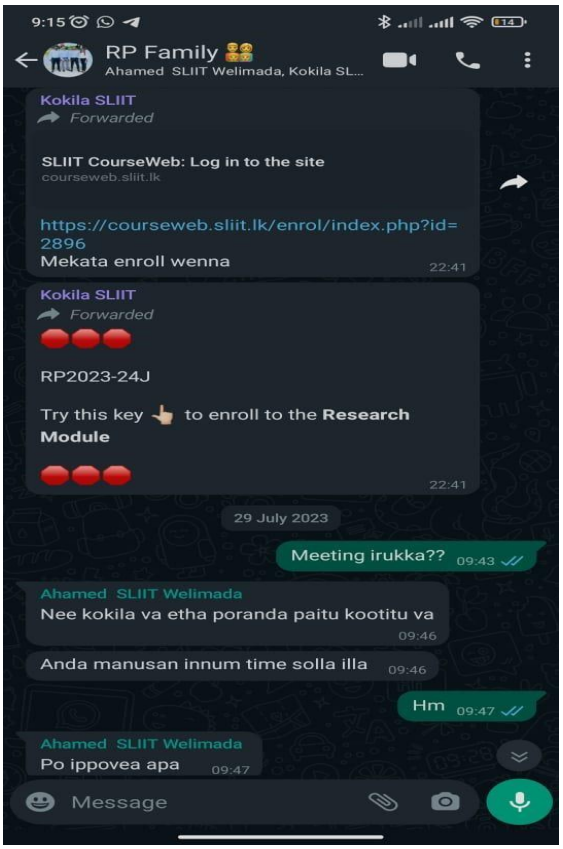


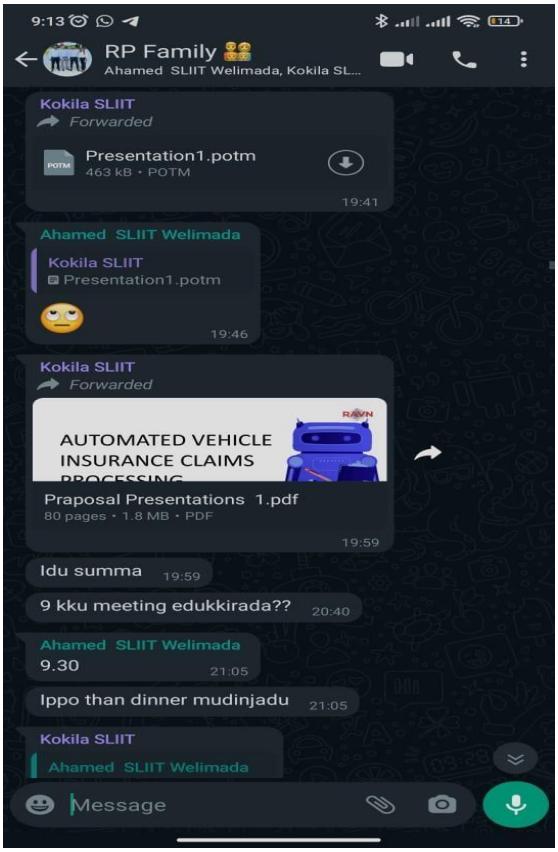


4. WhatsApp Call and Chat with Team









5. Email and planned Teams Events

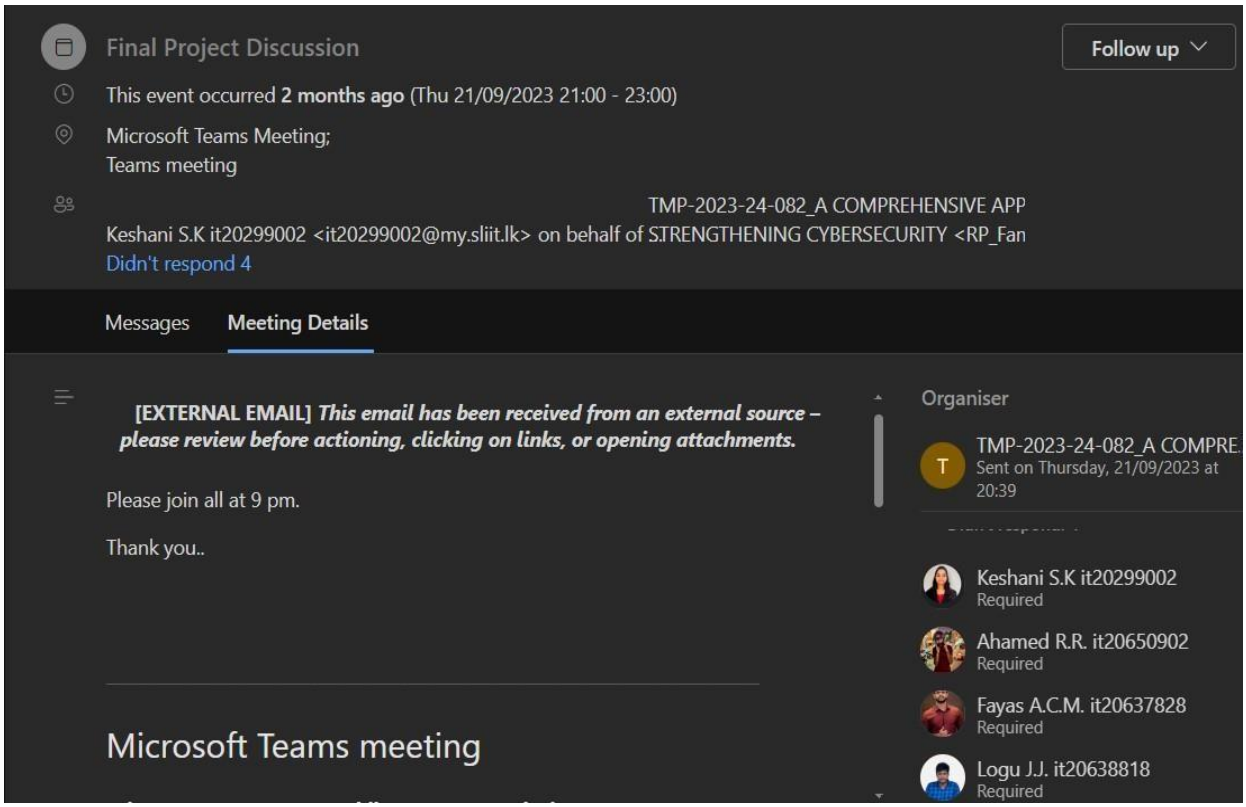


Fig: Planned MS Teams Meeting

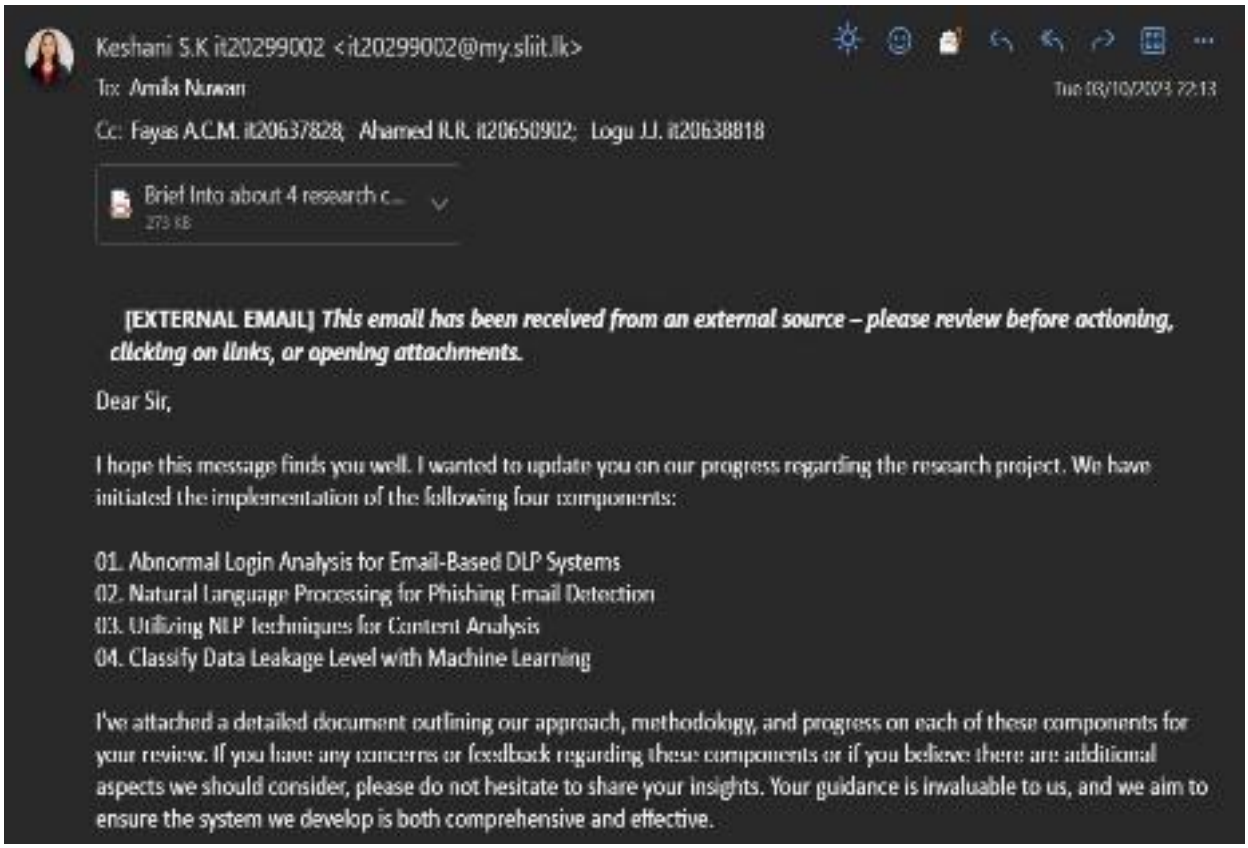


Fig: Email Communication with Supervisor

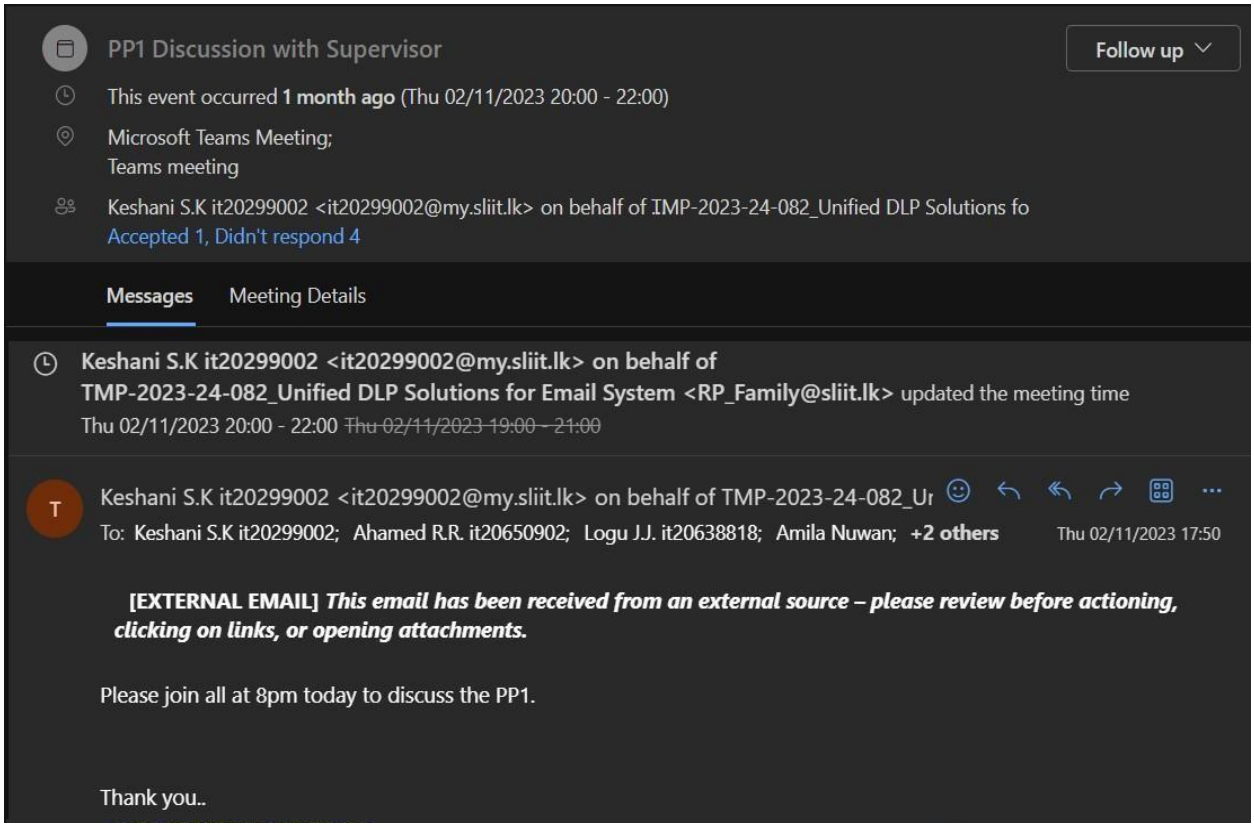


Fig: PP1 Discussion Meeting with Supervisor

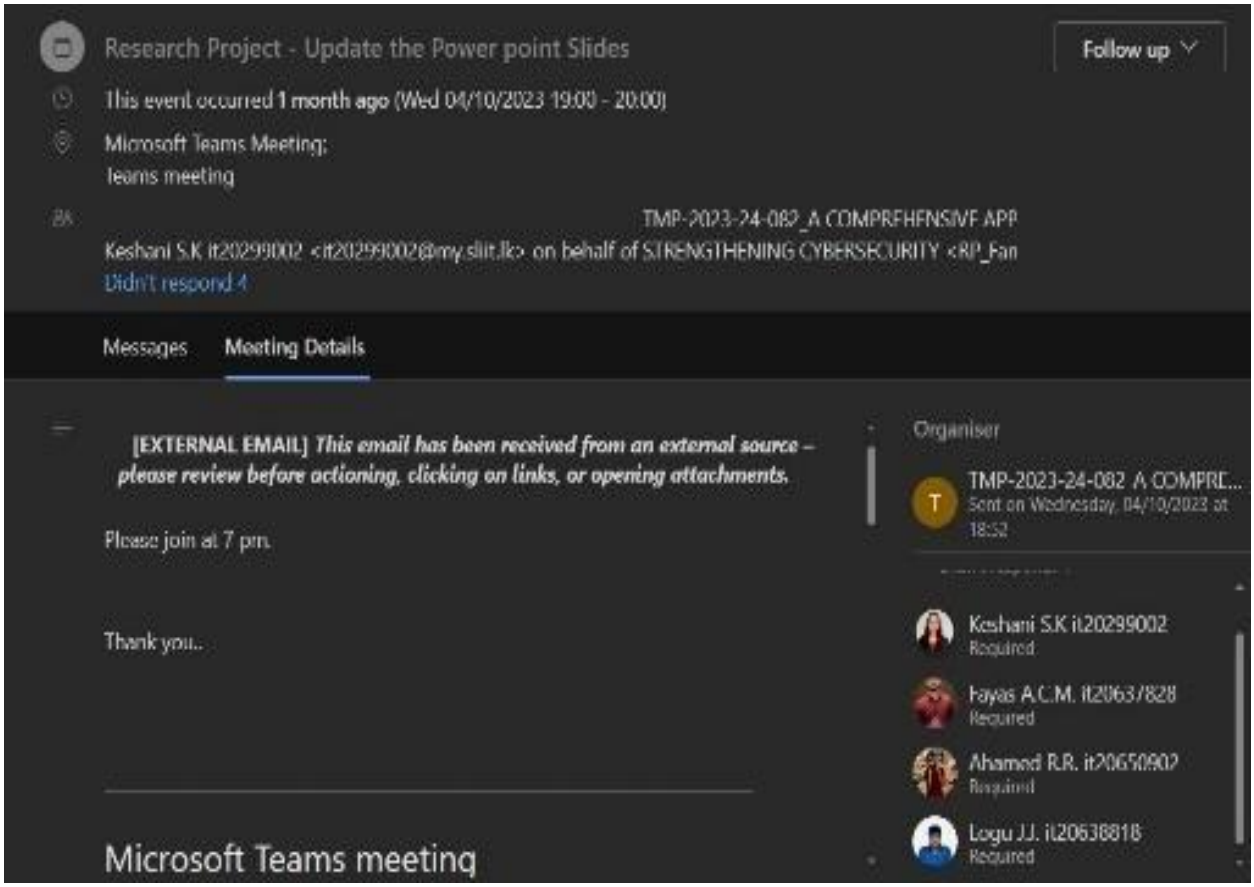
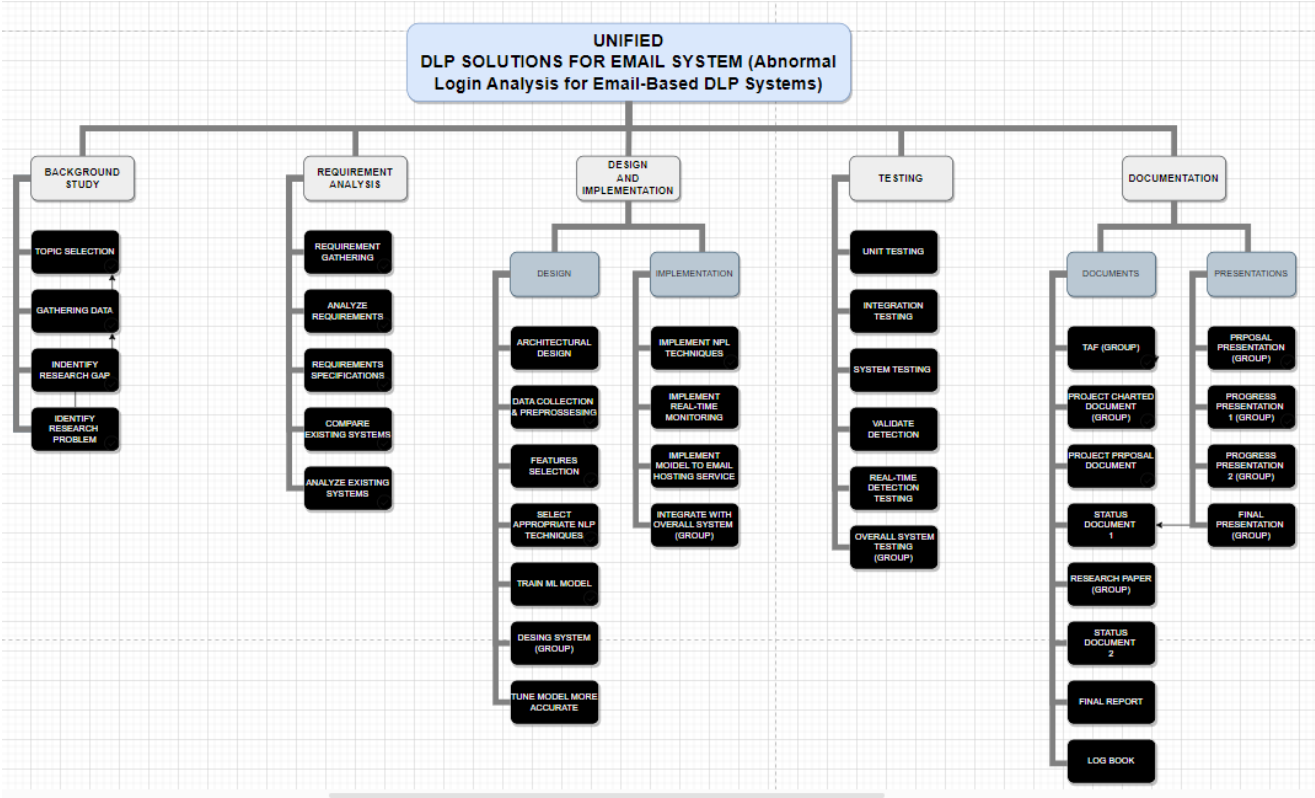


Fig: PP1 Slides Updating Meeting with Team Members

6. Gannt Chart

7. Work Breakdown Structure (WBS)



8. Gitlab Commits

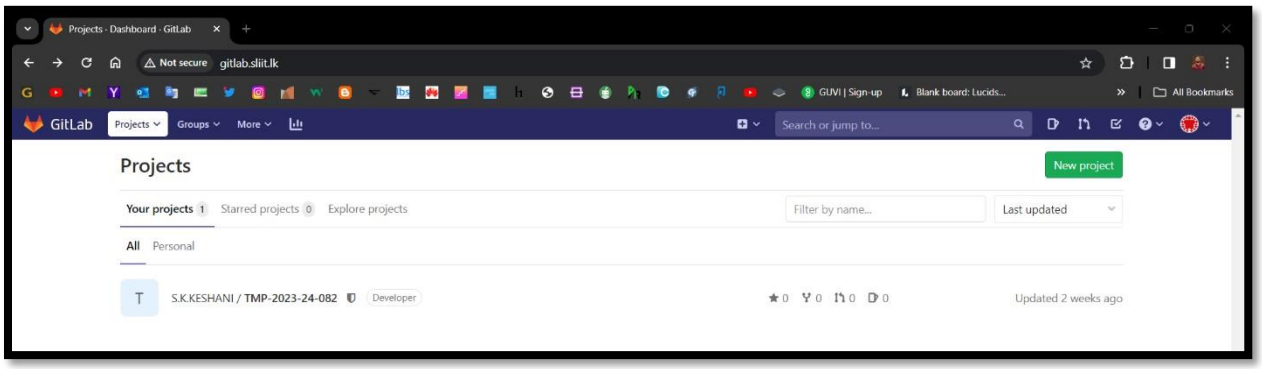


Fig: Project

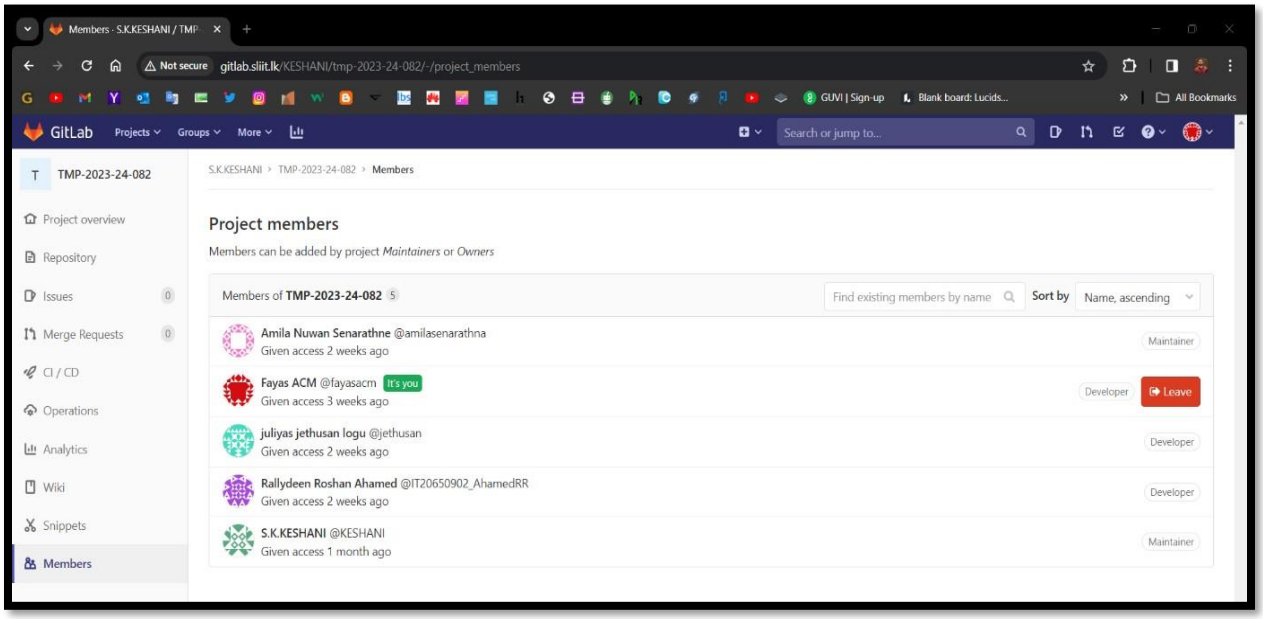


Fig: Team Members and Supervisor

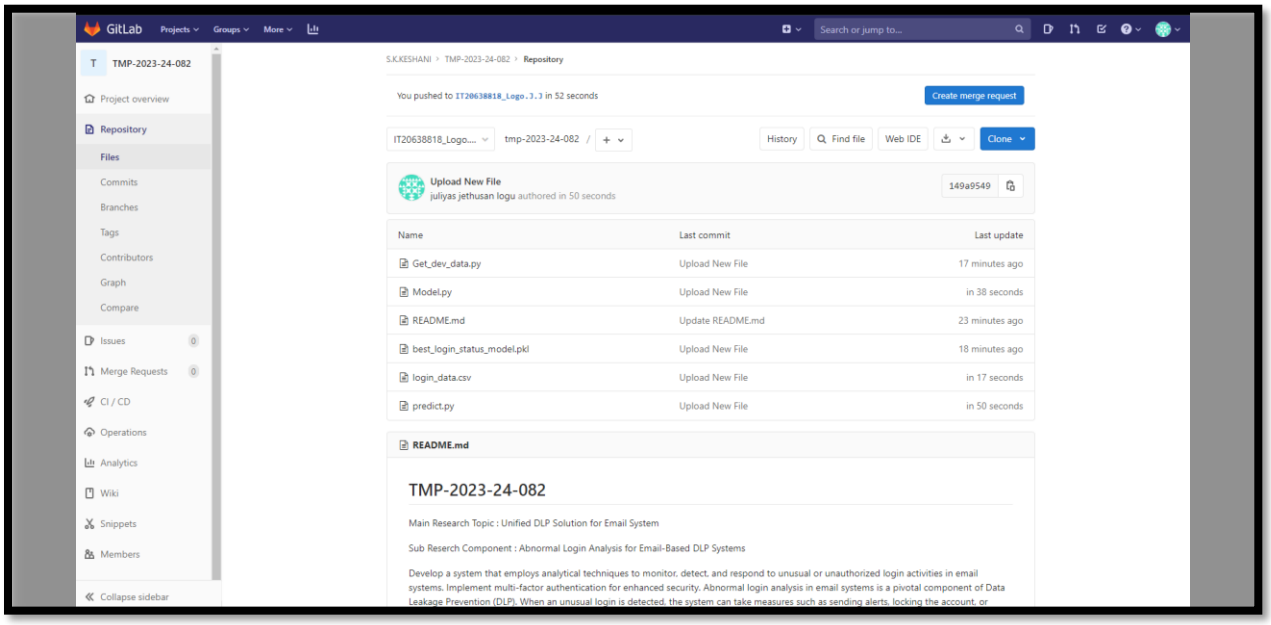


Fig: Code Repository

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