

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

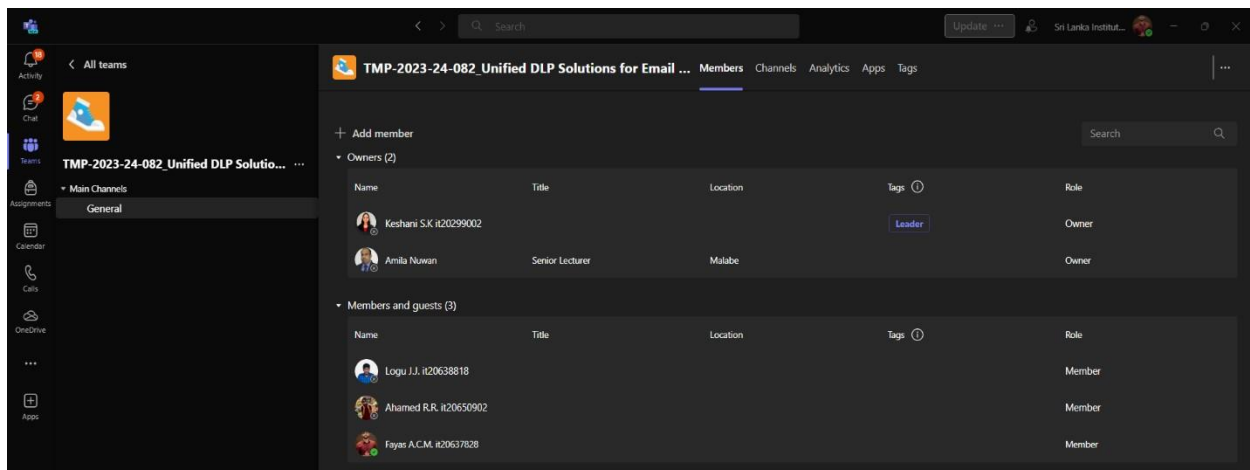
December 2023

Table of Contents

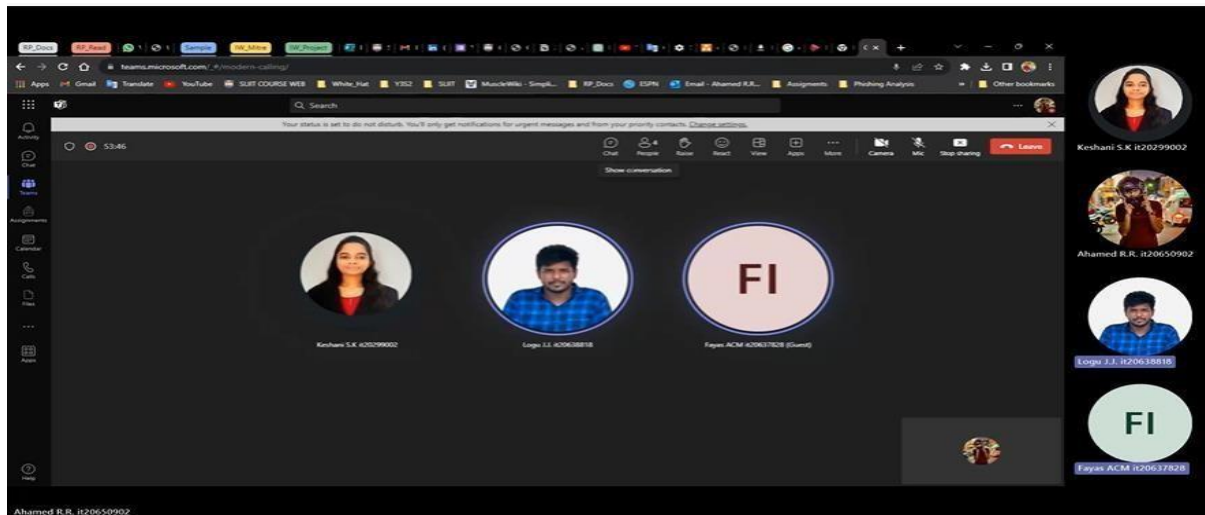
1. Microsoft Teams Details	3
1.1 Team Members	3
1.2 Team Meeting with Group Members	3
1.3 Team meeting with Supervisor.....	5
2. MS Teams Planner	7
2.2 Planner Board	7
2.2 Team Planner Charts.....	8
3. WhatsApp chat with Supervisor	9
4. WhatsApp Call and Chat with Team.....	10
5. Email and planned Teams Events	11
6. Gantt 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






Muhammed Fayas



kokila keshani

2. MS Teams Planner

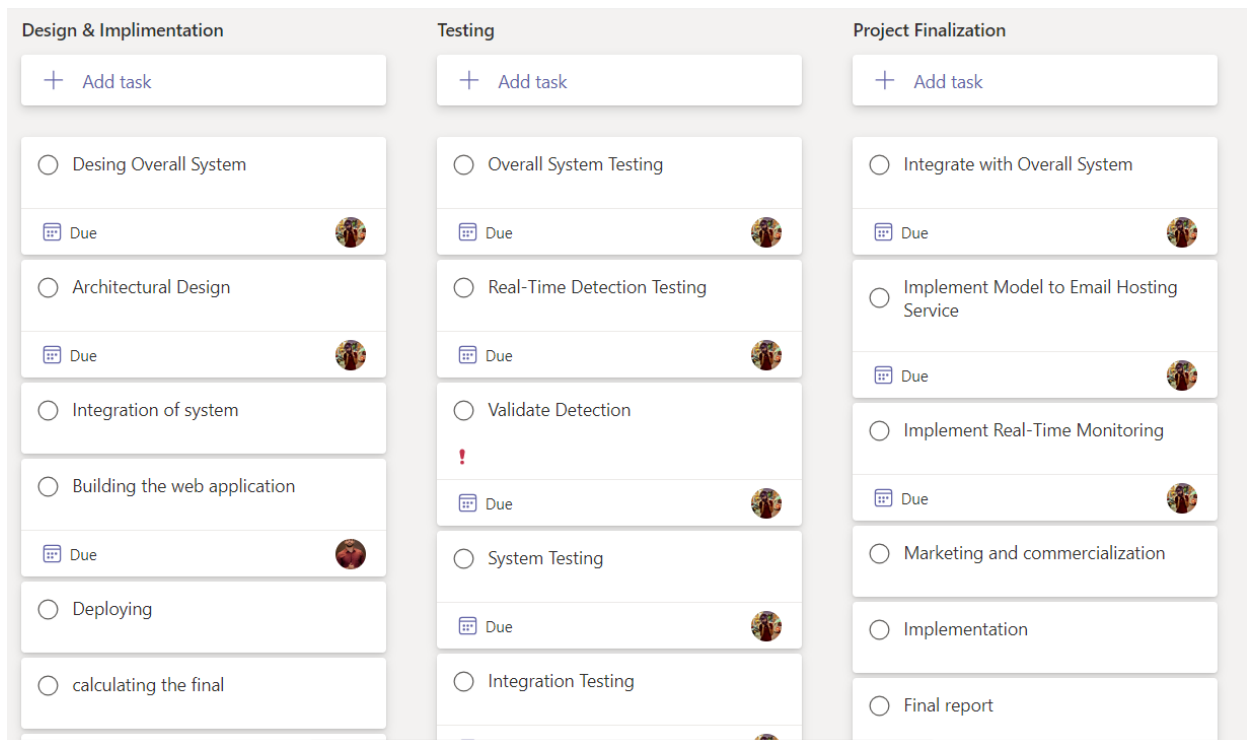
2.2 Planner Board

Completed Tasks

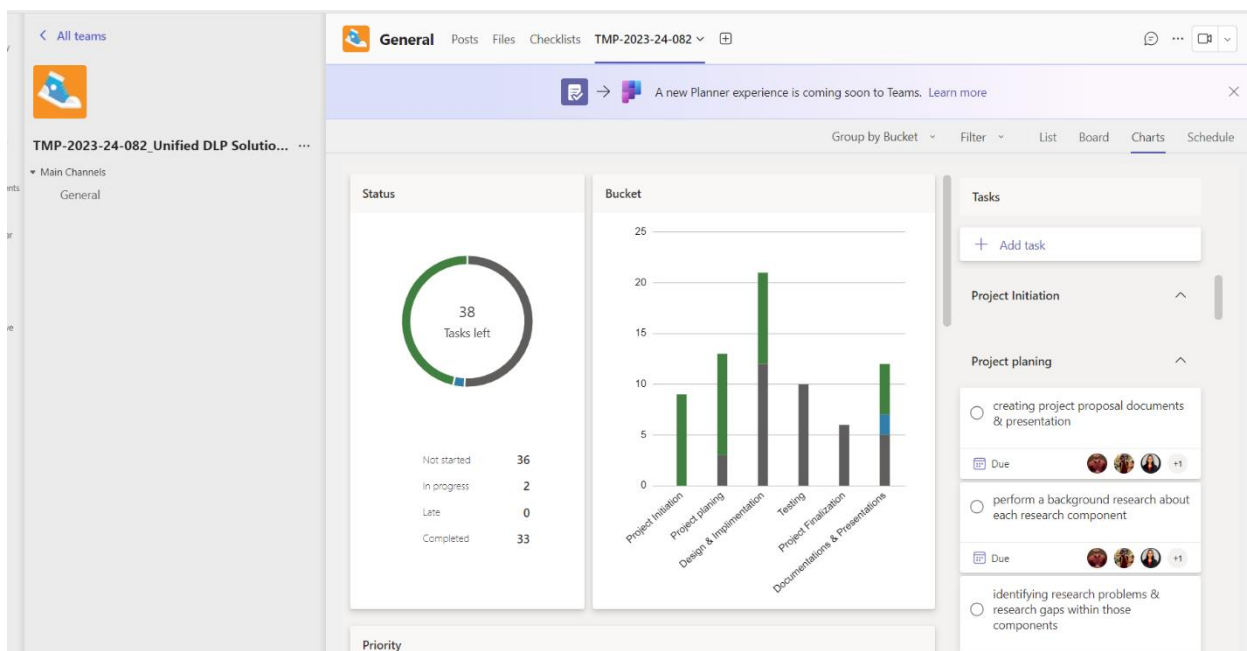
The screenshot displays a MS Teams Planner board with two columns: "Project Initiation" and "Project planning". Each column contains a list of completed tasks, each preceded by a checkmark icon and followed by a "Completed by" status. The tasks are as follows:

Project Initiation	Project planning
+ Add task	+ Add task
Completed by Ahamed R.R. it206...	Completed by Logu J.J. it206388...
✓ Evaluation	✓ creating a gantt chart
Completed by Fayas A.C.M. it206...	Completed by Logu J.J. it206388...
✓ feasibility study	✓ Specifying main objective & sub-objectives
Completed by Logu J.J. it206388...	Completed by Logu J.J. it206388...
✓ Requirement Analysis	✓ Deciding on functional & non-functional requirements
Completed by Logu J.J. it206388...	Completed by Ahamed R.R. it206...
✓ Performing a background study about the topic	✓ Identify the main research problem
Completed by Fayas A.C.M. it206...	Completed by Ahamed R.R. it206...
✓ Selecting a research topic	

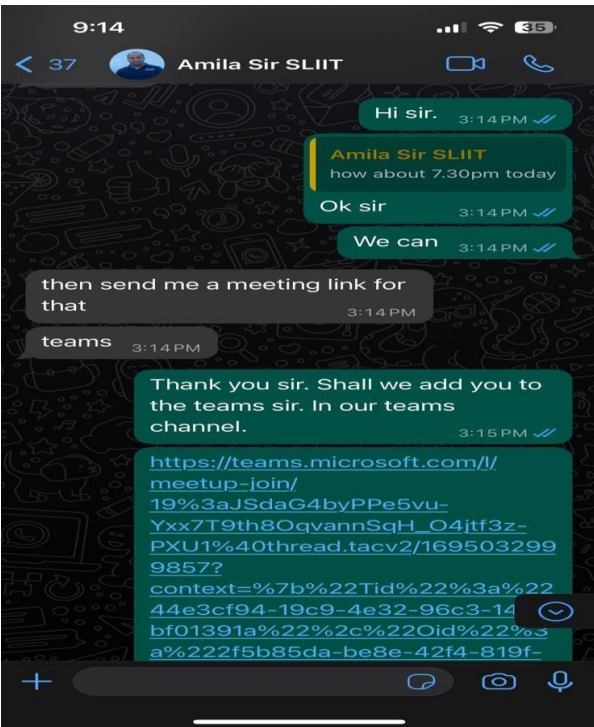
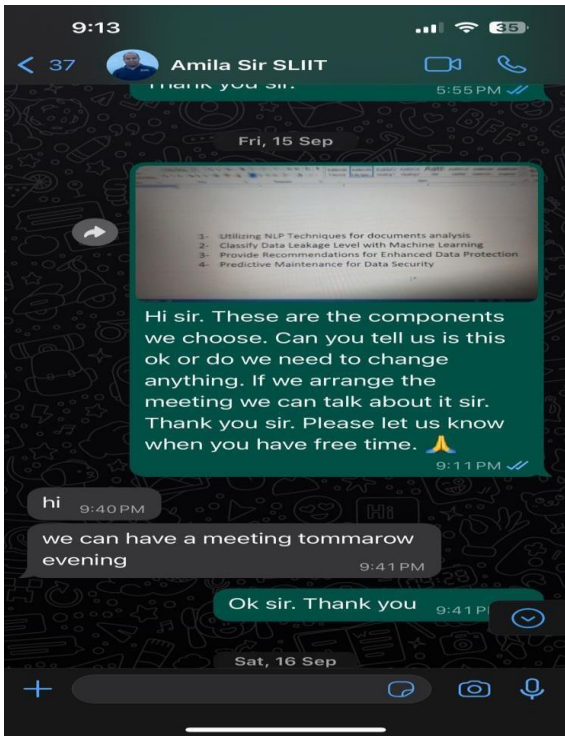
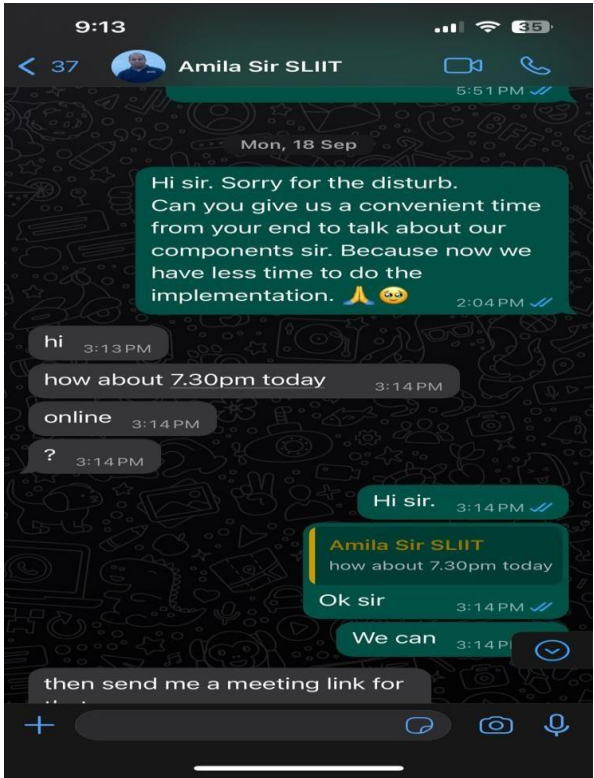
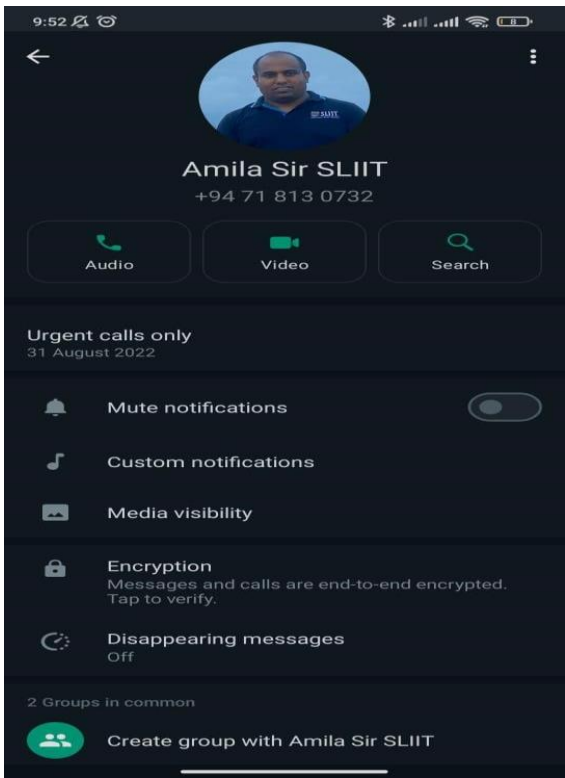
Pending Tasks



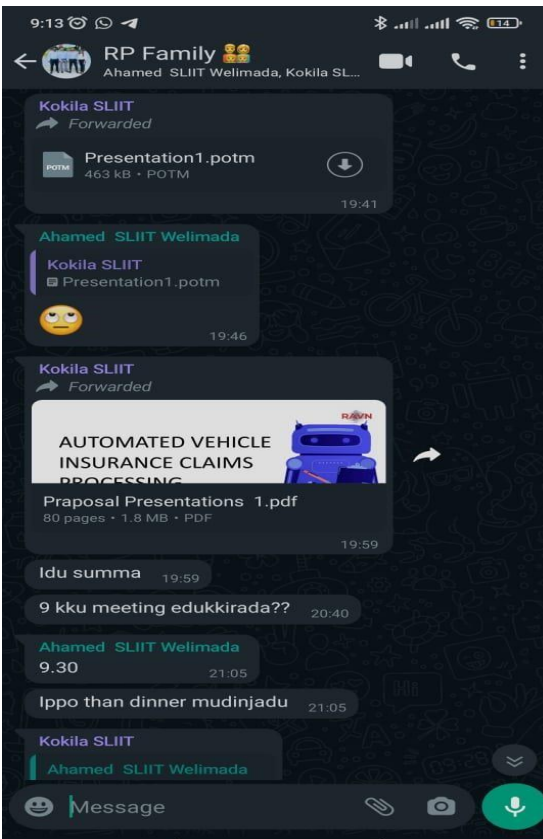
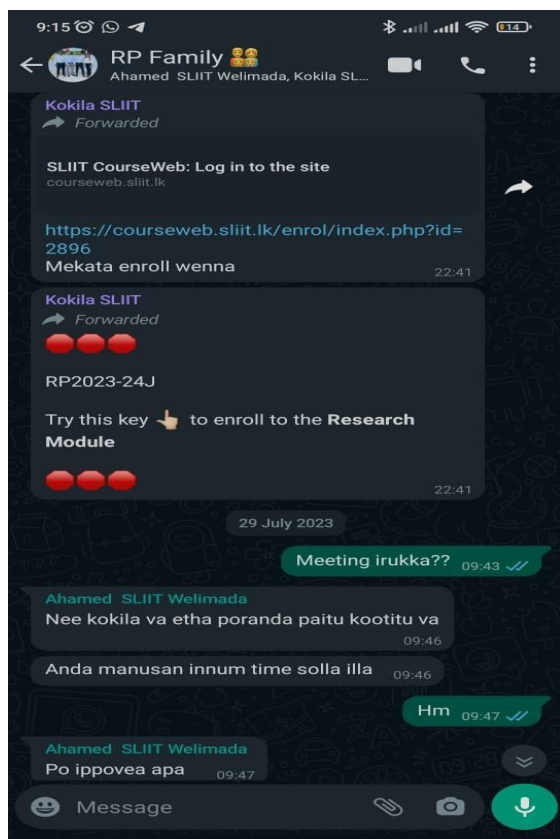
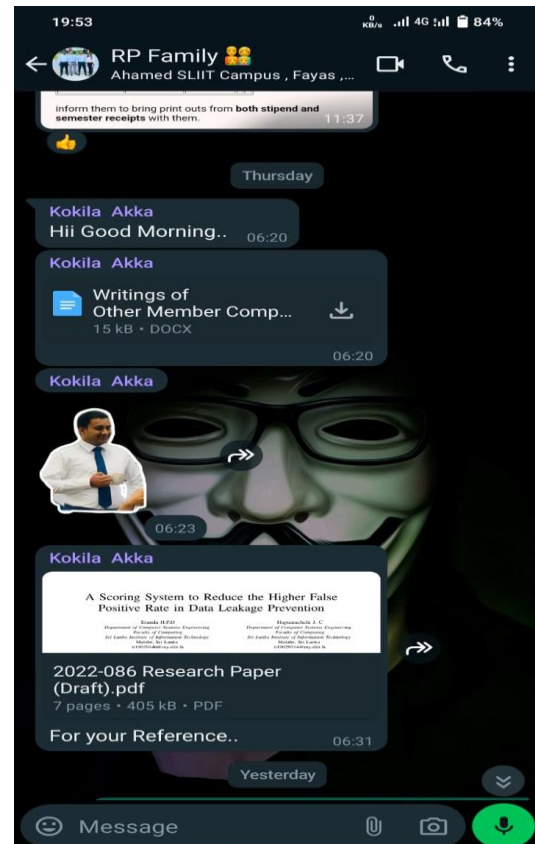
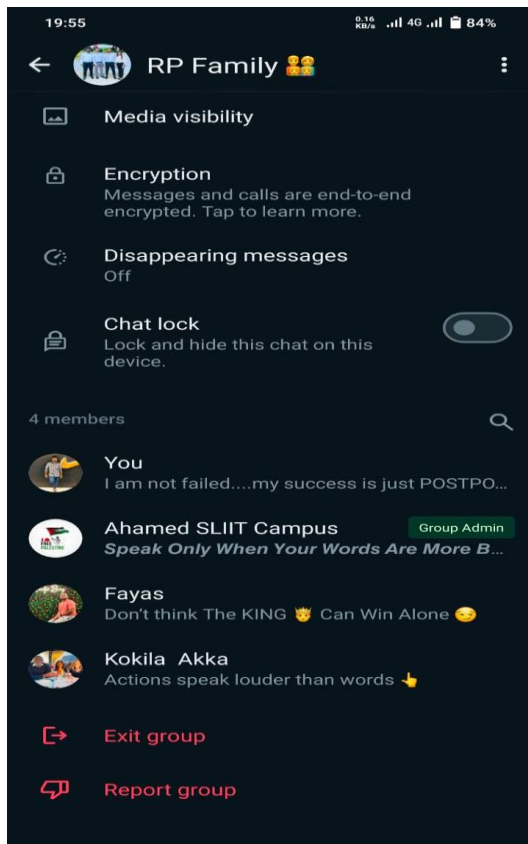
2.2 Team Planner Charts



3. WhatsApp chat with Supervisor



4. WhatsApp Call and Chat with Team



5. Email and planned Teams Events

The screenshot shows a Microsoft Teams meeting invitation titled "Final Project Discussion". It indicates the event occurred 2 months ago on Thursday, 21/09/2023, from 21:00 to 23:00. The meeting is a Microsoft Teams Meeting. The organizer is Keshani S.K. (it20299002) on behalf of STRENGTHENING CYBERSECURITY <RP_Fan>. A note says "Didn't respond 4". The interface has tabs for "Messages" and "Meeting Details". The "Meeting Details" tab is active, showing a warning: "[EXTERNAL EMAIL] This email has been received from an external source – please review before actioning, clicking on links, or opening attachments." Below the warning, it says "Please join all at 9 pm." and "Thank you..". At the bottom, it says "Microsoft Teams meeting". On the right, there is a list of participants under the heading "Organiser":

- TMP-2023-24-082_A COMPRE (Sent on Thursday, 21/09/2023 at 20:39)
- Keshani S.K. it20299002 (Required)
- Ahamed R.R. it20650902 (Required)
- Fayas A.C.M. it20637828 (Required)
- Logu J.J. it20638818 (Required)

Fig: Planned MS Teams Meeting

The screenshot shows an email from Keshani S.K. (it20299002) to Amila Nuwan. The email is dated Tuesday, 08/10/2023, at 22:13. The subject is "Brief Into about 4 research c..." (273 KB). The email body contains a warning: "[EXTERNAL EMAIL] This email has been received from an external source – please review before actioning, clicking on links, or opening attachments." Below the warning, it says "Dear Sir," and "I hope this message finds you well. I wanted to update you on our progress regarding the research project. We have initiated the implementation of the following four components:"

01. Abnormal Login Analysis for Email-Based DLP Systems
02. Natural Language Processing for Phishing Email Detection
03. Utilizing NLP techniques for Content Analysis
04. Classify Data Leakage Level with Machine Learning

The email concludes with: "I've attached a detailed document outlining our approach, methodology, and progress on each of these components for your review. If you have any concerns or feedback regarding these components or if you believe there are additional aspects we should consider, please do not hesitate to share your insights. Your guidance is invaluable to us, and we aim to ensure the system we develop is both comprehensive and effective."

Fig: Email Communication with Supervisor

PP1 Discussion with Supervisor

Follow up

This event occurred 1 month ago (Thu 02/11/2023 20:00 - 22:00)

Microsoft Teams Meeting;
Teams meeting

Keshani S.K it20299002 <it20299002@my.sliit.lk> on behalf of IMP-2023-24-082_Unified DLP Solutions fo
Accepted 1, Didn't respond 4

Messages

Meeting Details

Keshani S.K it20299002 <it20299002@my.sliit.lk> on behalf of
TMP-2023-24-082_Unified DLP Solutions for Email System <RP_Family@sliit.lk> updated the meeting time
Thu 02/11/2023 20:00 - 22:00 Thu 02/11/2023 19:00 - 21:00

T

Keshani S.K it20299002 <it20299002@my.sliit.lk> on behalf of TMP-2023-24-082_Ur

To: Keshani S.K it20299002; Ahamed R.R. it20650902; Logu J.J. it20638818; Amila Nuwan; +2 others

Thu 02/11/2023 17:50

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

Please join all at 8pm today to discuss the PP1.

Thank you..

Fig: PP1 Discussion Meeting with Supervisor

Research Project - Update the Power point Slides

Follow up

This event occurred 1 month ago (Wed 04/10/2023 19:00 - 20:00)

Microsoft Teams Meeting;
teams meeting

TMP-2023-24-082_A COMPREHENSIVE APP
Keshani S.K it20299002 <it20299002@my.sliit.lk> on behalf of STRENGTHENING CYBERSECURITY <RP_Fan
Didn't respond 4

Messages

Meeting Details

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

Please join at 7 pm.

Thank you..

Organiser

T

TMP-2023-24-082_A COMPRE...

Sent on Wednesday, 04/10/2023 at 18:52

Keshani S.K it20299002

Required

Fayaz A.C.M. it20637828

Required

Ahamed R.R. it20650902

Required

Logu J.J. it20638818

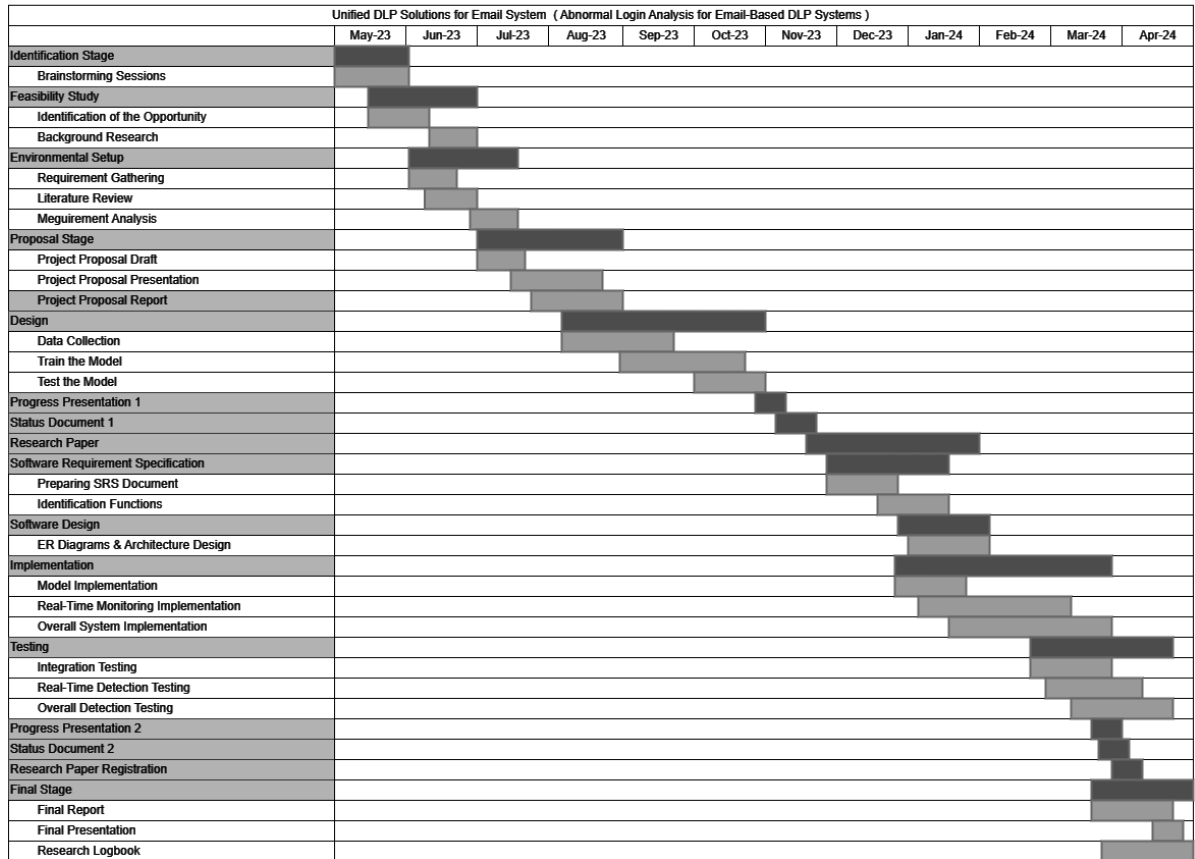
Required

Microsoft Teams meeting

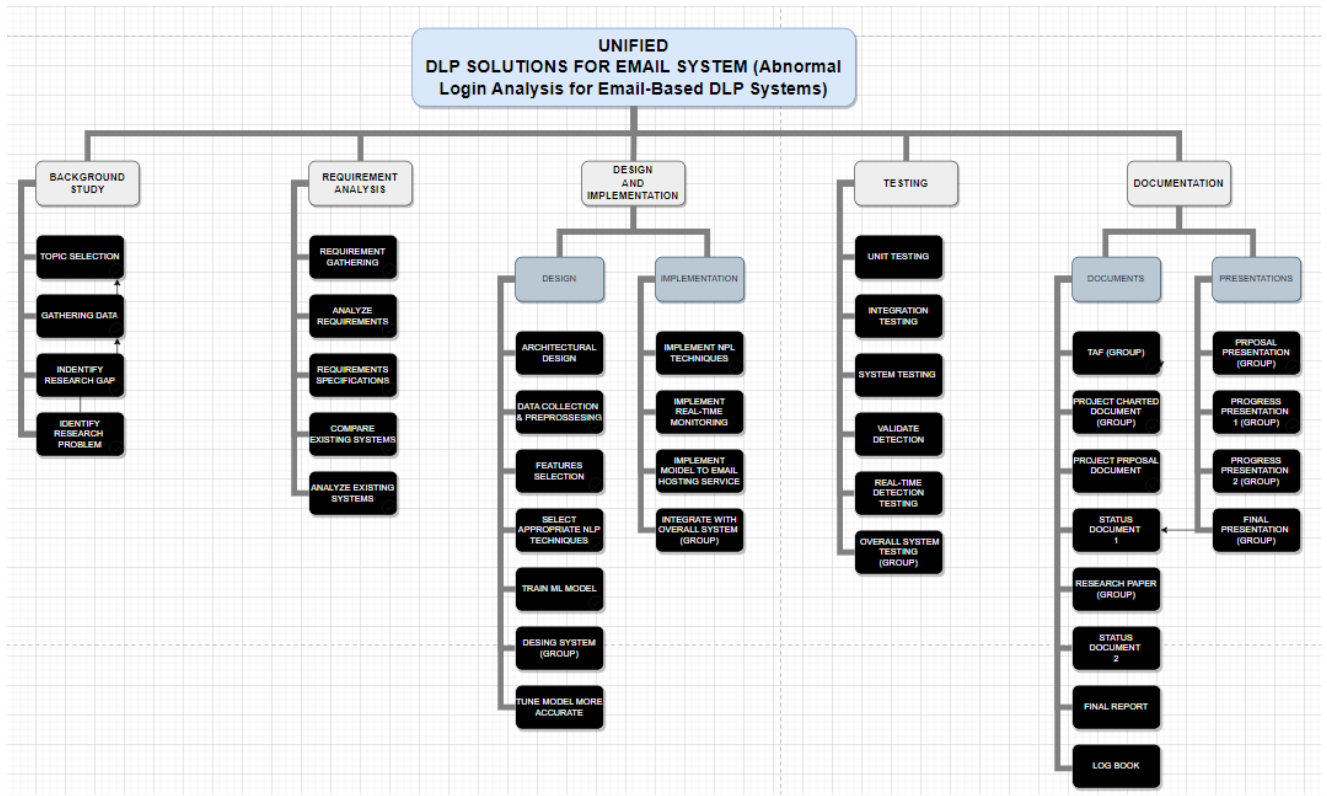
12 | Page

Fig: PP1 Slides Updating Meeting with Team Members

6. Gantt Chart



7. Work Breakdown Structure (WBS)



8. Gitlab Commits

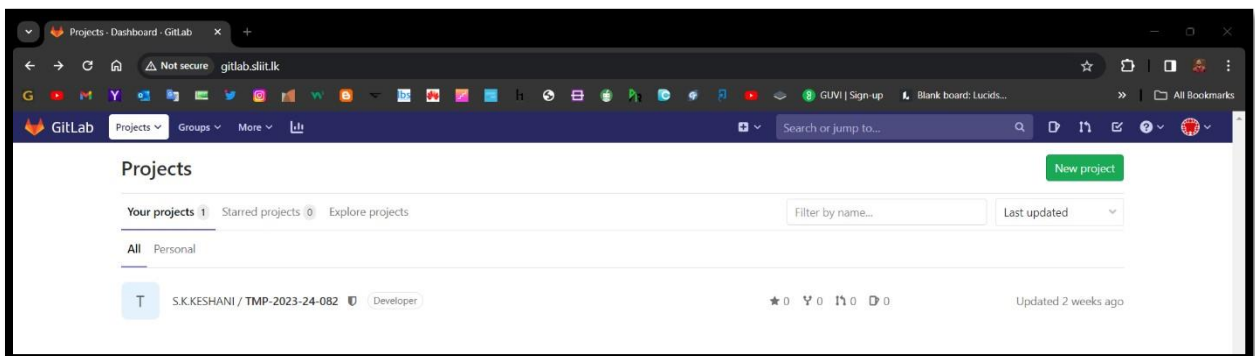


Fig: Project

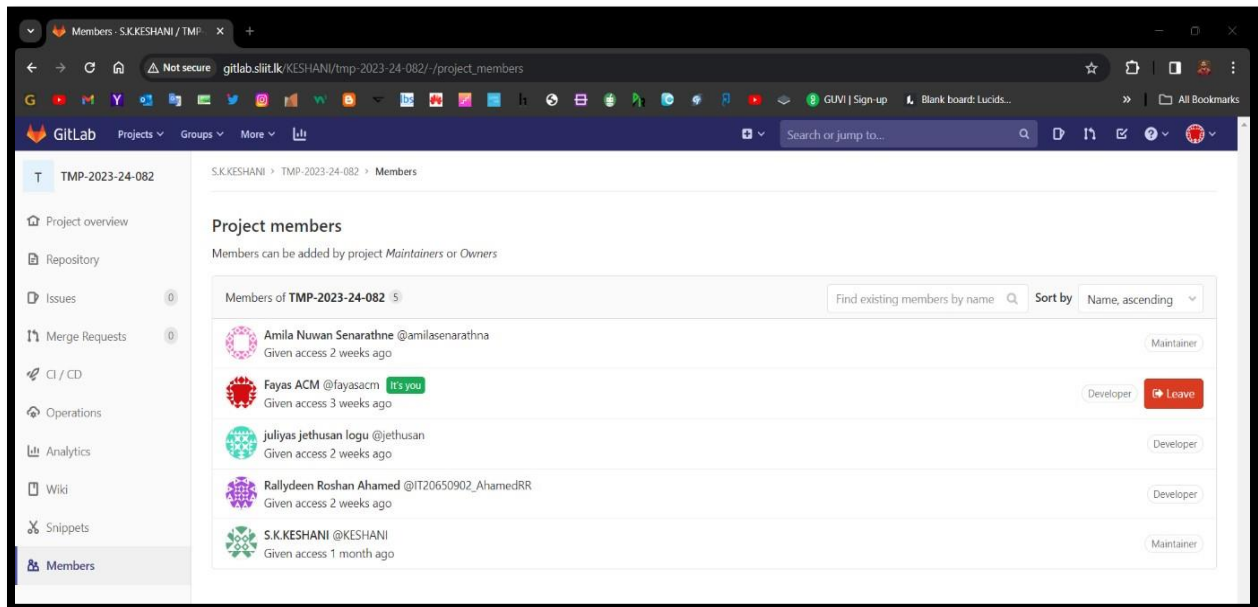


Fig: Team Members and Supervisor

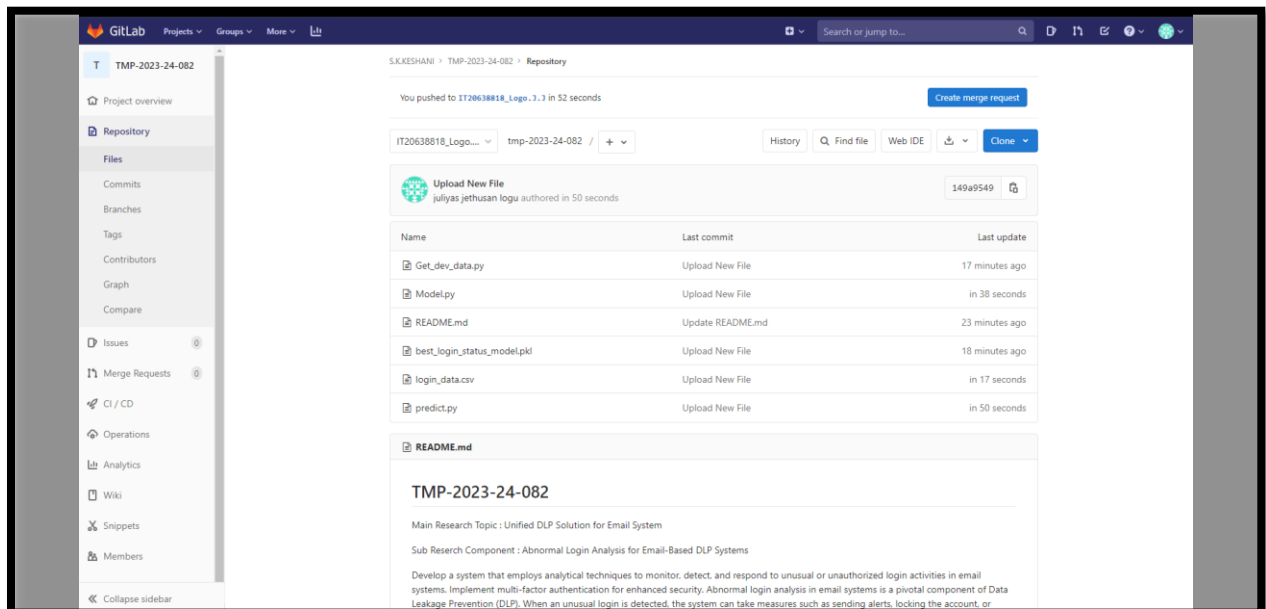


Fig: Code Repository

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