Y24 OPEN SOURCE ENGINEERING

BY

STUDENT : KODURI KEERTHANA

ID NO: 2400033253

DEPARTMENT: B.TECH, CSE-HTE

KL UNIVERSITY

1. LINUX DISTRIBUTION

A Linux distribution is a ready-made version of the Linux operating system that includes system tools, software, updates, and a desktop environment. Examples include Ubuntu, Fedora, and Kali Linux.

Ubuntu is one of the most popular and beginner-friendly Linux operating systems. It is completely free, open-source, and designed to be simple for everyday users as well as students and developers. Ubuntu provides a clean interface, regular security updates, and a huge library of software that you can install easily from its Software Center. Because it runs smoothly even on older laptops and is free from viruses, many people prefer Ubuntu for learning and daily use.

Ubuntu is widely used for programming, web development, cybersecurity learning, and running self-hosted servers. It supports many programming languages and offers powerful tools that make coding easier. Many companies also use Ubuntu on cloud platforms and servers because it is stable and secure. Whether you want to browse the internet, write documents, learn Linux commands, or develop applications, Ubuntu provides a fast, safe, and reliable environment.

2. ENCRYPTION AND GPG

ENCRYPTION

Encryption is the process of converting normal readable data into a secure, unreadable form so that only the intended person can access it. It protects our files, messages, and digital identity from hackers or unauthorized users. Encryption is widely used today in emails, online banking, WhatsApp chats, and even in storing passwords. It ensures privacy, security, and trust while sharing or storing information on the internet.

GNU PRIVACY GUARD (GPG)

GPG (GNU Privacy Guard) is a free and open-source tool used to encrypt data and digitally sign documents or emails. It uses a pair of keys: a public key for others to send you encrypted data, and a private key that only you can use to decrypt it. Students and developers use GPG to securely send emails, verify software authenticity, and protect important files. It is one of the most common tools used in Linux systems for privacy and strong encryption.

3. SENDING ENCRYPTED EMAIL

Sending an encrypted email means your message is protected so that only the intended person can read it. Even if someone tries to intercept the email during transfer, they cannot understand the content because it is converted into unreadable encrypted text. This ensures privacy and safety when sharing sensitive information such as passwords, personal details, or important documents.

To send an encrypted email using GPG, both you and the receiver exchange your public keys. You use the receiver's public key to encrypt the email before sending it, and they use their private key to decrypt and read it. This method provides end-to-end security, meaning only the correct person can unlock the message. Students, developers, and professionals commonly use this for secure communication in Linux environments.

4. PRIVACY TOOLS

Privacy Tools from Prism-Break

1. Tor (Anonymizing Network)

Tor helps protect your identity by routing your internet traffic through multiple volunteer-run servers. This makes it very difficult for anyone to track your IP address or online activity. It is widely used for safe and private web browsing.

2. WireGuard (VPN Tool)

WireGuard is a fast and modern VPN protocol that encrypts your internet connection. It keeps your online activity private by hiding your real IP address and protecting your data from attackers. It is lightweight, secure, and easy to configure on Linux systems like Ubuntu.

3. KeePassXC (Password Manager)

KeePassXC securely stores all your passwords inside an encrypted vault protected by one master password. You only need to remember one password while the tool handles the rest safely. It helps prevent password theft and encourages stronger, unique passwords.

4. Nextcloud (Self-Hosted File Storage)

Nextcloud allows you to store files, photos, and documents on your own personal server instead of third-party cloud services. This gives you full control over your data and keeps it private. It also supports secure file sharing, syncing, and collaboration.

5. Thunderbird (Email Client)

Thunderbird is a secure, open-source email application that supports encrypted email using GPG. It helps keep your messages private and protected from unauthorized access. It also includes strong spam filtering and works smoothly on Ubuntu.

5. SELF-HOSTED TASK MANAGEMENT SERVER

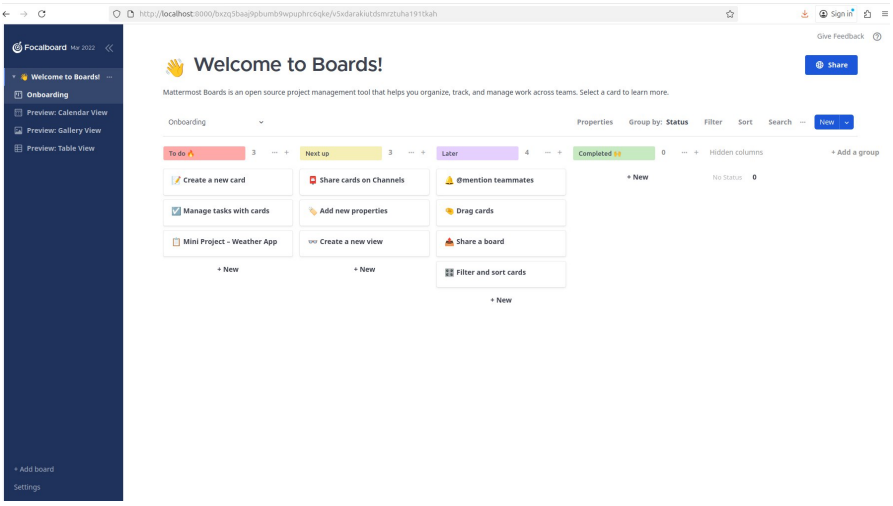
Self-Hosted Task Management Server – About and Installation

Self-Hosted Task Management Server

A self-hosted task management server allows you to organize tasks, to-do lists, and projects on your own system instead of relying on cloud services like Google Tasks, Microsoft To-Do, or Trello. Self-hosting ensures full control over your data, improves privacy, and keeps all your task information secure on your own server.

My Self-Hosted Server: Task Management on Ubuntu

This server is designed to manage personal or team tasks efficiently. It allows you to create tasks, to-do lists, and boards, track progress, set priorities, and collaborate securely. By hosting it on your own Ubuntu server, you retain complete control over the data, access permissions, and customizations.



Installation Steps for Task Management Server on Ubuntu 24.04

1. Update your system packages:

   ```
   sudo apt update
   sudo apt upgrade -y
   ```

2. Install required dependencies such as Node.js, MongoDB, or PostgreSQL depending on the server software:

   ```
   sudo apt install nodejs npm mongodb -y
   ```

3. Download or clone the task management server software from its official repository:

   ```
   git clone <repository-link>
   cd <repository-folder>
   npm install
   ```

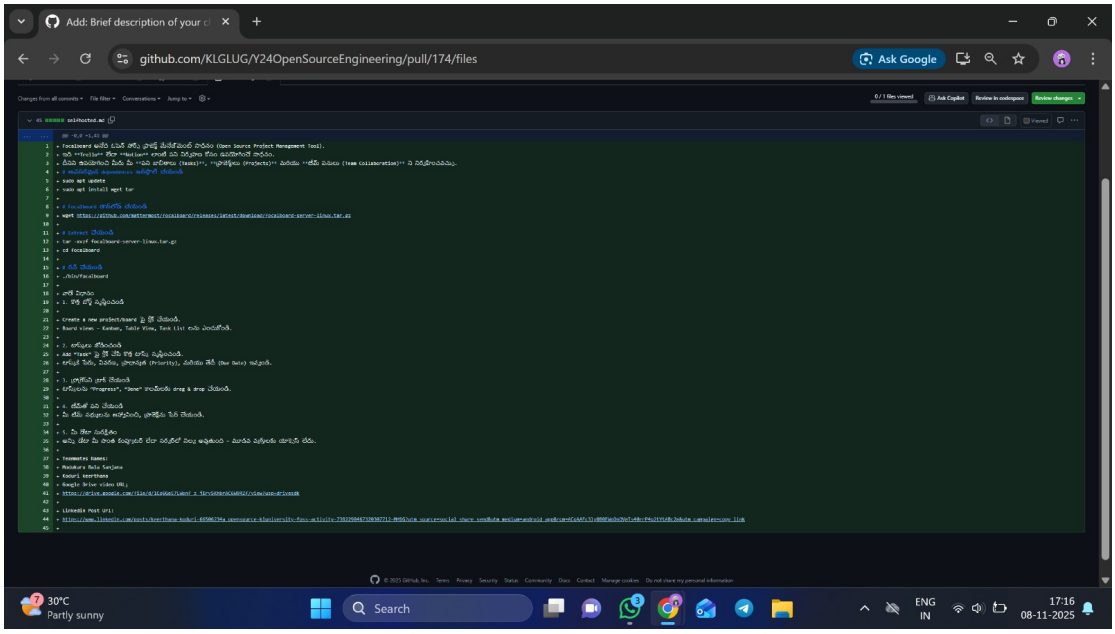
4. Start the server:

```
npm start
```

5. Open the task management interface in your browser using your server's IP (for example: http://localhost:3000 or http://your-server-ip:3000) and set up your first project and to-do lists.

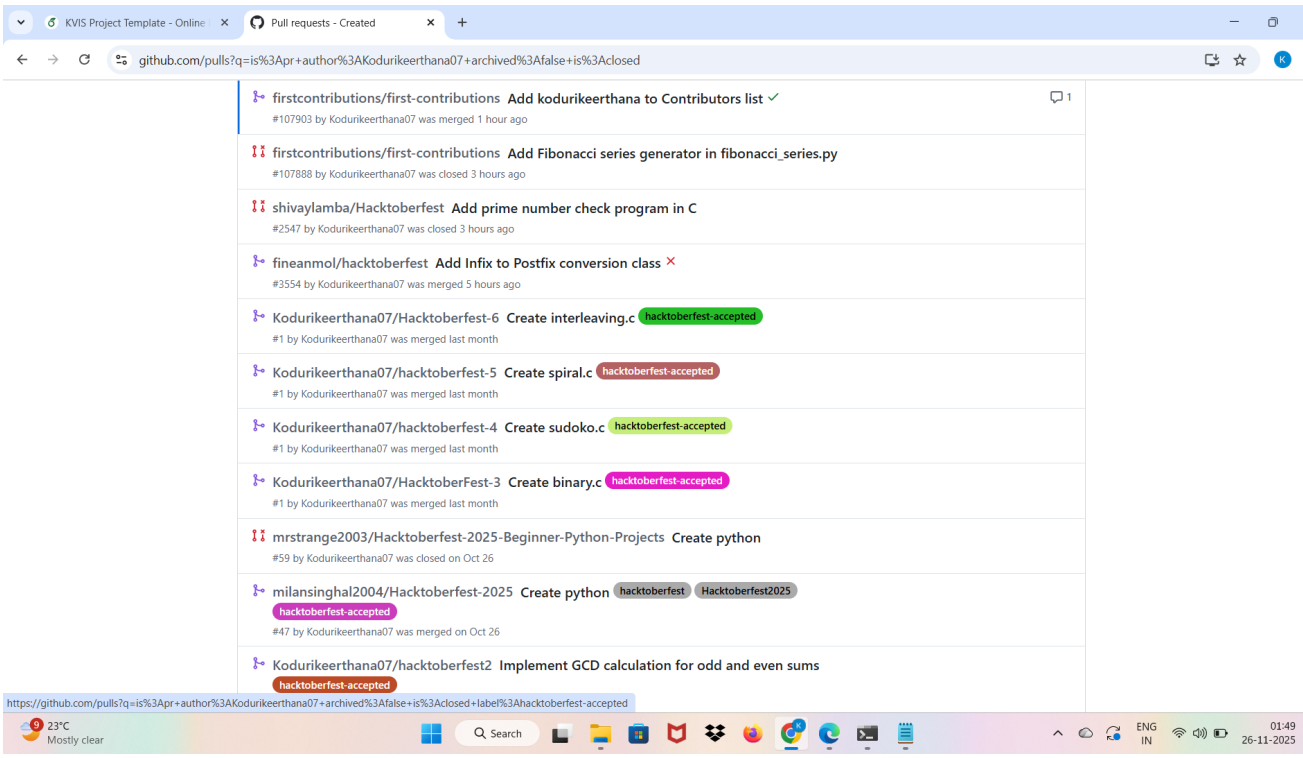
6. Optional: Configure a reverse proxy with Nginx and SSL to make your server accessible securely from the internet.

Localized (Translated) Document – Telugu



Self-Hosted Poster

0.1 My Merged Pull Requests



8. LinkedIn Posts

0.1.1 Self Hosted Server – BookStack

Click here to view the LinkedIn Post

0.1.2 PRs Merged

Click here to view the LinkedIn Post

0.1.3 Blog Post

Click here to view the LinkedIn Post