Department Of HTE
Open Source Engineering

Name : Manikonda Anjali
IDNo : 2400032163
Branch: CSE

November 2025

Contents

1 About the Linux Distro used:

I used Ubuntu 22.04 LTS, a popular open-source operating system based on Debian. It is widely used by developers, students, and organizations due to its stability, large software repository, and community support. Ubuntu provides a user-friendly interface, regular updates, and strong security features. It is commonly used for programming, cloud servers, cybersecurity, and open-source development.Ubuntu is one of the most stable and widely supported Linux distributions, especially for development and server-related tasks.
Reason for choosing this distribution are it is long-term support (LTS), strong community support, stable for development, compatibility and ease of use. The primary package manager used is:APT (Advanced Package Tool) Command examples: sudo apt update, sudo apt install ¡package-name¿ sudo apt upgrade
I used the default GNOME 42 desktop environment, known for its clean interface and productivity-focused design.Ubuntu 22.04 ships with the Linux 5.15 kernel, offering improved performance and hardware support.

2 Encryption and GPG:

In open source engineering, encryption ensures secure communication, protects sensitive data, and verifies the authenticity of code contributions. GPG (GNU Privacy Guard) is an encryption tool that provides secure communication and file protection. It uses public-key cryptography, where each user has a public key (shared with others) and a private key (kept secret).It is widely used for secure emails, software signing, and open-source security. GPG allows to:

-Encrypt files and messages

-Sign documents to verify identity

-Ensure confidentiality and integrity

-GPG (GNU Privacy Guard):

GPG implements the OpenPGP standard and is commonly used in open source projects. It allows developers to, generate encryption key pairs, encrypt or decrypt files, sign git commits or tagsand verify the authenticity of software releases.To create a key pair: gpg –full-generate-key,

3 Sending Encrypted Email:

Sending encrypted email means securing your message so only the intended receiver can read it. This is done using GPG/PGP encryption, which protects your communication from hackers, trackers, and unauthorized access.
-Encrypted Email Is Used to:

- Protects private information
- Prevents hacking and unauthorized access
- Ensures secure communication in open-source projects
- Meets privacy standards and good security practices

-Encrypted email uses asymmetric encryption, which involves two keys:

1. Public Key:-

- Shared with others
- Used to encrypt a message

2. Private Key:-

- Kept secret by the user
- Used to decrypt messages
- Used to digitally sign outgoing mail

So, when you send an encrypted email,you use the receiver's public key to encrypt the message, receiver uses their private key to decrypt it.

4 Five Privacy Tools (from prism-break.org):

- F-Droid - Open Source App Store for Android
- Nextcloud - self-hosted storage
- Tor Browser - Anonymous Browsing
- Signal - Secure messaging
- Tutanota - Encrypted Email

5 Open Source License used:

The license I used GNU Affero General Public License (AGPL) v3. The GNU AGPL v3 is a strong copyleft open-source license designed to ensure that software and any modifications remain free and accessible to all users.

This license prevents companies from taking open-source code, modifying it, and running it as an online service without giving the improvements back to the community. AGPL is chosen when developers want to ensure transparency even for cloud-server software, prevent closed-source commercialization of web apps, protect community contributions and encourage sharing of improvements.

It is widely used for web apps, servers, and cloud-based open-source tools. It allows commercial use, but the code must stay open when deployed publicly. Developers choose AGPL when they want maximum openness and sharing.

6 Self-hosted Server-About and Installation

I hosted a Nextcloud server which is an open-source, self-hosted cloud platform that lets us to store, sync, and share files securely. It works like Google Drive or Dropbox but with one major advantage is we can fully control your data because it runs on your own server. It also provides additional tools such as calendars, contacts, notes, video calls, and collaboration apps, making it suitable for personal, academic, and organizational use.

Nextcloud supports file sharing, collaborative document editing, calendars, contacts, video calls, and integrates well with Linux servers. Nextcloud is lightweight, scalable, and ideal for universities, developers, open-source communities, and individuals who want a secure personal cloud.

The installation of a Nextcloud server involves setting up a secure, self-hosted cloud platform that allows users to store, sync, and access files from any device. The process begins by installing a web server such as Apache, along with PHP and required extensions. After that, a database server like MariaDB or MySQL is configured to store Nextcloud data.

Once the environment is ready, the Nextcloud package is downloaded "http://localhost/nextcloud", extracted into the web directory, and proper file permissions are assigned. Finally, the setup is completed through a web-based installer where the admin account, database details, and storage configuration are provided. This installation gives full control over personal data while offering features like file sharing, calendar sync, contacts, collaboration tools, and secure access across devices.

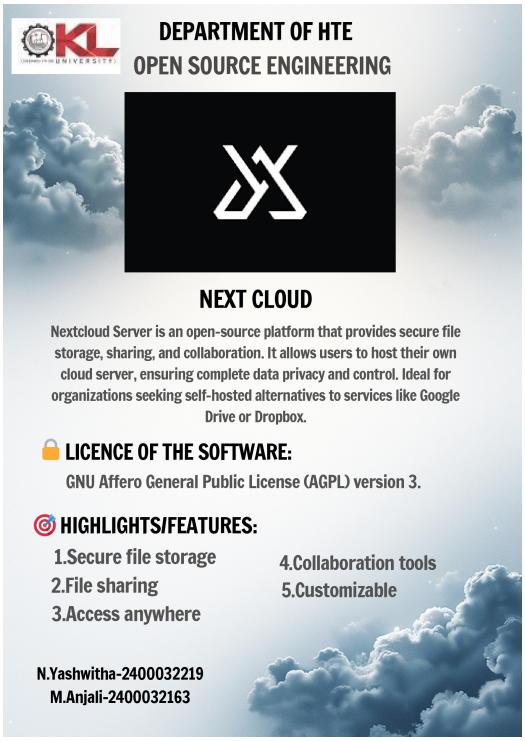

Figure 1: Next cloud server poster

7 Open Source Contributions (PRs):

While creating my Pull Request (PR), I gained hands-on experience with several essential Git commands such as git clone, git checkout -b, git add, git commit, and git push. Understanding how these commands work together helped me manage branches efficiently and contribute to open-source projects effectively. After submitting the PR, I also received automated emails indicating issues in my initial submission, including changes that were not approved or merged. These reviews helped me identify mistakes and guided me to improve my contribution.

Based on the feedback, I fixed an important documentation issue in the repository. The project lacked a clear introduction section, making it difficult for new contributors to understand the purpose and overall goals of the project. To address this, I added a well-structured "Introduction" section to the README.md, explaining the project context and helping future contributors get started more easily. Additionally, I corrected formatting inconsistencies by adjusting heading levels and improving documentation clarity.

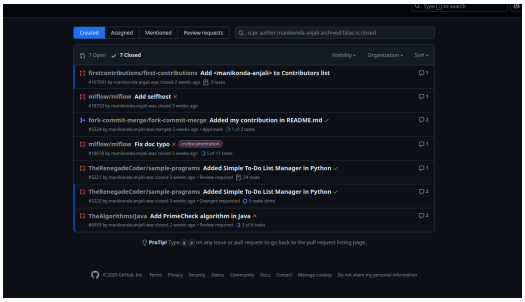

Figure 2: PR's raised

8 LinkedIn Posts

- Self-hosting post: https://www.linkedin.com/posts/manikonda-anjali-64780a348$_{o}pensource-kluniversity-foss-share-7382317098447958017-hTWs?utm_{s}ource = shareutm_{m}edium = member_{d}esktoprcm = ACoAAFb5JxcBpdDn_{i}10$
- Blog post: https://www.linkedin.com/posts/manikonda-anjali-64780a348$_{u}gcPost-7399027025384120321-c5s0?utm_{s}ource = shareutm_{m}edium = member_{d}esktoprcm = ACoAAFb5JxcBpdDn_{i}10sfsKwXliUt9Rj9_{a}Eg0$
- PR post: https://www.linkedin.com/posts/manikonda-anjali-48780a367$_{u}gcPost-7399027025384853221-c5s0?utm_{s}ource = shareutm_{m}edium = member_{d}esktoprcm = ACoAAFb5JxcBpdDn_{i}10sfsKwXliUt9Rj9_{a}Eg0$