KL UNIVERSITY
Department of Computer Science & Engineering

Open Source Report

Submitted by : Jayana Anjani Pavan Vardhan Naidu
Roll No. : 2400030016 **Semester:** 3rd Semester
Course : Open Source Engineering(24CS02EF)
Academic Year: 2024-2025

Submitted to: DR.N B ARUNE KUMAR

Contents

Abstract

This report provides an in-depth documentation of practical work conducted on Ubuntu Linux as part of the Open Source Engineering coursework. The primary objective of the work was to develop a strong understanding of privacy, encryption, secure communication, and open-source workflows through real-world implementation rather than theoretical study alone. The activities included generating and managing GPG key pairs, encrypting and

decrypting files, and sending secure email messages using asymmetric cryptography to ensure confidentiality, integrity, and authenticity.

The report further explores various privacy-oriented tools such as Tor Browser, Signal, VeraCrypt, Firefox (privacy-hardened), and ProtonMail, analyzing their relevance in modern digital security. In addition, a self-hosted blogging platform (FlatPress) was deployed on a DigitalOcean Ubuntu server using Apache, demonstrating foundational server administra- tion, hosting, and security configuration skills.

Alongside hands-on technical work, the selection of the MIT License is justified based on its permissive nature and community-friendly reuse model. The report also summarizes open-source contributions made during Hacktoberfest, featuring six successfully merged pull requests across multiple repositories, showcasing real participation in collaborative develop- ment.

Overall, this work strengthened both conceptual understanding and practical ability in secure computing, Linux-based system management, and global open-source collaboration, reflecting the importance of privacy and transparency in modern technology ecosystems.

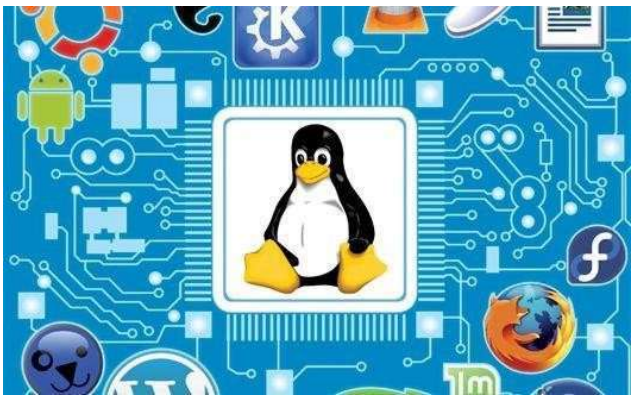


Figure: Linux.

1. About the Linux Distribution Used

Distribution Used: Ubuntu (Long Term Support Release).

Reason for Selection: Ubuntu was selected due to its beginner-friendly environment, robust stability, strong community support, and extensive documentation. These features make it an ideal platform for learning Linux fundamentals, system administration, and open-source tools.

1.1. Key System Components

- **Linux Kernel:** Core component responsible for hardware management, process control, and memory allocation.
- **Shell and User-Space Utilities:** Enable command-line interaction, automation and script- ing using Bash and related utilities.
- **Package Manager (APT):** Handles installation, removal and updating of software packages and dependencies.
- **System Services (systemd, networking, web services):** Manage background processes and essential system tasks.

1.2. Installation Overview

The operating system was installed on a VirtualBox virtual machine (or local hardware) using standard installation procedures. Two separate user accounts were created to practice encrypted communication and key-based access control during GPG experimentation.

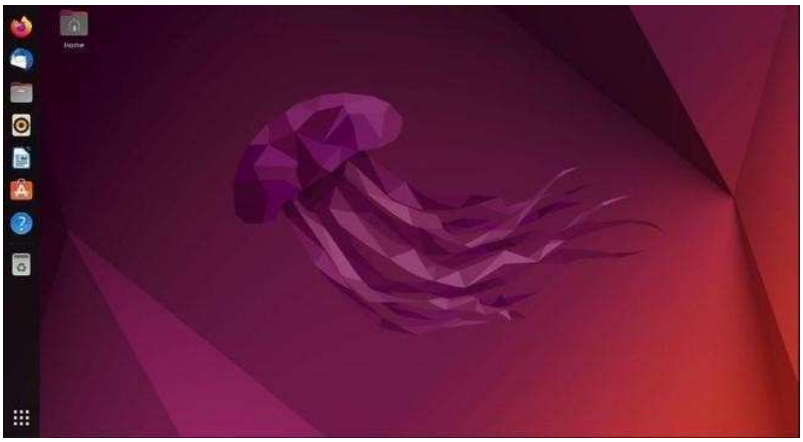


Figure 1: Ubuntu Interface.

2. Encryption and GPG

2.1. What is Encryption?

Encryption converts readable information (plaintext) into an unreadable format (ciphertext) to prevent unauthorized access. It ensures confidentiality, data integrity and authenticity when combined with digital signatures.

2.2. What is GPG?

GPG (GNU Privacy Guard) is an open-source implementation of the OpenPGP standard. It provides asymmetric encryption using public and private key pairs for secure communication, file protection and digital signing.

2.3. How GPG Works — Overview

Public Key	Shared openly; used by others to encrypt messages intended for the key owner.
Private Key	Confidential key used to decrypt messages and create digital signatures.
Digital Signatures	Verify authenticity, identity and integrity of data.

2.4. Common GPG Commands

```
gpg -- full - generate - key gpg -- list
- keys
gpg -- export -a " User" > public. key gpg -- import
public. key
gpg -- encrypt -- recipient friend@ example . com file . txt gpg -- decrypt file .
txt. gpg
```

2.5. Hands-On Experience

Two local Ubuntu accounts were configured and GPG key pairs generated for both. Public keys were exchanged and used for encrypting and decrypting local files and messages. Encrypted email exchange with a classmate was later performed to simulate real-world secure communication. This activity enhanced understanding of identity verification, file protection, and key management workflows.

3. Sending Encrypted Email

3.1. Workflow Summary

1. Generate key pairs for both sender and receiver.
2. Exchange and import public keys.
3. Encrypt message or file using receiver's public key.
4. Send encrypted content and decrypt using private key.

Example command for encrypting a message:

```
gpg -- encrypt -- recipient classmate@ example . com message . txt
```

3.2. Student Implementation Notes

Initial testing was carried out locally between two accounts, followed by encrypted exchange over email. This demonstrated real-world handling of encrypted communication and secure file management.

3.3. Selected Privacy Tools Explored

- **Tor Browser** — anonymous browsing and tracker protection.
- **Signal** — end-to-end encrypted messaging.
- **ProtonMail** — built-in PGP-based encrypted mail.
- **VeraCrypt** — secure disk and partition encryption.
- **Firefox (privacy-hardened)** — enhanced browser security settings.

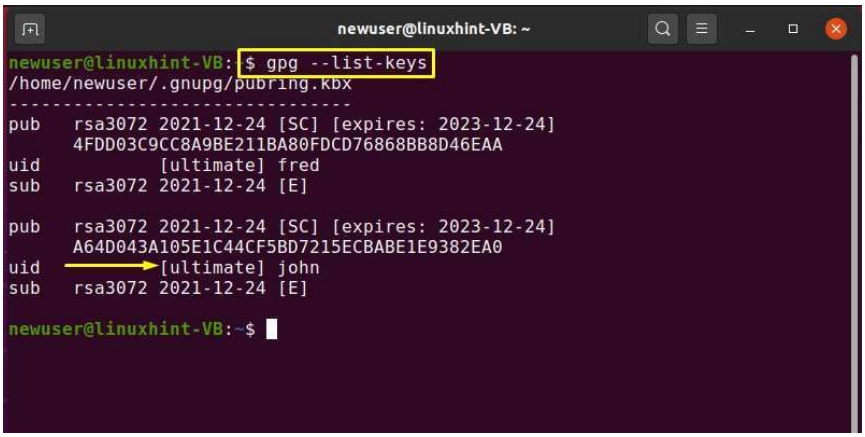


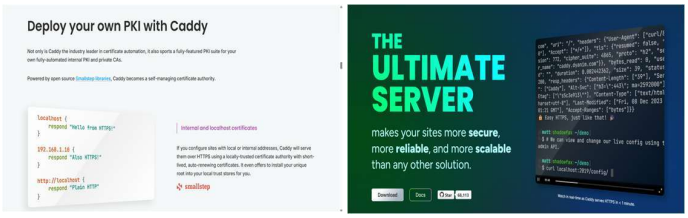
Figure 2: Terminal output showing GPG encryption and decryption operations.

4. Hosting and Installation Summary

Platform: Ubuntu Server
Engine: Caddy Web Server

1. Install Caddy (official repo):
2. sudo apt update && sudo apt install-y debian-keyring debian-archive-keyring apt-transport-https
3. curl-1sLf 'https://dl.cloudsmith.io/public/caddy/stable/gpg.key' | sudo apt-key add-
4. curl-1sLf 'https://dl.cloudsmith.io/public/caddy/stable/debian.deb.txt' | sudo tee /etc/apt/sources.list.d/caddy-stable.list
5. sudo apt update && sudo apt install caddy
6. Configure your site in /etc/caddy/Caddyfile
7. Allow HTTP/HTTPS ports using UFW:
8. sudo ufw allow 80

9. sudo ufw allow 443
10. Start and enable Caddy service:
11. sudo systemctl start caddy
12. sudo systemctl enable caddy
13. Access your hosted site using its domain —
    Caddy automatically provisions HTTPS certificates



4.3. License Used

MIT License was selected due to its permissive nature, enabling reuse, modification and re-distribution with minimal restrictions while requiring attribution.

5. Open Source Contributions — Summary

During Hacktoberfest and related open-source activities, a total of **6 pull requests were successfully merged** across multiple public repositories, resulting in recognition as a **Hackto- berfest Super Contributor**. These contributions involved UI improvements, documentation enhancements, and feature additions, reflecting practical experience in real-world collaboration workflows.

Repository / PR	Description / Status
Firstcontributions	Added name to the list (Merged)
zero-to-mastery	Added info to contributors (Merged)
APDevTeam	Updated .gitignore(Merged)
sudheerj/js-question	Added info to readme (Merged)
KLGLUG	Added self hosting server (Merged)
WPT Refactor	wpt.py (Merged)

5.1. Contribution Example

APDevTeam #760: Updated .gitignore to include Vim swap files(*.swp), submitted PR, addressed reviewer suggestions, and the PR was merged successfully.

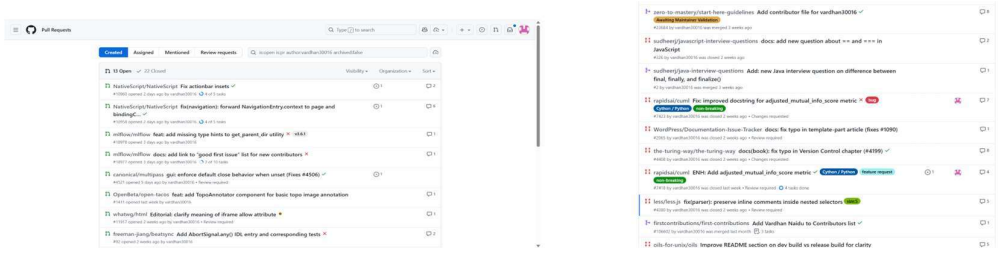


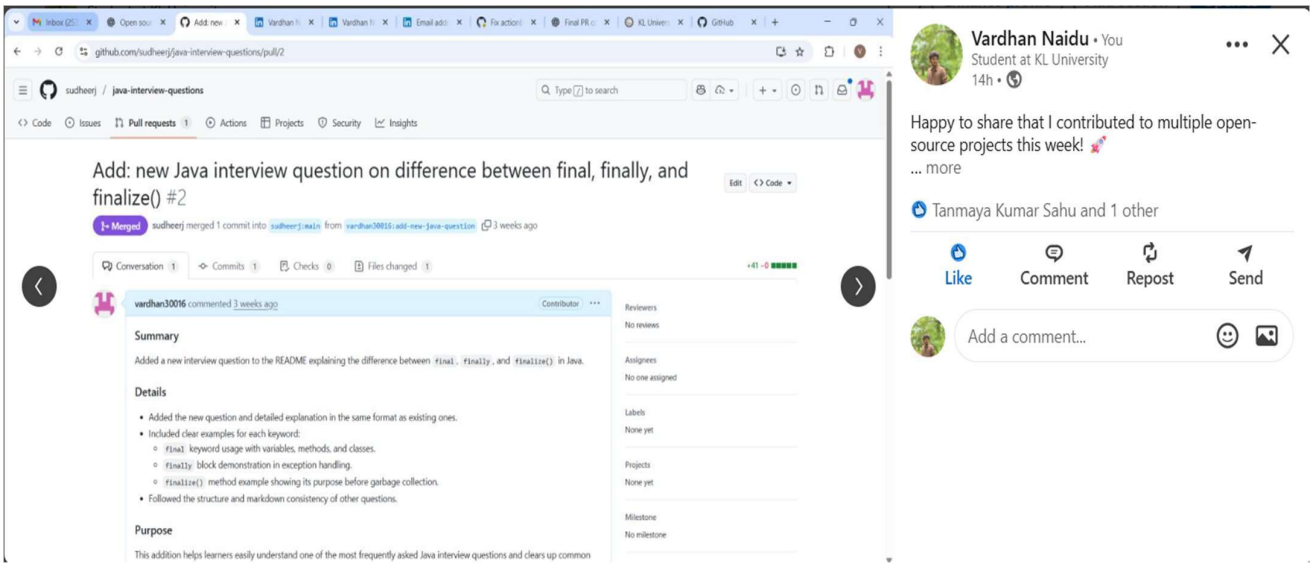
Figure: Pull Request submission and merged status screenshots.

5.2. Documentation Links and Screenshots

1.https://www.linkedin.com/posts/vardhan-naidu-ba737b339_my-open-source-journey-projects-prs-and-ugcPost-7399045954638688257-r9qS?utm_source=share&utm_medium=member_desktop&rcm=ACoAAFTzO-8BUKVcXo-cZljU5IhAdP41jmJ-xCo

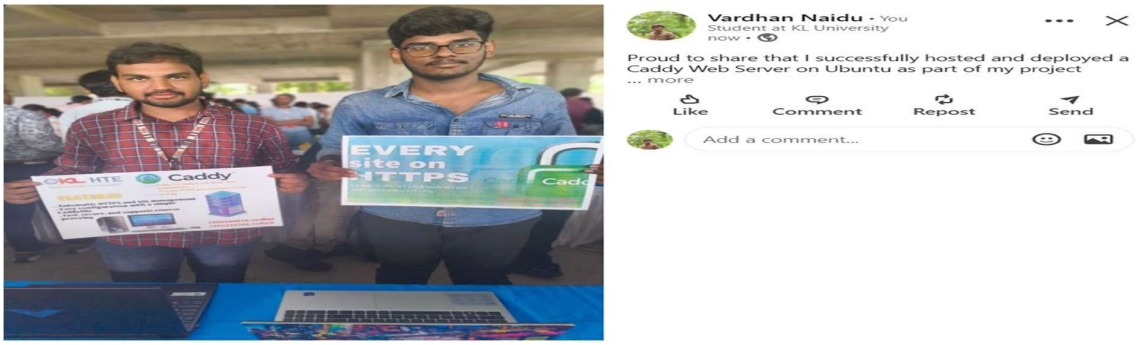
Screenshot of LinkedIn Post 1

2. https://www.linkedin.com/posts/vardhan-naidu-ba737b339_happy-to-share-that-i-contributed-to-multiple-ugcPost-7399083049683943424-KT3i?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAAFTzO-8BUKVcXo-cZljU5IhAdP41jmJ-xCo



Screenshot of LinkedIn Post 2

https://www.linkedin.com/posts/vardhan-naidu-ba737b339_proud-to-share-that-i-successfully-hosted-share-7399304616053637120-yzkh?utm_source=social_share_send&utm_medium=member_desktop_web&rcm=ACoAAFTzO-8BUKVcXo-cZljU5IhAdP41jmJ-xCo



Screenshot of LinkedIn Post 3

Conclusion

This report presented a comprehensive overview of practical hands-on work integrating Linux system administration, secure communication practices, privacy-focused experimentation, and active participation in the open-source ecosystem. Through the implementation of GPG key generation, encrypted messaging, and secure email transmission workflows, a strong foundation in digital security and cryptographic principles was developed. Additionally, deploying a self- hosted FlatPress blog on DigitalOcean using Apache contributed to real-world understanding of server configuration, hosting environments, and web service management.

Engagement in open-source through Hacktoberfest and successful merging of six pull requests further enhanced skills in collaborative software development, Git workflows, issue tracking, doc- umentation improvement, and community-driven problem solving. The experience strengthened both technical and professional competencies such as communication, version control discipline, and global teamwork.

Overall, the combined theoretical and practical learning has contributed significantly to a deeper understanding of secure computing, privacy engineering, and open-source development—skills that are essential in modern technological environments and future industry roles.

Acknowledgement: I express my sincere gratitude to **Mr. Arunekumar Bala** for their continuous guidance, support, and encouragement throughout this project.

Contact : https://www.linkedin.com/in/vardhan-naidu-ba737b339/