OPEN SOURCE ENGINEERING

STUDENT NAME : VASA SAIKUMAR
STUDENT ID: 2400100073

Under the guidance of : Dr. Sripath Roy Koganti

1 Understanding the Core Ubuntu Linux Distribution

1.0.1 1. Overview and Philosophy

Ubuntu is a free and open-source operating system based on Debian Linux. It is one of the most popular Linux systems used on desktops. Ubuntu is known for being easy to use, stable, and suitable for beginners as well as developers. It is developed by Canonical Ltd. The main idea of Ubuntu is "Linux for human beings," which means it focuses on making the system simple, user-friendly, and accessible to everyone.

1.0.2 2. The Desktop Experience (GNOME)

Ubuntu uses the GNOME desktop environment, which gives a clean, modern, and simple interface. It has a dock on the left side for quick access to important apps. The Activities Overview, opened by pressing the Super/Windows key, helps you see all open windows, switch workspaces, and search for anything on the system. This makes working on Ubuntu smooth and fast. Ubuntu also supports most hardware automatically, so installation and setup are easy for users.

1.0.3 3. Software Management and Packaging

Ubuntu uses two main methods to install and manage software.

- APT is the traditional package manager that handles DEB packages from Ubuntu's official repositories.
- Snaps are modern, container-based packages created by Canonical. They include all the files an app needs, so the app works the same on different Ubuntu versions.

Snaps also run in a protected (sandboxed) environment, which improves security. With APT and Snap together, users get access to a large and updated collection of software.

2 Encryption and GPG

2.1 Types of Encryption in Ubuntu

Ubuntu mainly provides two types of encryption: Full Disk Encryption (FDE) and File/Directory Encryption.

2.1.1 1. Full Disk Encryption (FDE)

- What it is:
  FDE encrypts the whole hard disk or a large partition. This includes the OS files, swap area, and your personal data.

- How it works:
  Ubuntu uses LUKS (Linux Unified Key Setup) for FDE. When you start the computer, it asks for a passphrase. If the passphrase is correct, the whole disk gets unlocked and you can use the system normally.
- Purpose:
  FDE protects your data if someone steals your laptop or hard drive. Without the LUKS passphrase, the data cannot be read.
- Implementation:
  FDE is usually turned on during Ubuntu installation by selecting "Encrypt the new Ubuntu installation."
  Enabling it after installation is possible but more difficult.

2.1.2 2. File and Directory Encryption

- What it is:
  This encrypts only selected files or folders. It gives you more control over what you want to protect.
- Tools:
  - GPG (GNU Privacy Guard): Used to encrypt individual files and for secure communication using public and private keys.
  - eCryptfs (older): Used earlier to encrypt the Home folder but now mostly replaced by Full Disk Encryption.

2.2 GPG (GNU Privacy Guard) Explained

GPG is a tool that follows the OpenPGP standard. It is used to secure files and to send safely encrypted messages.

2.2.1 1. Core GPG Concepts

GPG uses asymmetric cryptography, meaning it works with two keys:

- Public Key:
  You can share this key with anyone. Others use it to encrypt messages for you or verify your digital signatures.

- Private (Secret) Key:
  This key must be kept safe and protected with a passphrase.
  You use it to decrypt messages sent to you or to sign files so others know they are really from you.

2.2.2 2. Basic GPG Command-Line Usage

GPG is usually already installed on Ubuntu and is mainly used in the Terminal.

A. Generating a Key Pair

To create your public and private keys:

gpg --full-generate-key

You will be asked to choose:

- Key type (RSA is common)
- Key size (4096 recommended)
- Expiry date
- Your name and email
- A strong passphrase for your private key

B. Encrypting a File for Yourself (Symmetric Encryption)

This method uses one passphrase to lock the file:

gpg -c myfile.txt

This creates an encrypted file named myfile.txt.gpg.

C. Encrypting a File for Someone Else (Asymmetric Encryption)

You must have the other person's public key (imported using gpg --import):

gpg --encrypt --recipient "recipient@example.com" mysecretfile.doc

This creates mysecretfile.doc.gpg, which only the recipient can decrypt with their private key.

D. Decrypting a File

To open a file encrypted for you:

gpg --decrypt mysecretfile.doc.gpg

You will be asked for the passphrase of your private key.
Use --output to save the decrypted file with a name you choose.

3 Sending Encrypted Email

3.1 Prerequisite: Setting Up GPG

Before sending or receiving encrypted emails, both you and the other person must set up GPG keys and share them with each other.

1. Generate Keys:
   Both people must create their own public/private key pair using:
   gpg --full-generate-key
2. Exchange Public Keys:
   You need the recipient's Public Key, and they need yours.
   Ways to share keys:
   - Export and send the key file:
     gpg --armor --export 'Recipient Name' > recipient_key.asc
   - Or upload your key to a public key server.
3. Import the Recipient's Key:
   Add their key to your GPG keyring:
   gpg --import recipient_key.asc

3.2 Sending the Encrypted Email

The easiest way to send GPG-encrypted email in Ubuntu is by using Mozilla Thunderbird, which has built-in OpenPGP support.

3.2.1 1. Compose the Message

- Open Thunderbird and create a new email.
- Write your message normally.

3.2.2 2. Encryption and Signing

When sending a secure email, two things happen:

1. Encryption:

- You encrypt the message using the recipient's Public Key.
- Only their Private Key can open (decrypt) it.
- If sending to multiple people, the email must be encrypted for each person's Public Key.

2. Digital Signing:
   - You sign the email using your Private Key.
   - This proves to the recipient that the email is really from you.

In Thunderbird, you simply open the OpenPGP or Security menu and select Encrypt and Sign for the message.

3.2.3 3. Verification and Sending

- Thunderbird will check if you have the needed Public Keys for all recipients.
- If a key is missing, it will warn you.
- When you click Send, Thunderbird encrypts the email and adds your digital signature automatically.

3.2.4 4. Recipient's Experience (Decryption)

1. The recipient receives the encrypted (scrambled) message.
2. Their email client uses their Private Key and passphrase to decrypt and read the message.
3. Their client also uses your Public Key to confirm the digital signature, proving the message is real and unchanged.

4 Privacy Tools From Prism Break

4.0.1 1. Tor Browser (Private Web Browsing / Anonymous Network)

- What it is:
  Tor Browser is a special browser based on Firefox. It sends your internet traffic through the Tor network, which is made up of volunteer-run servers.
- Privacy Focus:
  It hides your IP address and location, making it very hard for websites to track you. It also has strong anti-tracking and anti-fingerprinting features.
- PRISM Break Note:
  Recommended when you need maximum privacy and anonymity while browsing the internet.

4.0.2 2. Debian (Secure Operating System)

- What it is:
  Debian is a popular GNU/Linux operating system known for being stable and strictly open-source.
- Privacy Focus:
  Since all its software is open-source, anyone can review the code. This ensures transparency and reduces the risk of hidden tracking or spyware. It is more privacy-friendly than proprietary systems like Windows or macOS.
- PRISM Break Note:
  Suggested as an excellent choice for users moving away from closed-source operating systems.

4.0.3 3. Thunderbird (Secure Email Client)

- What it is:
  Thunderbird is a free and open-source email application created by Mozilla.
- Privacy Focus:
  It supports built-in OpenPGP (GPG) encryption. This lets you send encrypted emails and digitally sign messages easily, providing strong end-to-end security.
- PRISM Break Note:
  Recommended as one of the best secure email clients because of its open-source design and native GPG support.

4.0.4 4. KeePassXC (Local Password Manager)

- What it is:
  KeePassXC is a free and open-source password manager available on all major platforms.
- Privacy Focus:
  It saves all your passwords in a single, encrypted file stored only on your device. No cloud syncing or third-party storage is used, giving you complete control over your data.
- PRISM Break Note:
  Preferred for its strong encryption, open-source nature, and offline storage.

4.0.5 5. Firefox (Privacy-Friendly Web Browser)

- What it is:
  Firefox is a secure, fast, and flexible browser developed by Mozilla, a non-profit organization.
- Privacy Focus:
  Firefox includes strong tracking protection, privacy containers, and many trusted add-ons like uBlock Origin for ad-blocking. It is fully open-source and customizable for higher privacy.

- PRISM Break Note:
  Recommended for everyday browsing.
  While Tor Browser is best for anonymity, Firefox is suggested when websites don't work properly on Tor. It becomes more privacy-friendly when you adjust its settings and use a privacy-focused search engine.

5 Open Source License

5.1 The Core Purpose and Classification

The GNU GPL v3 (General Public License version 3) is one of the most widely used and influential open-source licenses. Created by the Free Software Foundation (FSF), its main purpose is to ensure that software remains free for all users—free to use, study, modify, and share. GPL v3 is classified as a strong copyleft license, meaning any modified versions or redistributed copies must also remain open-source under the same GPL v3 terms. This protects user freedom and prevents the software from becoming closed-source or used in ways that restrict others.

5.2 Granted Rights and Permissions

The GNU GPL v3 allows anyone who receives the software to use it for any purpose, study how it works, modify the source code, and share copies with others. Users may also distribute modified versions of the software. However, whenever the software is shared—whether original or modified—the entire source code must be made available under the GPL v3. This ensures that improvements remain free and open for the whole community.

5.3 The Copyleft Requirements for Distribution

Unlike permissive licenses, GPL v3 has strict rules to protect software freedom. When distributing the software, users must follow these requirements:

1. Source Code Availability: You must provide access to the complete source code, including any modifications you made.
2. Same License Requirement: Any shared or modified version must also be released under GPL v3 only, not under a different license.
   These rules ensure that no one can take GPL v3 software and turn it into a closed-source or proprietary product.

5.4 Disclaimer of Warranty and Liability

Disclaimer of Warranty for Blogosfera

Blogosfera is a self-hosted blogging platform powered by Ghost CMS and is provided solely for educational, experimental, and personal demonstration purposes. This system is offered "AS IS" and "AS AVAILABLE" without any guarantees or warranties, either express or implied.
The developer of Blogosfera makes no representations or warranties regarding: • System reliability or uptime • Data protection or recovery • Security against cyber threats • Performance consistency • Compatibility with all devices or networks
Blogosfera may experience downtime, software bugs, configuration errors, or security vulnerabilities typical of self-managed server environments. The developer shall not be held liable for any direct or indirect damages, including data loss, service interruption, unauthorized access, or system failure resulting from the use or misuse of this platform.
Users are solely responsible for maintaining backups, applying security updates, and ensuring safe usage of the Blogosfera server. By using this platform, you acknowledge and accept all associated risks and responsibilities.

6. Self Hosted Server (Blogosfera)

6.1 About

Blogosfera is a self-hosted blogging platform built using the Ghost CMS. The project focuses on creating a modern, fast, and secure content publishing system that is hosted on my own local/server environment. By implementing Ghost as the core of Blogosfera, I gained practical experience in deploying and managing a real-world production-ready blog server.
The self-hosted setup allows full control over performance, configuration, themes, user access, and content management, making Blogosfera a flexible and scalable blogging solution.

6.1.1 Key Features

• Modern blogging platform powered by Ghost CMS.
• Self-hosted server with full administrative control.
• Fast and responsive user interface.
• Secure content management with user authentication.
• Custom theme support and content personalization.
• SEO-friendly architecture for better visibility.
• Open-source environment allowing customization and extension.
• Real-time content publishing and management dashboard.

6.2 Installation Process (Self Hosting Ghost for Blogosfera)

1. Update Ubuntu System

sudo apt update && sudo apt upgrade -y

2. Install Required Packages

sudo apt install nginx mysql-server nodejs npm -y

3. Install Ghost CLI

sudo npm install -g ghost-cli

4. Create a Directory for Blogosfera

sudo mkdir -p /var/www/blogosfera

sudo chown $USER:$USER /var/www/blogosfera

cd /var/www/blogosfera

5. Install Ghost

ghost install

During installation, you will configure:
• Blog URL
• MySQL database
• Nginx configuration
• SSL (optional)
• SystemD startup

6. Start Ghost Server

ghost start

Your Blogosfera blog will now be live on the configured URL.

Accessing the Server
To run the Blogosfera server, execute:
ghost start

Then open the displayed URL (for example: http://localhost:2368) in your browser.
To access from another device on the same network:

1. Find your system IP address using:

ip a

2. On another device, open:
   https://24769.176236.638

Ensure the port is allowed through the firewall using:
sudo ufw allow 2368

For public access, configure port forwarding in your router and set up a domain name if required.

What I Learned From This Project

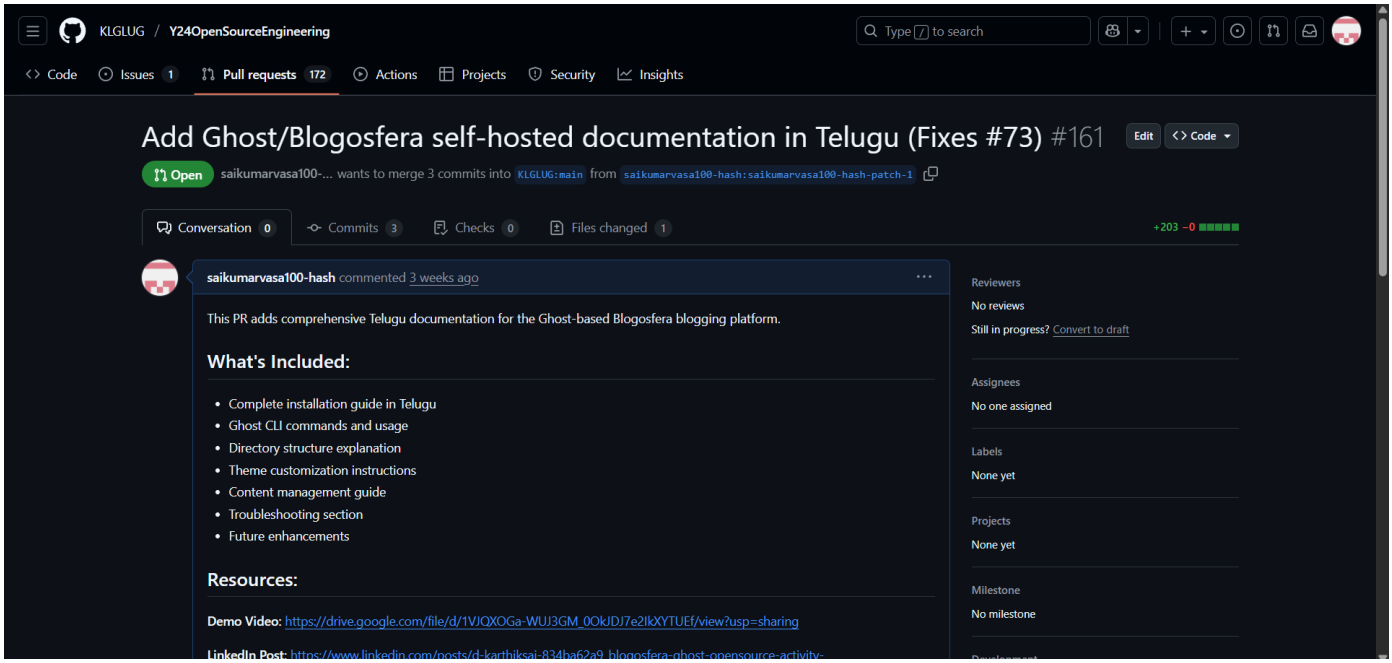
- Installing and managing Ghost CMS on a self-hosted server
- Configuring and maintaining Nginx web server
- Understanding reverse proxy and server routing
- Setting up and managing MySQL databases
- Implementing SSL and secure connections
- Hosting a live service on a local and network environment
- Managing server permissions and file ownership
- Gaining hands-on experience with real-world server deployment
- Troubleshooting server and configuration errors

BLOGOSFERA

7 Open Source Contribution

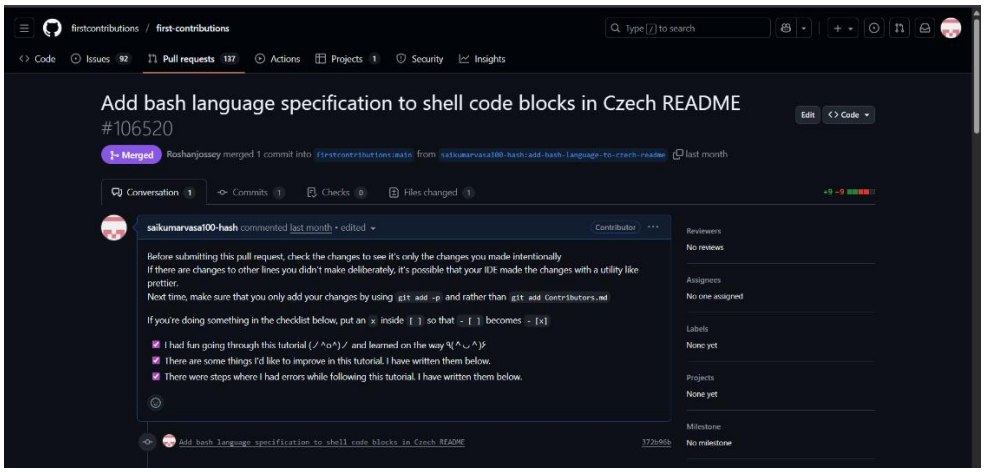
PR 1

Project: KLGUG/Y24OpenSourceEngineering (Blogosfera)
PR Title: Add Ghost/Blogosfera self-hosted documentation in Telugu (Fixes #73) #161
Description: This PR adds comprehensive Telugu documentation for the Ghost-based Blogosfera blogging platform, including complete installation guide, Ghost CLI commands, directory structure explanation, theme customization, content management guide, and troubleshooting section.
Status: Open (+203 lines added)



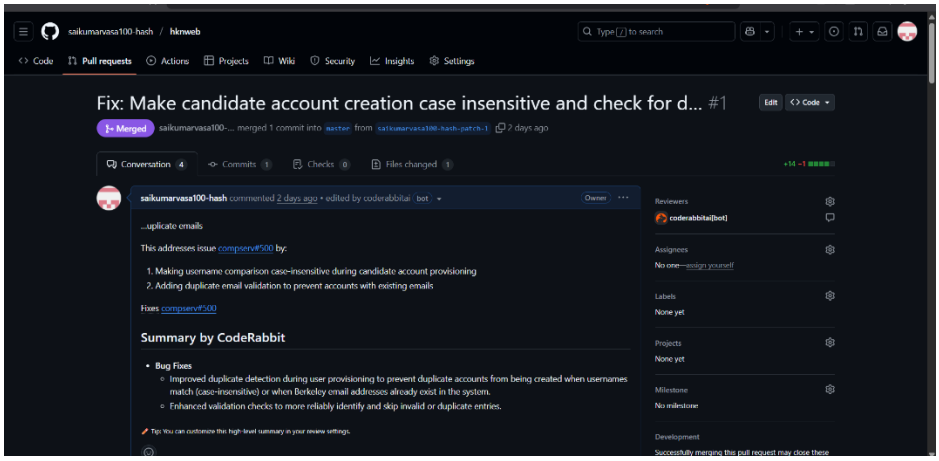
PR 2

Project: firstcontributions/first-contributions
PR Title: Add bash language specification to shell code blocks in Czech README #106520
Description: This PR adds the missing bash language tag to all shell code blocks in the Czech README file, improving syntax highlighting and readability for users following the First Contributions tutorial.
Status: Merged (+9 −9)



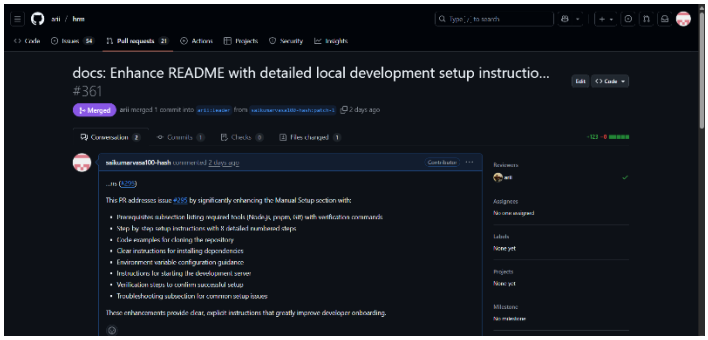
PR 3

Project: saikumarvasa100-hash/hknweb
PR Title: Fix: Make candidate account creation case insensitive and check for duplicate emails #1
Description: This PR fixes issue compserv#500 by making username comparison case-insensitive during candidate account creation and adding validation to prevent duplicate accounts with existing email addresses.
Status: Merged (+14 −1)



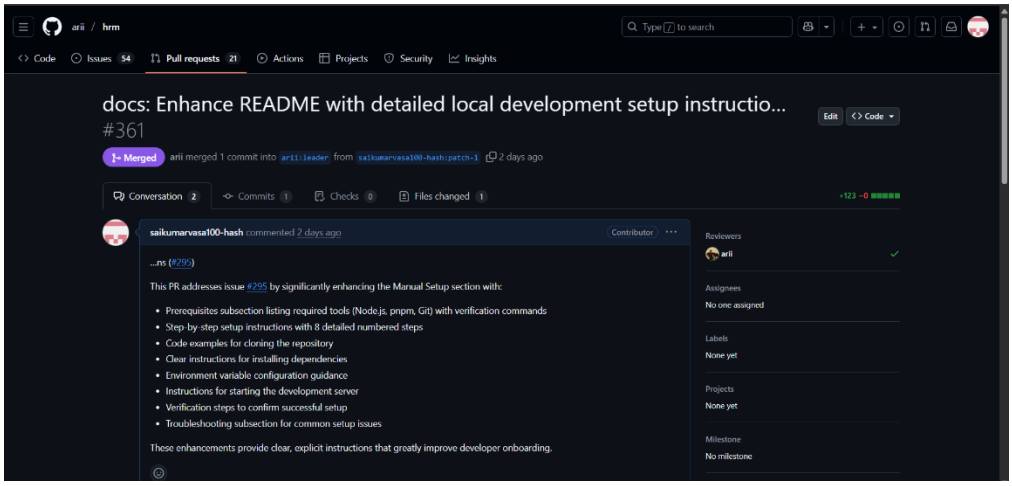
PR 4

Project: saikumarvasa100-hash/doc_parser
PR Title: Document LLM/VLM endpoint configuration details #1
Description: This PR adds detailed documentation for LLM/VLM endpoint configuration, including usage guidelines, recommended patterns, parameter descriptions, deployment options, best practices, and troubleshooting guidance.
Status: Merged (+89 −0)



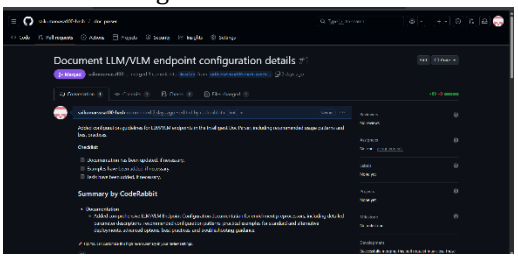
PR 5

Project: arii/hrm
PR Title: docs: Enhance README with detailed local development setup instructions #361
Description: This PR enhances the Manual Setup section by adding prerequisites, step-by-step setup instructions, cloning examples, dependency installation guidance, environment variable setup, server start instructions, verification steps, and troubleshooting notes.
Status: Merged (+123 −0)



PR 6

Project: saikumarvasa100-hash/ggshield
PR Title: feat: use OS port selection for OAuth server #1
Description: This PR implements OS-based port selection for the OAuth server by enabling automatic port assignment (port 0), removing the USABLE_PORT_RANGE constant, and simplifying server initialization error handling.



Status: Merged (+9 −19)

8 Linkedin Post Links

8.1PR : https://www.linkedin.com/posts/sai-kumar-8a7206300_another-open-source-contribution-has-been-activity-7399370405549084672-IbNx?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEzqxX8BkHzERDTPb54-yLKZI44LBdrdOY8

Journey Of Open Source : https://www.linkedin.com/posts/sai-kumar-8a7206300_activity-7399420908605427713-AnRy?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEzqxX8BkHzERDTPb54-yLKZI44LBdrdOY8

Self Hosted Project :

https://www.linkedin.com/posts/sai-kumar-8a7206300_opensource-samyak-kluniversity-activity-7399363969779666944-r34s?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEzqxX8BkHzERDTPb54-yLKZI44LBdrdOY8