

Home Network Solutions

Team Members:

Bryan Bermudez (bbermudez2023@my.fit.edu)

Brennan Ramsey (bramsey2023@my.fit.edu)

Joshua Revels (jrevels2023@my.fit.edu)

Nicholas Bleeker (nbleeker2024@my.fit.edu)

Faculty Advisor:

Dr. Mohan (rmohan@fit.edu)

Meeting Date:

August 26 - 12:20 PM

Goals and Motivations:

Home networks may include devices of varying hardware, each running their own applications and services. With each system running independently of one another, there is little to no interconnectivity. Because of this, the user may need to jump between devices on the home network to complete day-to-day tasks. This can be a tedious process and hinders productivity. When the user is away from the home network, many systems may be entirely inaccessible.

Our goal is to develop a system that links many convenient and essential features across devices on a home network, as well as make the network more comfortable to utilize in general. The aim for seamless integration will allow the user to worry less about the linkage, or lack thereof, between devices. Instead, users can focus on their tasks at hand.

Key Features:

1. Home Security Application

The user will be able to control all the security features of their home network using a single application. All project features provided will be able to be accessed, monitored, and configured from this application. The application provided will be user friendly with a clean and easy setup and user interface.

2. File Manager

The user will be able to share, sync, and manage files across multiple devices on the same network. The user can access synchronized folders within the user-friendly file manager. The user can utilize version control, akin to GitHub, for easy version synchronization or restoration of files.

3. Ad-block

The user will have online ads blocked across their home network. Using specialized hardware the adblocker will function across all supported smart devices such as mobile devices, desktop, smart TVs, etc. The ad-blocker will be configurable and modifiable through the home security application.

4. IP Sharing

The user will be able to share their home network IP address with other devices. This feature can be used for security purposes or to use services that are only available in the region of the home network, like localized webpages or streaming services. The user can configure how IP sharing functions and what devices can use this service.

5. VPN

The user will be able to connect their devices to a chosen VPN with the server acting as a gateway. This allows the user to browse under an anonymous IP address instead of the household's IP address.

6. AI Agent

The user will be able to connect an AI agent of their choice (Claude, GPT, Grok, Deepseek, Gemini, etc.) to the server's web portal using their own API key. The agent will act as a normal agent with the ability to access the server, run diagnostics, restart services, and adjust configuration based on a list of permitted operations, with actions logged and password protected before execution.

Novel Functionalities:

1. Integrating 3rd party AI to access files on the server & local devices.

The user will be able to use a 3rd-party AI agent of their choice to access and modify most files stored on the server while away from home.

2. VPN Toggle

The user will be able to easily toggle user-provided VPNs on or off.

3. User File Manager

The user will be able to upload and download their files from any device securely, similar to Google Drive's functionality.

4. Game/Screen Casting

The user will be able to stream content from one device on a home network to another. The user can stream a desktop environment, games, or other applications.

Tools:

1. Pi-hole

- The user can block ads on a local network using a custom, locally hosted DNS server.

2. Tailscale

- The user will be able to access all of their devices from anywhere by simulating a local network, as well as access the internet from any connected device's network.

3. ProtonVPN

- The user will be able to anonymously access the web, as well as change their location. The user may provide alternative VPNs; ProtonVPN can be included as a default.

4. Home Assistant

- The user can control their home's smart devices or security systems from one application.

5. Matter

- The user will be able to connect all of their smart devices using one service.

6. Git

- The user will be able to view version history of their files and roll them back if necessary.

7. EXT4 file management

- We plan to use EXT4 to manage user files as it is best suited for simplicity and low resource usage. The main downside is that it does not allow for native drive pooling.

8. Samba

- The user can access shared folders and files stored on a home server. The user can manage the read and write permissions for multiple users, per folder.

9. Jellyfin

- The user can view locally stored video and audio files in a clean, streaming service-like interface. The user can organize their media catalogue as desired.

10. CubeCoders AMP

- The user can easily host and manage video game servers locally.

11. Ubuntu (Server)

- The user can host all the tools and features of this project on a device running Ubuntu.

12. Docker

- The user can control which services are run on the home server at any given time. The user can opt to have their services containerized to enhance cyber security.

Technical Challenges:

1. Version Control

- Saving a snapshot of each individual file on a machine would be costly. It may be tricky to decide which files to save and when.

2. Some ads are not blocked by Pi-Hole

- A potential solution would be for the host machine to load a browser-based adblock and send that data to the client machine.

3. VPN Interactions

- Since Tailscale functions as tunneling software, it could cause problems when a VPN is in use.
- A kill switch may be implemented when the VPN disconnects unexpectedly.
- The ad-blocking tools may conflict with VPN tools.
- Having away-from-home devices tunnel to use the home network can compromise the home network.
- Connection speed is capped by the slowest link between the home network and VPN server; most commonly this is the home network's upload speed

4. AI integration

- Allowing the user to select any AI they want could slow down development. We could only select 4 of the most popular agents for users to connect to.
- Creating an allow list for server side commands brings about data exposure and prompt injection. We may just want to create a separate “settings” type page on the local web app that is dedicated to server settings / diagnostics.

5. Creating a web app interface

- An admin interface that can be used from away-from-home devices creates an easy point of attack. This web app should only be accessible from the local network.
- Real-time server status may require websockets
- Built with HTML, CSS, and JS; or with frameworks that use these languages.

6. Creating a mobile app

- Development of a dedicated mobile app will slow down project development. Alternatively, an away-from-home version of the web app accessible to mobile devices will minimize development time while retaining this feature.

7. Cybersecurity

- Accessing the home server and its features while outside the home network can pose security risks.
- Some solutions may involve utilizing VPNs, proxy servers, folder encryption, user permissions, passwords, and other methods.

Approval from Faculty Advisor:

“I have discussed with the team and approved this project plan. I will evaluate the progress and assign a grade for each of the three milestones.”

Signature: _____

Date: _____