Data Nest
(A centralized Storage Solution for Home)

A minor project report submitted in partial fulfillment for the award of degree of

Bachelor of Engineering

in

Computer Science & Engineering

by

Amisha Gurndwal [2021a1r062]

Sania Fotedar [2021a1r082]

Amjid Khan [2021a1r106]

Aniket Dhiman [2021a1r172]

Under the supervision of

Ms. Harashleen Kour
Assistant Professor,CSE

DEPARTMENT OF COMPUTER SCIENCES AND ENGINEERING

MODEL INSTITUTE OF ENGINEERING AND TECHNOLOGY
JAMMU, J&K, INDIA

BATCH 2021-2025

MIET/CSE/PR/.../2024-25

Model Institute of Engineering & Technology, Jammu

Certificate

This is to certify that this Minor Project entitled **Data Nest (A centralized Storage Solution for Home)** is a bonafide work of **,Amisha Gurndwal, Sania Fotedar, Amjid Khan, Aniket Dhiman** submitted to the Model Institute of Engineering & Technology, Jammu in partial fulfillment of the requirements for the award of the degree of "Bachelors of Engineering" in Computer Science & Engineering.

(Ms. Harashleen Kour)
Guide

(Name and sign)
External Examiner

College Seal

(Name and sign)
Internal Examiner

(Dr. Navin Mani Upadhyay)
HOD,CSE

Certificate of Approval of Examiners

The Minor Project report entitled **Data Nest (A centralized Storage Solution for Home)** by **Amisha Gurndwal, Sania Fotedar, Amjid Khan, Aniket Dhiman** is approved for the award of Bachelors Of Engineering Degree in **Computer Science & Engineering**.

_____
Internal Examiner

_____
External Examiner

Date:
Place: Jammu

Acknowledgement

Project work plays a significant role in the field of engineering, and the success of any project is the result of contributions from numerous individuals and organizations. The present work is no exception, having been shaped by the support and guidance of many people.

We would like to express our sincere gratitude to the **Model Institute of Engineering and Technology (Autonomous), Jammu**, for providing us with the opportunity to work on this project as part of our academic curriculum. This project has been a valuable learning experience, and we are thankful for the guidance and resources provided throughout its duration.

Our heartfelt thanks go to **Prof. (Dr.) Ankur Gupta** (Director, MIET), **Prof. Devanand Padha** (Senior Professor, CSE), **Dr. Navin Mani Upadhyay** (HOD, CSE), and all the project evaluators for their unwavering support, continuous encouragement, and valuable insights. Their expertise and guidance have been instrumental in shaping this project work, and we are truly grateful for their contributions. We also extend our thanks to the faculty members whose advice and inputs have significantly contributed to our development.

We would also like to express our deep appreciation to our mentor, **Ms. Harashleen Kour**, for her invaluable guidance and consistent support throughout this project. Her advice, expertise, and encouragement have played a pivotal role in the successful completion of this project.

Furthermore, we would like to acknowledge the support of our parents, whose encouragement and belief in us have been a constant source of motivation. Their support has been invaluable in helping us navigate this project.

We also wish to express our gratitude to Overleaf, the excellent collaborative writing platform, which provided an intuitive and efficient environment for creating and documenting this project. **Overleaf's** ease of use and collaborative features have been invaluable, enabling us to efficiently organize and present our work.

DECLARATION

I **Amisha Gurndwal, Sania Fotedar, Amjid Khan, Aniket Dhiman,** hereby declare that the work which is being presented in the project report entitled, **"Data Nest(Centralized Storage Solution For Home)"** in the partial fulfillment of requirement for the award of degree of **B.E. (CSE)** and submitted in the **Department of Computer Science Engineering, Model Institute of Engineering and Technology (Autonomous), Jammu** is an authentic record of my own work carried by me under the supervision of **Ms. Harashleen Kour**. The matter presented in this project report has not been submitted in this or any other University / Institute for the award of B.E. Degree.

_____
Signature

_____
Amisha Gurndwal
Sania Fotedar
Amjid Khan
Aniket Dhiman

Date:
Place: Jammu

Abstract

Network Attached Storage (NAS) is a specialized file storage system designed to provide centralized, aggregated disk storage to users within a Local Area Network (LAN) over a standard Ethernet connection. By enabling seamless network access to files, NAS devices play a crucial role in modern data management. These systems are engineered to cater to the needs of both home and business users, offering robust solutions for data sharing, backup, and secure storage. Their versatility and efficiency have positioned NAS as an indispensable component of IT infrastructure, suitable for addressing a wide range of storage requirements.

This paper explores the fundamental features, architecture, and benefits of NAS systems, focusing on their ability to enhance the effectiveness of data management. NAS devices simplify file sharing and access across networks, providing centralized control that strengthens data security and streamlines administrative tasks. With scalable storage options, NAS systems can adapt to the evolving needs of users, accommodating growing datasets without compromising performance or accessibility. Advanced functionalities such as RAID (Redundant Array of Independent Disks) and snapshot capabilities are highlighted, showcasing how these features offer robust data protection, improved recovery options, and greater operational reliability.

The study also examines the adaptability of NAS systems across various industries and use cases, ranging from basic home applications like media servers to complex enterprise environments requiring sophisticated storage solutions. These examples illustrate the versatility of NAS in managing data for diverse workloads, from personal multimedia libraries to mission-critical business operations. Furthermore, the paper investigates emerging trends and innovations in NAS technology, including the integration of

cloud computing for hybrid storage environments, advancements in data deduplication to optimize storage efficiency, and the growing adoption of AI-driven features for smarter data management.

Concluding the discussion, the paper underscores the significance of NAS as a cornerstone of contemporary IT ecosystems. Its reliable, scalable, and cost-effective nature ensures that NAS continues to meet the increasing demands of a data-driven world. The ongoing advancements in NAS technology, particularly the fusion of local storage with cloud capabilities, promise to redefine the possibilities of data management, positioning NAS as a vital tool for the efficient, secure, and scalable handling of data in both personal and professional contexts.

Contents

List of Figures

List Of Abbreviations

ACL	Access Control List
DNS	Domain Name System
DAS	Direct-Attached Storage
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
JFS	Journaled File System
LVM	Logical Volume Management
NAS	Network-Attached Storage
NFS	Network File System
NVMe	Non-Volatile Memory Express
RAID	Redundant Array of Independent Disks
Rsync	Remote Sync
S.M.A.R.T.	Self-Monitoring, Analysis, and Reporting Technology
SAN	Storage Area Network
SDS	Software-Defined Storage
SCP	Secure Copy Protocol
SHH	Secure Shell
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
TCP/IP	Transmission Control Protocol/Internet Protocol
UUID	Universally Unique Identifier
UPnP	Universal Plug and Play
USB	Universal Serial Bus
WOL	Wake on LAN

Chapter 1

Introduction

The Network Attached Storage (NAS) project provides a centralized data storage solution, enabling secure and efficient file sharing across networks. Designed for scalability and ease of use, it integrates with various devices, ensuring seamless access and data protection. NAS supports backup, collaboration, and media streaming for personal or professional use.

1.1 Background

Information Technology (IT) is an essential part of today's business. IT technology is, among others, in key role for storing business knowledge into a stored format for later use. While IT gives clear advantages over previously used methods for storing knowledge, it also generates various new threats which are discussed in this project. However, these threats can be identified and minimized with the proper combination of hardware and software. This study focuses on utilizing various hardware and software to overcome the threats and it is based on design science

NAS (Network-attached storage) is a data storage, which is connected to a computer network. NAS acts as a file-server in a network, offering data storage to be located in a stand-alone unit, which other computers can be connected. NAS can be seen as a network drive (via Ethernet) and as such, it can be used to save documents and files as well as read them. Fundamentally, a NAS is a computer, optimized in hardware and software,

to be a file server.

The benefits from using NAS are clear; firstly it will improve the security of the data since it will be located in one place only, rather than divided into several PC's of the users personnel. That greatly decreases the chances of information leaks due to thefts, mistakes and accidents. Secondly, it will improve the maintenance of the data, allowing the local administrator to locate the data from one place and because of that, it can be managed easier than if the data would be located in several different places. Thirdly, it allows backing up the data frequently with an efficient way, so that the valuable data will not be destroyed in an accident or a single system failure. Fourthly, it improves the accessibility greatly by allowing users to connect to the device via web from practically anywhere. That allows users to gain access to their documents from home and practically anywhere which has an internet connection. In this case study, NAS will be designed, configured and finally implemented into existing local network to act as a file-server for the users. The project tries to solve and find out the proper way to implement it, as well as how to utilize it correctly. However, a significant focus will be on finding the most affordable solution without losing on features and fault-tolerance. The budget in this project is limited. The aim is to support simultaneous users. The outcome of this project will be a proper implementation of a NAS and as such it can be applied to any existing local network in a small- sized company.

1.2 Problem Statement

Traditionally, individuals manage their data by relying on personal devices like laptops or external hard drives. However, this approach poses significant risks of data loss. Accidental deletion, theft of a device, or hard drive failure can lead to irretrievable loss of important data or potential misuse of sensitive information. Additionally, when multiple family members store their data separately, managing backups and ensuring security across devices becomes challenging. A centralized home network-attached solu-

tion addresses these issues by providing a shared, secure, and redundant storage system for all family members, ensuring data safety, accessibility, and simplified management for the entire household.

1.3 Objective and Methodology

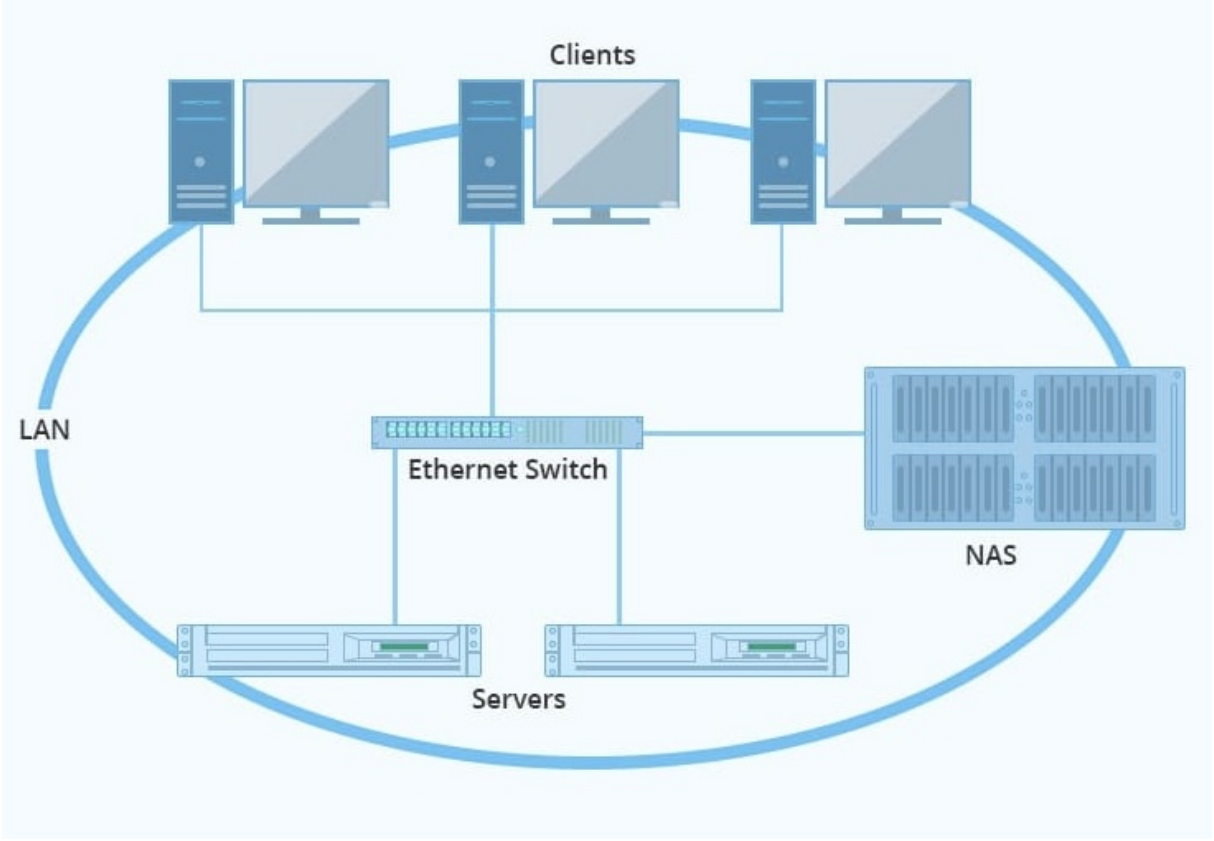


Figure 1.1: Network Attached Storage[29]

In above figure. The aim of this project is to create a data storage system for users which utilizes and fulfills the following requirements:

- External access over Internet
- Access from LAN
- Optimized data security
- Maintainability
- Future expansions
- System health monitoring

This project allows users to increase their data security in multiple ways as well as increases their mobility as their centralized data storage can be

accessed over Internet. This project can also be used as a guide in the implementation stage of a NAS-system in most scenarios. The project is applicable to be utilized in either home use, or in small offices.

1.4 NETWORK STORAGE CONCEPTS

In basic terms, network storage is simply about storing data using a method by which it can be made available to clients on the network. Over the years, the storage of data has evolved through various phases. This evolution has been driven partly by the changing ways in which we use technology, and in part by the exponential increase in the volume of data we need to store. It has also been driven by new technologies, which allow us to store and manage data in a more effective manner. Network storage is a generic term used to describe network based data storage, but there are many technologies within it which all go to make the magic happen. Storage is frequently used to mean the devices and data connected to the computer through input/output operations - that is, hard disk and tape systems and other forms of storage that don't include computer memory and other in-computer storage. For the enterprise, the options for this kind of storage are of much greater variety and expense than that related to memory. In a more formal usage, storage has been divided into:

Primary storage: which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache.

Secondary storage: which holds data on hard disks, tapes, and other devices requiring input/output operations.

1.4.1 Storage devices

It is alternatively referred to as digital storage, storage, storage media, or storage medium, a storage device is any hardware capable of holding information either temporarily or permanently.

There are two types of storage devices used with computers: a primary storage device, such as RAM, and a secondary storage device, like a hard drive. Secondary storage can be removable, internal, or external storage. Without a storage device, your computer would not be able to save any settings or information and would be considered a dumb terminal

1.4.2 Examples of Storage devices

Magnetic storage devices:
Today, magnetic storage is one of the most common types of storage used with computers and is the technology that many computer hard drives use. Floppy diskette, Hard drive, Super drive, Tape cassette, Zip diskette

Optical storage devices:
It uses lasers and lights as its method of reading and writing data
Blu-ray disc, CD-ROM disc, $\mathrm{CD}_{R}andCD-Wdisc$

Flash Memory devices:
$Jumpdrive, Memorycard, Memorystick, SSD$

Online and Cloud:
$Networkmedia, Dropbox, Onedrive$

1.4.3 Storage location

When saving anything on a computer, it may ask you for a storage location, which is the area in which you would like to save the information. By default, most information is saved to your computer hard drive. If you want to move the information to another computer, save it to a removable storage device such as a flash drive.

1.4.4 Primary storage

Primary storage, also known as main storage or memory, is the area in a computer in which data is stored for quick access by the computer's processor. The terms random access memory (RAM) and memory are often as synonyms for primary or main storage. Primary storage is volatile and can be contrasted with non-volatile secondary storage, also known as auxiliary storage. The terms main storage and auxiliary storage originated in the days of the mainframe computer to distinguish the more immediately accessible data storage from data stored on punch cards that required input/output (I/O) operations. when mainframe data storage contained ferrite cores, the term core storage was often used in place of primary storage.

In the label primary storage is often used to describe storage for data that is in active use, as opposed to data at rest in a backup. In this usage, the label primary storage may actually be describing the non-volatile secondary storage referred to in meaning above. It should be noted that although these two meanings conflict, the appropriate meaning is usually apparent from the context. For example, primary storage in a tiered-storage architecture might consist of hard disks or flash-based solid state drives on a centralized storage-area network (SAN) or network- attached storage (NAS)array that stores transactional data or mission- critical application data that requires extremely high performance.

1.4.5 Direct Attached Storage (DAS)

Direct attached storage is the term used to describe a storage device that is directly attached to a host system. The simplest example of DAS is the internal hard drive of a server computer,though storage devices housed in an external box come under this banner as well. DAS is still by far the most common method of storing data for computer systems. Over the years, though new technologies have emerged which work if you'll excuse the pun out of the box.

1.4.6 Network Attached Storage (NAS)

Network Attached Storage, or NAS, is a data storage mechanism that uses special devices connected directly to the network media. These devices are assigned an IP address and can then be accessed by clients via a server that acts as a gateway to the data, or in some cases allows the device to be accessed directly by the clients without an intermediary. An increasing number of companies already make use of NAS technology, if only with devices such as CD- ROM towers (stand-alone boxes that contain multiple CD-ROM drives) that are connected directly to the network.
Some of the big advantages of NAS include the expandability; need more storage space, add another NAS device and expand the available storage. NAS also bring an extra level of fault tolerance to the network. In a DAS environment, a server going down means that the data that server holds is no longer available. With NAS, the data is still available on the network and accessible by clients. Fault tolerant measures such as RAID, can be used to make sure that the NAS device does not become a point of failure.

1.4.7 Storage Area Network (SAN)

A SAN is a network of storage devices that are connected to each other and to a server, or cluster of servers, which act as an access point to the SAN. In some configurations a SAN is also connected to the network. SAN's use special switches as a mechanism to connect the devices. These switches, which look a lot like a normal Ethernet networking switch act as the connectivity point for SAN's. Making it possible for devices to communicate with each other on a separate network brings with it many advantages. Consider, for instance the ability to back up every piece of data on your network without having to 'pollute' the standard network infrastructure with gigabytes of data. This is just one of the advantages of a SAN which is making it a popular choice with companies today, and is a reason why it is forecast to become the data storage technology of choice in the coming years.

1.4.8 Secondary storage

Computer storage is made up of primary and secondary storage. Primary storage typically refers to random access memory (RAM) placed near the computer's CPU to reduce the amount of time it takes to move data between the storage and CPU. Secondary storage (sometimes referred to as secondary memory) is at the lower level of the storage hierarchy. It commonly refers to hard disk drives (HDDs), solid-state drive (SSD) storage (flash) or other types of storage devices. Computers use primary and secondary storage for a number of reasons.

• RAM based storage is versatile

• RAM is far more expensive than non-volatile storage on cost-per giga byte

• RAM offers faster read/write speeds: The high speed of RAM enables quick data access and execution of commands, which significantly enhances system performance. This makes it ideal for tasks that require frequent data manipulation, such as running applications or handling real-time data processing.

• Secondary storage provides long-term data retention: Unlike RAM, secondary storage is non-volatile, meaning it retains data even when the power is turned off. This makes secondary storage essential for saving permanent files, operating system data, and user information over extended periods.

Chapter 2

LITERATURE SURVEY

This chapter contains the theories and the background to justify the usage of NAS based solutions in business. When implemented properly, it lowers the risk for a data loss as well as greatly improves the mobility of the work thus allowing employees to work abroad. This chapter contains the basic knowledge of the NAS based solutions as well as different ways to implement them.

RELATED WORKS

Due to the exceptional growth of Internet in the past few years, computing resources are available everywhere. The existing system uses cloud computing for data storage. Cloud Computing Environment consists of two components. a. Infrastructure Providers: Infrastructure providers handle the cloud platforms and rent out resources according to usage b. Service Providers: Service providers lease resources from infrastructure providers and make it available to end users. In spite of this technology having many opportunities and applications in today's world, there still exist a number of challenges which need resolution. The biggest challenge faced is the open characteristic and multi-tenant nature of the cloud. This technology has a huge impact in the field of information security. The various impacts are described in detail below.

1. There is no security boundary in this technology due to features such as dynamic scalability, service abstraction, and location transparency. In

addition there is no fixed infrastructure for the applications and data making it difficult to keep the information secure.

2.There is a need for quick information processing in this kind of storage because the platform will be dealing with large amount of data. The security needs to be in line with this high speed processing.

3. In this type of system, it is difficult to have a common security measure as the resources may belong to multiple providers.

4.There is a possibility of unauthorized user access due to the openness of cloud and sharing virtualized resources by multi-tenant .

2.1 NAS ARCHITECTURE

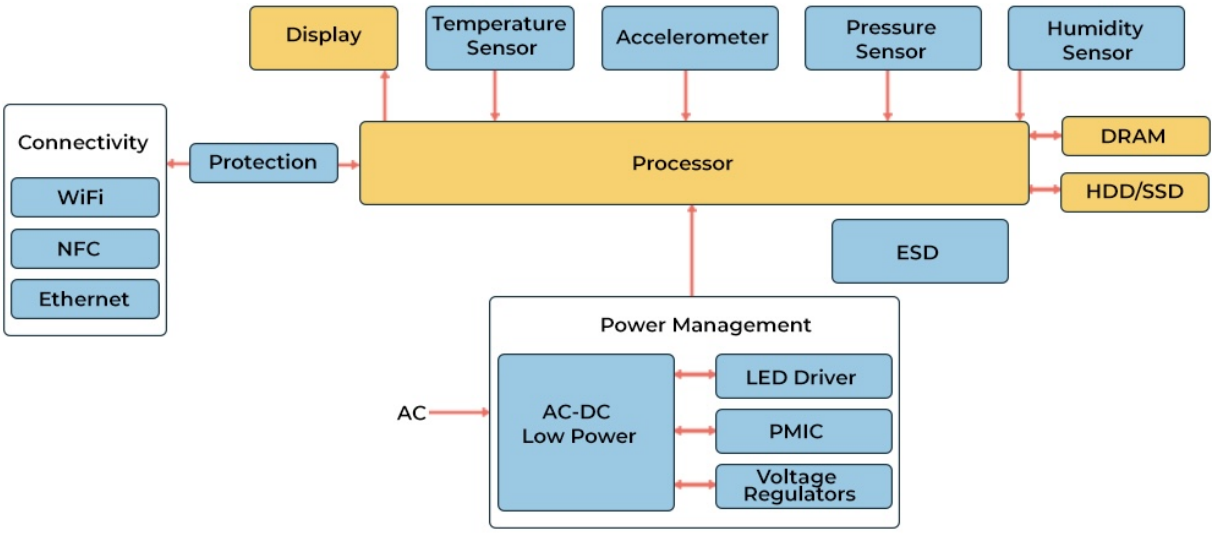


Figure 2.1: NAS Architecture[30]

The above figure shows a typical NAS architecture. NAS helps the organizations to quickly and easily add file storage capacity to their technology infrastructure. NAS focuses mainly on serving files ,while hiding many of the details of the actual file system implementations. NAS appliances are easy to deploy and are self sustained. NAS works well for organization that

need to deliver data to multiple clients over a network. NAS functions well in places where data must be transferred over long distances. NAS can be used for domestic automation of data storage.

2.1.1 STORAGE

There are basically two modes of data storage:
a) Offline storage: This is the storage media that must be manually inserted into the system. The information is safely stored and retrieved when required. The data stored is permanent and its is unaltered until edited by user, the data stored is also more portable and can be accessed easily . eg: hard disk ,pen drives.
b) Online storage: It is a concept of storing of electronic data over a network. This type of data is more secured , portable and can be accessed from any part of the world . It helps in sharing of files among the multiple users at the same time. Networked storage: Networked storage is an online data storage mechanism that uses special devices connected directly to the network media. These devices will be assigned with an IP address and can then be accessed by the clients via the server. The server acts as the gateway to the data. In some cases, networked storage allows the device to be directly accessed without any intermediate source .The biggest advantage of networked storage is expandability.

2.1.2 RASBERRY PI

The raspberry pi is a series of small single board computer developed by the Raspberry pi foundation to promote teaching of basic computer science in schools. The Raspberry Pi platform can run the Linux operating system, which means that the Applications of open source software can be used directly with it.

The SD card inserted into the slot on the board acts as the hard drive to the Raspberry. It is powered by USB and the video output can be viewed on a traditional RCA TV set, a more modern monitor, or even a

TV using a HDMI port .This enables all the basic features of a computer. It also has an extremely low power consumption of 5 watt.

The availability of drivers for opened source software makes the raspberry pi interfaced with devices such as keyboard, camera with USB, and adapter of WIFI, without having any source proprietary alternatives. Raspbian is a Debian based operating system for Raspberry pi. There are several versions available including Raspbian Stretch and Raspbian lassie. The operating system is a UNIX type, open source model. The latest release includes Raspbian Stretch with Desktop .The working platform involves ARM i386 version. The kernal is a monolithic environment.

2.2 NAS Appliance Theory of Operation

A NAS device is essentially a plug-and-play storage appliance, designed to respond to client requests for stored data in real time. NAS devices are well suited to serve networks that have a heterogeneous mix of clients and servers, such as UNIX, Microsoft Windows, and Linux. The NAS appliance can do this by running a suite of file system software compatible with the clients it services. When a client on the LAN requests data from the storage system, the application layer of the client sends a data request over the network to the NAS platform. The local file system of the NAS determines the origin of the request and sends the appropriately formatted data back to the originating client.

A NAS system provides file security, through methods such as "Access Control Lists," and it performs all file and storage services through standard network protocols, including TCP/IP for data transfer, Ethernet for media access, and HTTP, CIFS, and NFS for remote file services. In addition, a high-performance NAS appliance may handle tasks such as Web cache and proxy, audio and video streaming, and tape backup.

2.3 SOFTWARE CONSIDERATIONS

This section provides a comprehensive analysis of the software layers within the solution stack, detailing the role and function of each layer in creating a cohesive and efficient system. It covers key components, including the operating system, file management systems, data protection mechanisms, and user access controls, illustrating how each layer contributes to the overall performance and security of the solution. The section also explores the technical considerations essential for successful software implementation. These considerations include ensuring compatibility between various software components, optimizing the system for high performance, and designing it for scalability to accommodate future growth. Additionally, security measures are a focal point, with particular emphasis on encryption, access control, and authentication protocols, which ensure the integrity and protection of data. Finally, the section highlights potential challenges during implementation and provides strategies for mitigating risks, ensuring the system operates efficiently, securely, and reliably in a dynamic, data-driven environment.

2.3.1 BIOS and Drivers

In addition to the various vendors offering BIOS solutions for Intel processors, equipment manufacturers often develop customized BIOS versions tailored to their specific hardware and system requirements. These custom BIOS versions are designed to optimize the performance, compatibility, and stability of the system, ensuring that the hardware functions seamlessly with the other components. Custom BIOS development can include specialized features such as power management optimizations, hardware-specific settings, or unique configuration options that are crucial for the performance of proprietary systems.

Original Equipment Manufacturers (OEMs), who build and sell hardware solutions, may also develop drivers specifically for their own hardware components, such as hard drives, network adapters, or graphics cards.

These custom drivers are essential to ensure the hardware operates correctly within the system, enabling features like improved speed, reliability, and compatibility with the operating system. In many cases, OEMs will also incorporate drivers provided by Intel or other hardware manufacturers to support third-party components, allowing for broader compatibility and enhanced performance across various systems. This approach ensures that the system operates smoothly, whether the hardware components are proprietary or from third-party manufacturers. Through these efforts, manufacturers aim to deliver highly optimized systems that meet the unique needs of their users, offering a stable and efficient computing experience across a range of devices and applications.

2.3.2 Operating System

The operating system (OS) manages all the software applications and hardware resources on the system. NAS appliances may use off-the-shelf desktop or server operating systems, such as Windows, Linux, or UNIX, or may utilize an embedded OS, such as Windows CE or Embedded Windows NT*. Another alternative is a real-time operating system (RTOS) such as VxWorks* or QNX*.

The main considerations for a NAS OS are the size and performance. Desktop operating systems are easier for the customer to implement, but take up more disk space (which means less storage) and also contain unnecessary overhead that usually degrades performance. An RTOS offers a smaller footprint and may even reside in Flash rather than on disk. Development using an RTOS allows for more direct control of the hardware, enabling optimum performance tuning. However, there is a significant investment required in developing with an RTOS. Plus, this may limit the ability to include value-added functionality, such as using the NAS device as a Web server. Embedded operating systems such as Embedded Windows NT are good alternatives because they are modular and provide tools to allow only the necessary modules to be installed. Many Linux packages also have this

capability. High Availability (HA) is also becoming a key consideration for OS selection. Linux, for example, has an HA initiative underway.

2.3.3 Application Software and Protocols

The application software layer in a Network Attached Storage (NAS) solution can be segmented into several distinct functional areas, each designed to enhance the device's performance, security, and usability. These functional areas include services, access permissions, storage, fault tolerance, and networking. Each of these components plays a critical role in ensuring that the NAS device functions optimally and meets the needs of its users.

The services component typically includes essential features such as file sharing, remote access, and data synchronization. These services allow users to access and manage their data remotely, providing flexibility and convenience. The access permissions layer controls who can access specific files and folders, ensuring that sensitive data is protected from unauthorized access. By defining granular access rights, administrators can ensure that only authorized individuals or devices have access to certain resources.

The storage layer focuses on managing the physical and logical organization of data, ensuring that files are stored efficiently and can be retrieved quickly when needed. NAS devices often support various storage technologies, such as RAID, to improve data redundancy and performance. Fault tolerance is another critical functional area, as it ensures the NAS system can recover from hardware failures without losing data. Techniques such as data replication, RAID configurations, and backup solutions help ensure continuous data availability and system reliability.

Finally, networking ensures seamless communication between the NAS device and client devices over the network. This includes protocols like SMB, NFS, and FTP. Aside from these core functionalities, many NAS manufacturers provide value-added capabilities like encryption, cloud integration,

and advanced backup solutions to differentiate their products from competitors. These additional features enhance the overall user experience and help address specific business needs, making NAS solutions more versatile and secure.

2.3.4 File Systems

The file system in Network Attached Storage (NAS) manages how data is stored, organized, and accessed across the network. It ensures efficient data retrieval, supports multiple file-sharing protocols, and provides features like security, backup, and scalability for users.

1.NFS: The Network File System (NFS) is an application that lets a computer user view, update, or store files on a remote computer as though they were on the user's local hard drive. Most UNIX and Linux operating systems include NFS client and server software.

2.SMB: The Server Message Block (SMB) protocol allows a Windows client to access, create, and update files on a remote server. The protocol also allows the same client to access other resources such as printers and mail slots. The SMB protocol can be used over TCP/IP or other network protocols such as IPX and NetBEUI. Microsoft Windows 95 and later versions of the operating system include client and server SMB protocol support. For UNIX and Linux systems, a shareware program called Samba is available. The SMB protocol originated at Microsoft and has gone through a number of developments, eventually evolving into the CIFS standard.

3.CIFS: Common Internet File System (CIFS) is a standard protocol that enables programs to request files and services on remote computers on the Internet. CIFS is an open variation of SMB. Like SMB, CIFS is built upon the TCP/IP protocol. CIFS is currently the most commonly used protocol for NAS systems because it is readily available on Windows, UNIX, and Linux operating systems, and can also be used in conjunction with Novell*

IPX/SPX protocols.

2.3.5 Networking Protocols

Networking protocols play a critical role in controlling the communication between the Network Attached Storage (NAS) device and other devices within the network. The NAS device itself connects to the network through a physical Ethernet connection, which allows it to communicate with various client devices, servers, and other networked systems. Ethernet is the standard communication medium for NAS devices, providing a stable and high-speed connection to facilitate data transfers.

Since NAS devices are designed to provide seamless access to data over a local area network (LAN), they typically support multiple networking protocols to ensure compatibility with different systems and applications. One of the most fundamental protocols used in NAS systems is TCP/IP (Transmission Control Protocol/Internet Protocol), which serves as the core communication language for the Internet and most modern networks. TCP/IP is essential for enabling devices on a network to communicate with each other, establishing reliable connections, and ensuring data is transmitted without errors.

In addition to the basic TCP/IP protocol, NAS devices also support higher-level protocols built on top of TCP/IP to handle specific types of data transfer. For example, HTTP (Hypertext Transfer Protocol) is commonly used for web-based interactions, allowing users to access files via a browser interface. FTP (File Transfer Protocol) is employed for transferring files between systems over the network, while Telnet is used for remote administration of the NAS device through a command-line interface. SMTP (Simple Mail Transfer Protocol) enables the sending of email notifications from the NAS device, often for alerting administrators about system statuses or errors.

By supporting these various networking protocols, NAS devices offer a flexible and robust solution for file sharing, data access, and remote management across diverse network environments. These protocols ensure that the NAS system can efficiently communicate with a wide range of devices and services, enhancing its utility and versatility in different use cases.

2.4 Literature Review

1. David F. Nagle, Gregory R. Ganger, Jeff Butler, Garth Goodson, and Chris Sabol have done project on Network Support for Network-Attached Storage. High- performance, low- latency networking is essential to achieving the potential of scalable network-attached storage. Userlevel networking solutions, such as VIA, have the potential to do this, but must be mindful of the amount of on-drive resources required connection state and buffering can consume considerable resources. However, Remote DMA can help minimize drive resources while providing a great deal of flexibility in drive scheduling and buffer management. Further, VIA's application-level flow control enables aggregation of flow control across arbitrary storage components, something low-level network flow control is not designed to support.[24]

2. Darrell D.E. Long University of California have done project on authenticating networkattached storage. The importance of distributed computing as the pivotal approach to managing computing resources and data is well recognized. Scaling distributed computing solutions is a challenge. Network-attached storage provides a solution for creating scalable network access to data, but requires reliable and efficient authentication techniques to ensure that while data is widely accessible, its content is secure from unauthorized access. The SCARED architecture provides a mechanism for efficient and reliable authentication to network accessible storage. We are building a distributed file system on top of SCARED which we call Brave. It is serverless in the sense that there is no central file server, but it stores all data and metadata on network-attached storage unlike the serverless

file system described earlier.[25]

3. Howard Gobioff, Garth Gibson, and Doug Tyger conducted a project focusing on security for Network Attached Storage Devices (NASD). Their work introduced the NASD architecture, a groundbreaking solution addressing the challenges of achieving high performance and cost-effective input/output (I/O) operations in network-attached storage systems. This innovative approach combined robust security measures with the inherent benefits of NAS, including enhanced scalability and performance.
The NASD architecture enabled clients to leverage the full potential of NAS systems while ensuring the protection of sensitive data. Security was a core aspect of this architecture, addressing the risks associated with data storage and transmission over a network. By integrating security features, the architecture allowed clients to confidently utilize NAS solutions without compromising the integrity or confidentiality of their data.
A central element of their approach was the capability scheme, which ensured secure access control. This scheme involved encapsulating the bearer's access rights to a specific version of a storage object. These rights were protected using a secret key that was shared exclusively between the capability issuer (such as a file manager) and the capability enforcer. This mechanism not only secured access but also maintained strict control over data interactions, ensuring that only authorized entities could perform specific operations on storage objects.
The project's outcomes demonstrated how NAS systems could balance performance, scalability, and security effectively. By addressing key concerns in data security while preserving the advantages of NAS, the NASD architecture set a new benchmark for secure, high-performance network-attached storage solutions.[26]

4. The project Best Practices for running VMware vSphere on Network Attached Storage by Paul Manning. Network Attached Storage has matured significantly in recent years and it offers a solid availability and high

performance foundation for deployment with virtualization environments. Following the best practices outlined in this paper will ensure successful deployments of vSphere on NFS. Many people have deployed both vSphere and VI3 on NFS and are very pleased with the results they are experiencing. NFS offers a very solid storage platform for virtualization. Both performance and availability are holding up to expectations and as best practices are being further defined, the experience of running VMware technology on NFS is proving to be a solid choice of storage protocols. Several storage technology partners are working closely with VMware to further define the best practices and extend the benefits for customers choosing to deployment VMware vSphere on this storage protocol option.[27]

5. Anna Suganthi, Karnavel, and Rajini Girinath.D developed a project focusing on Network Attached Storage (NAS) for data backup over a Local Area Network (LAN). The project aimed to create software capable of efficiently managing critical data within a LAN environment, providing users with robust and reliable data backup solutions.
The software featured multiple functionalities, including the ability to back up files from remote nodes, delete unwanted files from those nodes, and retrieve previously backed-up files. Users could also manage their group memberships by joining or unsubscribing from specific groups, enhancing collaborative workflows. These features were designed to cater to various user requirements while ensuring secure and organized data management.
To improve accessibility and usability, the software included a user-friendly graphical user interface (GUI). This GUI allowed users to perform tasks like writing data to, deleting data from, and retrieving data from the NAS seamlessly, even without extensive technical knowledge. The ease of use ensured that users could interact with the system intuitively.
Additionally, the project emphasized the reliability of data storage by integrating with external storage mediums through NAS.[28]

Chapter 3

PROPOSED WORK

Here in this chapter we will discuss the components we are using. Since this project is purely based on the concepts of networking therefore will discuss all networking related concepts and why we are using Raspberry Pi in the project.

3.1 Block Diagram

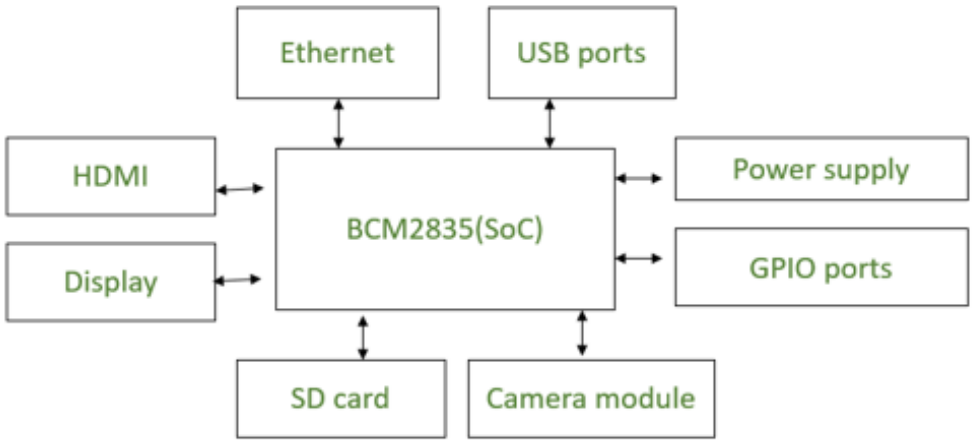


Figure 3.1: Raspberry Pi 4 Block Diagram[31]

The Raspberry is powered by USB and the video output can be viewed on a traditional RCA TV set, a more modern monitor, or even a TV using a HDMI port. This enables all the basic features of a computer. It

also has an extremely low power consumption of 5watt. Offline storage devices are connected through USB port to Raspberry pi and it also has a separate port to connect Ethernet cable. NAS solutions are configured as file serving appliances accessed through the workstations and servers using a network protocl TCP/IP. Network File System (NFS) or Common Internet File system (CIFS) are some of the application used for accessing the file. Most of the NAS connections reside between workstation clients and the NAS file sharing facility.

3.2 NAS vs SAN

The primary difference between NAS and SAN solutions is the type of access protocol. NAS protocols such as NFS and CiFS provide shared file level access to storage resources. The management of the file system resides with the NAS device. SAN protocols such as iSCSI and fiber channel provide block level access to storage resources. Block level devices are accessed by servers via the SAN, and the servers manage the file system. Despite their differences, SAN and NAS are not mutually exclusive, and may be combined in multi-protocol or unified storage arrays, offering both file-level protocols (NAS) and block-level protocols (SAN) from the same system.

Benefits of NAS

• NAS devices typically leverage existing IP networks for connectivity, enabling companies to reduce the price of entry for access to shared storage.
• The RAID and clustering capabilities inherent to modern enterprise NAS devices offer greatly improved availability when compared with traditional direct attached storage.
• Because NAS devices control the file system, they offer increased flexibility when using advanced storage functionality such as snapshots.
• With 10GE connectivity, NAS devices can offer performance on par with many currently installed fiber channel SANs.

3.3 Creating a NAS solution

NAS is a common storage infrastructure offering in data centers worldwide.
Eastern Computer has assisted many of our customers in justifying, designing, and implementing enterprise NAS solutions.
• Lower acquisition and management costs.
• Meet performance and availability requirements.
• Handle ever increasing annual storage growth with minimal to no impact to your business.

3.4 Implementation of NAS

We're going to use Raspberry Pi Imager to install Raspberry PiOS Lite onto your microSD card. Raspberry Pi Imager isavailable for free for Windows, macOS, Ubuntu for x86 and Raspberry Pi OS, and can be downloaded-: https://www.raspberrypi.com/software/

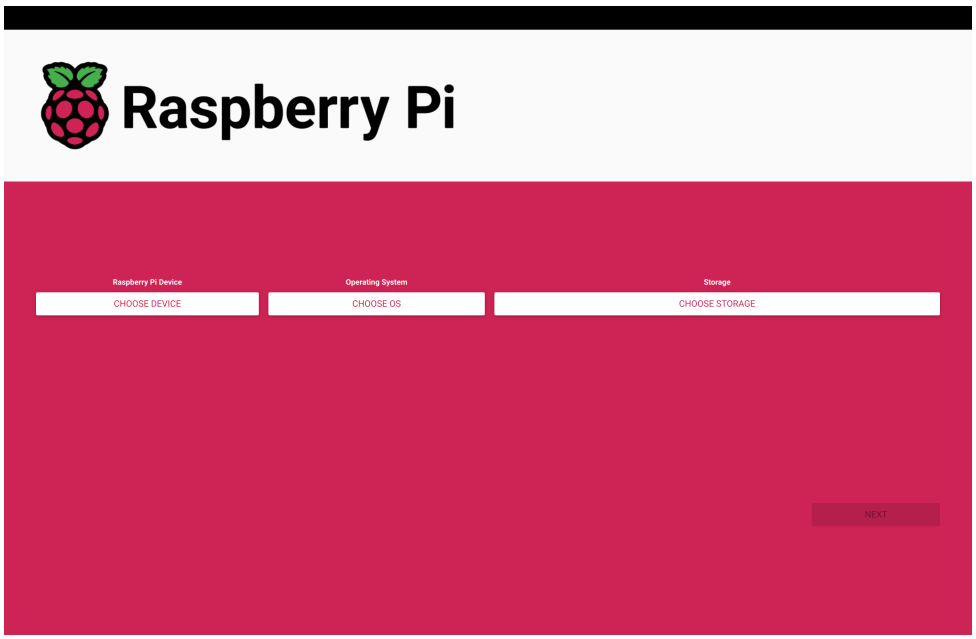


Figure 3.2: Raspberry Pi Imager[32]

Open the Imager application and connect your microSD card to your computer Connect your microSD card to your computer using an SD card adapter. We recommend a minimum storage size of 16GB.

Install Raspberry Pi OS to your microSD card.

Raspberry Pi Imager

CHOOSE OS: Raspberry Pi OS can be found under Raspberry Pi OS (other). We're using the smaller-sized Raspberry Pi OS Lite, as we do not need the desktop environment for our project.

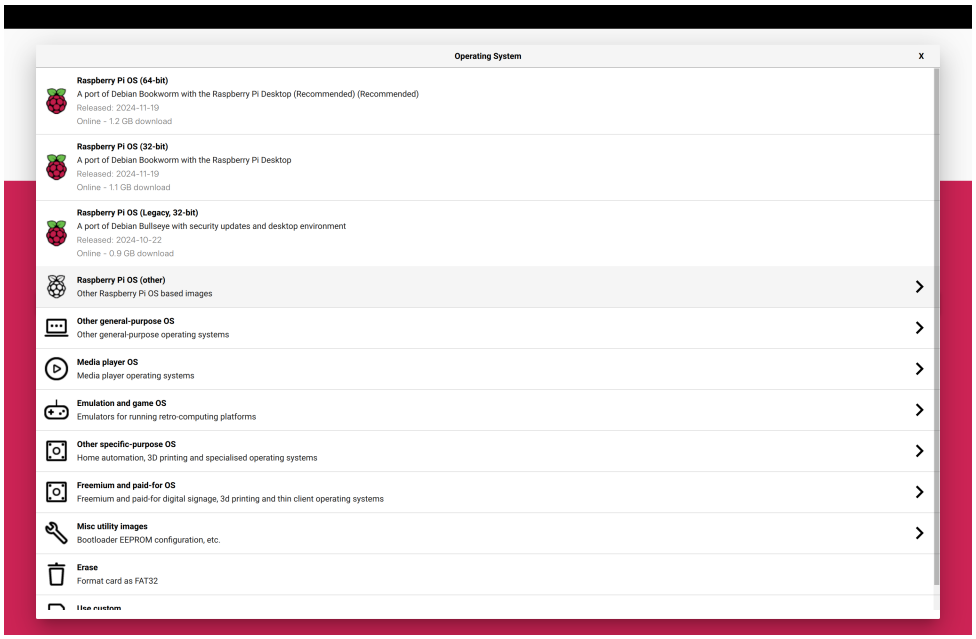


Figure 3.3: OS Selection

To enable SSH using Raspberry Pi Imager, start by opening the Imager and selecting the desired OS and storage device. Once you've chosen the OS and storage, press Ctrl+Shift+X or click the Advanced Menu button to open advanced settings. In the menu, check the Enable SSH box to allow remote access to your Raspberry Pi via SSH. You will be prompted to set a username and password for secure access. Optionally, you can also configure Wi-Fi settings here by entering your network's SSID and password, allowing the Pi to connect to Wi-Fi automatically when it boots. Once you've configured all settings, click Save, and the Imager will write the OS image to your storage device with the SSH and Wi-Fi settings enabled.

When preparing your Raspberry Pi, one of the most crucial steps is select-

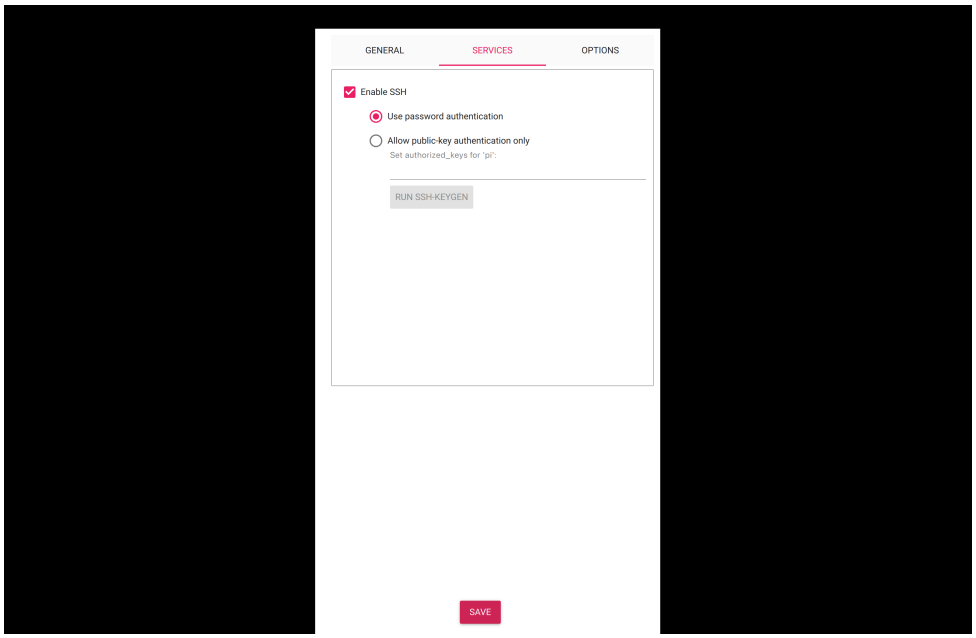


Figure 3.4: Enabling SSH

ing the correct storage device. For most Raspberry Pi models, the primary storage medium is a microSD card, which will house the operating system (OS) and any files or applications you intend to use. In Raspberry Pi Imager, after you've selected the OS you want to install, you'll be prompted to choose the storage device where the OS will be written. At this point, you need to select the microSD card that you've inserted into your computer's card reader. It's essential to ensure that the card has sufficient storage space, with a minimum of 8GB being recommended, though 16GB or larger is ideal for better performance and future expansion. The Imager will show all available storage devices connected to your computer, so it's crucial to double-check that you've selected the correct microSD card. Be careful not to overwrite any other drives or important data. Once you've confirmed the correct microSD card, the Imager will format it and write the selected OS to the card..

Storage options

For now, we will be using different types of storage options, including a portable USB hard drive and an internal hard drive connected via a SATA-to-USB adapter. These external storage devices offer more capacity

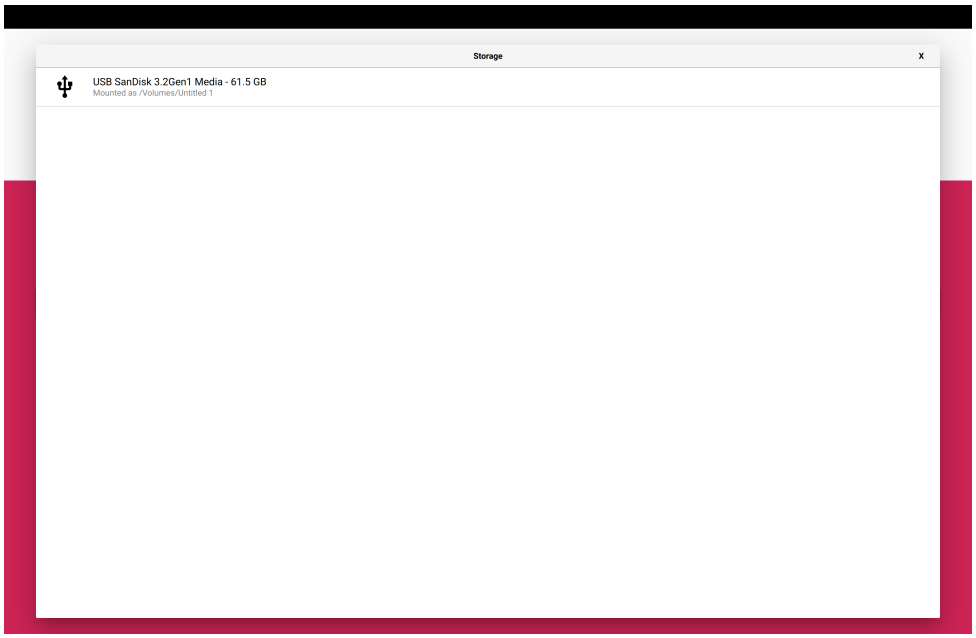


Figure 3.5: Storage Selection

compared to a standard microSD card, making them suitable for users who need additional storage space for their Raspberry Pi projects. While a USB flash drive can also be used, external hard drives generally provide better performance and storage capacity. It's important to clear the drive of any existing data before starting, as you may need to format it during the setup process. Additionally, to ensure a consistent and reliable power supply for the external drives, especially if they are larger and require more power, it is highly recommended to use a powered USB hub. This hub will ensure that your Raspberry Pi can supply adequate power to both the Raspberry Pi itself and the connected hard drives without overloading the USB ports, allowing for stable performance and avoiding power-related issues. Using a powered hub is especially important when dealing with multiple storage devices or high-power external drives.

Setting up your Raspberry Pi

Your Raspberry Pi needs to be connected to your network via an Ethernet cable. For most people, this means connecting the device directly to your router. Once connected, attach your storage to the powered USB hub, and the hub to your Raspberry Pi. Lastly, connect your Raspberry Pi to the

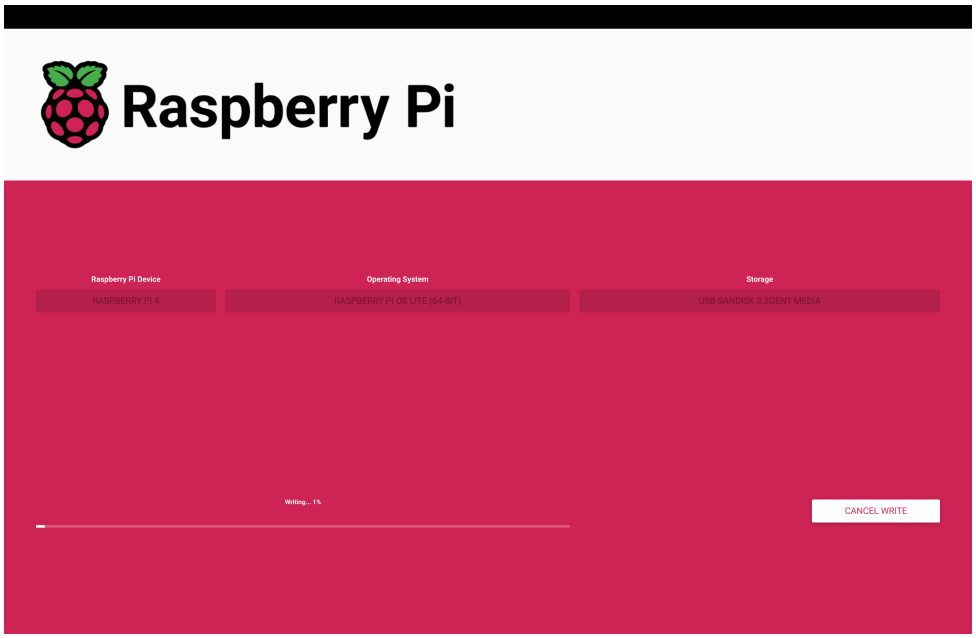


Figure 3.6: OS Installation

mains power via a USB-C power supply unit. Ensure that all cables are securely plugged in and that your power supply meets the required voltage and current specifications for your model. This will help avoid power fluctuations that could disrupt the system.

Retrieving your IP address

In order to access your Raspberry Pi via SSH from your usual computer, you're going to need the Raspberry Pi's IP address. An IP address is a unique string of numbers that identifies a device on your network. The easiest way to find it is to access your home router and check what devices are connected via Ethernet (LAN). The login details for accessing your router should be printed on it (look for a sticker on the side or the base), or alternatively you will be able to find them on the website of the router's manufacturer (or of your ISP if they provided the router).

Connect via PUTTY

PuTTY is an open-source application that supports a variety of network protocols, including SSH, Telnet, SCP, rlogin, serial port, and raw socket connections. It's widely used for remote administration and communication over TCP/IP sockets. While it supports basic protocols like Telnet,

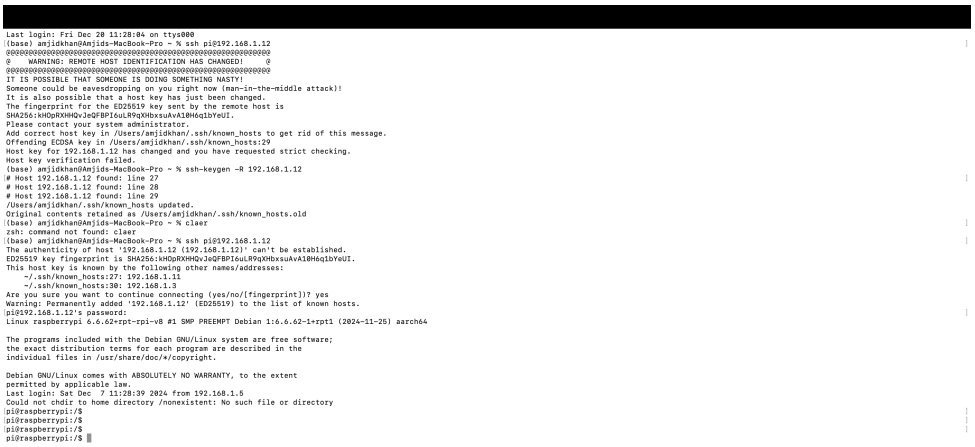


Figure 3.7: Accessing Raspberry pi using SSH

SSH is the most commonly used for secure communication, as it uses public key encryption to ensure a secure connection.

To connect to your Raspberry Pi using PuTTY, first, open the application. In the "Host Name (or IP address)" field, enter the IP address of your Raspberry Pi. Make sure the SSH option is selected under Connection Type. After that, click Open to initiate the connection.

Once you click Open, the Raspberry Pi terminal will appear in a new window, prompting you for the login credentials. You will be asked to enter the username and password you set up earlier. After successful authentication, you will be logged into your Raspberry Pi's terminal remotely, where you can run commands, manage files, and perform various tasks directly from your local machine.Once logged in, you can begin executing commands just as if you were working directly on the Raspberry Pi.

WHAT IS OPENMEDIAVAULT?

Openmediavault is the next generation network attached storage (NAS) solution based on Debian Linux. It contains services like SSH, (S)FTP,

SMB/CIFS, DAAP media server, RSync, BitTorrent client and many more. Thanks to the modular design of the framework it can be enhanced via plugins.

Openmediavault is primarily designed to be used in small offices or home offices, but is not limited to those scenarios. It is a simple and easy to use out-of-the-box solution that will allow everyone to install and administrate a Network Attached Storage without deeper knowledge.

Openmediavault includes the following key features:
Networking:
Link aggregation Wake On Lan, IPv6 support

Volume management:
HDD power management (APM/AAM), GPT partitions, EXT/ EXT4/ XFS/ JFS/ BTRFS/ ... filesystem support, Software RAID JBOD/ 0/ 1/ 5/ 6/ ..., Quota (per volume), ACL, Share management

Monitoring
Syslog, Watchdog, S.M.A.R.T., S N M P (v1/2c/3) (read-only), Email notifications, Proactive process and system state monitoring

Services
SSH, FTP, NFS (v3/v4), SMB/CIFS, RSync

Plugins: With the plugin system it is possible to add additional services Antivirus, DAAP/ MPD/ RSP server ¿ LVM, Shairport, SNMP, TFTP, UPS, USB Backup, Microsoft OneDrive, PhotoPrism, FileBrowser, S3, SSH web console

INSTALLING OPENMEDIAVAULT TO A RASPBERRY PI

Before we install OpenMediaVault, let's update the existing packages by

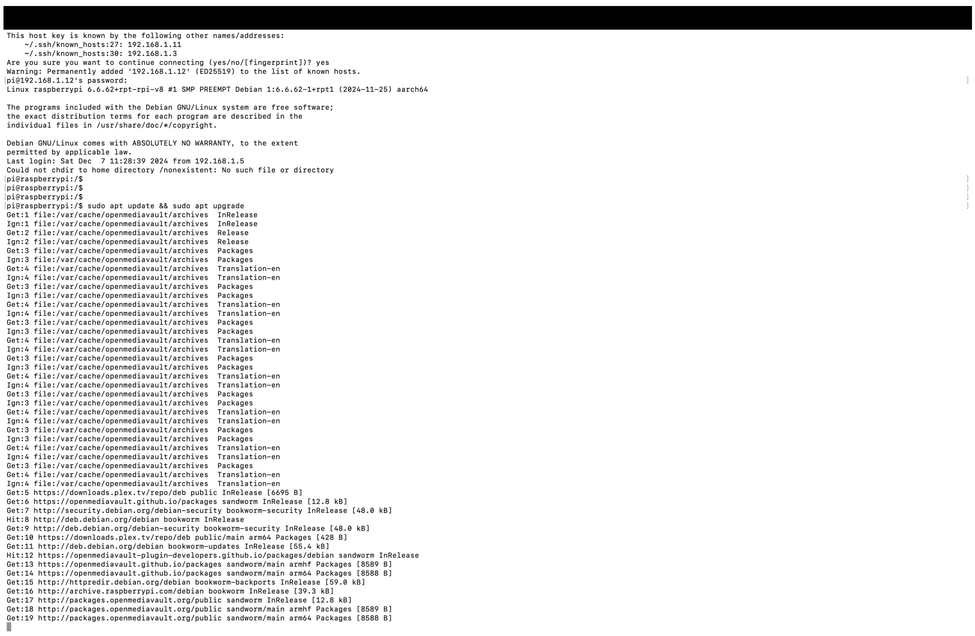
running the following command.

IN TERMINAL:

- sudo apt update
- sudo apt upgrade

Now, to install OpenMediaVault 5 on your Raspberry Pi, we can run a specific command to download the installation script directly from the official repository. This command will use curl or wget to fetch the script and then pipe it through to bash for execution. By doing this, the script will automatically download and install all the necessary packages and dependencies required for OpenMediaVault to run.

wget -O - https://raw.githubusercontent.com/OpenMediaVault-Plugin- Developers/installScript/master/install — sudo bash



```
[redacted]
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:27: 192.168.1.11
    ~/.ssh/known_hosts:30: 192.168.1.3
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.12' (ED25519) to the list of known hosts.
pi@192.168.1.12's password:
Linux raspberrypi 6.6.62+rpt-rpi-v8 #1 SMP PREEMPT Debian 1:6.6.62-1+rpt1 (2024-11-25) aarch64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Dec  7 11:28:39 2024 from 192.168.1.5
Could not chdir to home directory /nonexistent: No such file or directory
pi@raspberrypi:/$
pi@raspberrypi:/$
pi@raspberrypi:/$
pi@raspberrypi:/$ sudo apt update && sudo apt upgrade
Get:1 file:/var/cache/openmediavault/archives  InRelease
Ign:1 file:/var/cache/openmediavault/archives  InRelease
Get:2 file:/var/cache/openmediavault/archives  Release
Ign:2 file:/var/cache/openmediavault/archives  Release
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Ign:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:3 file:/var/cache/openmediavault/archives  Packages
Get:4 file:/var/cache/openmediavault/archives  Translation-en
Ign:4 file:/var/cache/openmediavault/archives  Translation-en
Get:5 https://downloads.plex.tv/repo/deb public InRelease [6695 B]
Get:6 https://openmediavault.github.io/packages sandworm InRelease [12.8 kB]
Get:7 http://security.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Hit:8 http://deb.debian.org/debian bookworm InRelease
Get:9 http://deb.debian.org/debian-security bookworm-security InRelease [48.0 kB]
Get:10 https://downloads.plex.tv/repo/deb public/main arm64 Packages [428 B]
Get:11 http://deb.debian.org/debian bookworm-updates InRelease [55.4 kB]
Hit:12 https://openmediavault-plugin-developers.github.io/packages/debian sandworm InRelease
Get:13 https://openmediavault.github.io/packages sandworm/main armhf Packages [8589 B]
Get:14 https://openmediavault.github.io/packages sandworm/main arm64 Packages [8588 B]
Get:15 http://httpredir.debian.org/debian bookworm-backports InRelease [59.0 kB]
Get:16 http://archive.raspberrypi.com/debian bookworm InRelease [39.3 kB]
Get:17 http://packages.openmediavault.org/public sandworm InRelease [12.8 kB]
Get:18 http://packages.openmediavault.org/public sandworm/main armhf Packages [8589 B]
Get:19 http://packages.openmediavault.org/public sandworm/main arm64 Packages [8588 B]
```

Figure 3.8: OpenMediaVault Installation

SETTING UP OPENMEDIAVAULT

Open the internet browser on your usual computer and type your Raspberry Pi's IP address into the address bar.

After finishing the installation, you will be prompted with a login screen

when accessing the OMV server thru your web browser. It is in the installation manual. Ididn't see it the first time either.

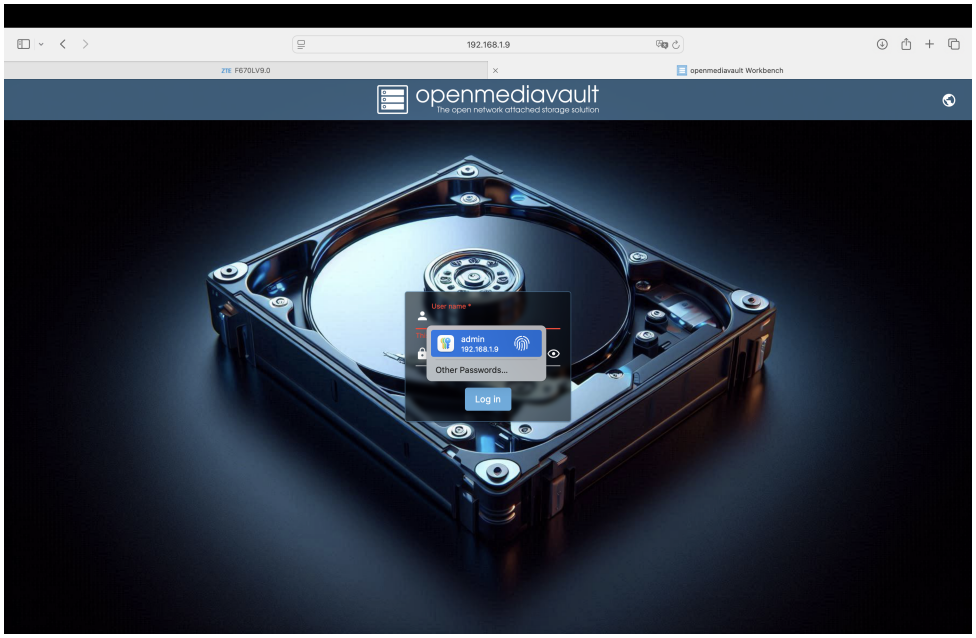


Figure 3.9: Signing in to OpenMediaVault[33]

Sign in to OpenMediaVault using the following credentials:
Username: admin
Password: openmediavault
To change your OpenMediaVault admin password, start by logging into the OpenMediaVault web interface. Once logged in, locate and click the "cog" icon in the top right corner of the screen. This icon opens the Settings menu, where you can access various system preferences. In the settings menu, look for the option to change the admin password. You will be prompted to enter your current password followed by the new password you want to set.

CREATING AN SMB/CIFS SHARE USING OPENMEDIAVAULT
Once your USB drive is wiped and formatted, the next step is to create a file system on the device. To do this, go to Storage ¿ File Systems in the OpenMediaVault interface, then click Create to select the formatted USB device. Choose the file system type, typically ext4, which is compatible

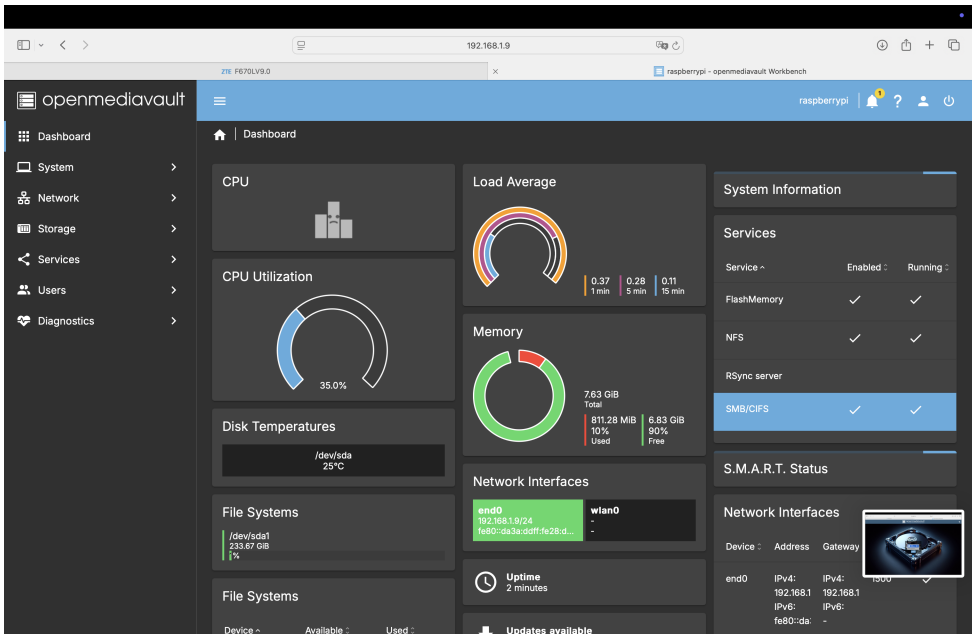


Figure 3.10: OpenMediaVault Interface

with OpenMediaVault. After creating the file system, the drive will appear in the list of available file systems. Select the drive and click Mount to make it accessible.

Now that the drive is prepared, go to Access Rights Management to configure user permissions, ensuring the correct individuals or devices can access the shared folder. Next, navigate to Services ¿ SMB/CIFS and enable the SMB/CIFS service. This step will allow your OpenMediaVault server to share the storage over the network using the SMB protocol. You can then create a shared folder on the mounted USB drive, specify its access rights, and determine whether it's publicly or privately accessible. Once everything is configured, the shared folder will be available for access from other devices on the same network, making it easy to store and share files.
Next, navigate to Storage and then select File Systems in the OpenMediaVault interface. At this point, you likely won't see any drives listed because you haven't yet created a file system on the device. To proceed, click on Create. This will bring up a dialog where you can choose the storage device that you formatted earlier, such as your USB HDD/SSD or thumb drive. Once you've selected the appropriate device, choose EXT4 as the

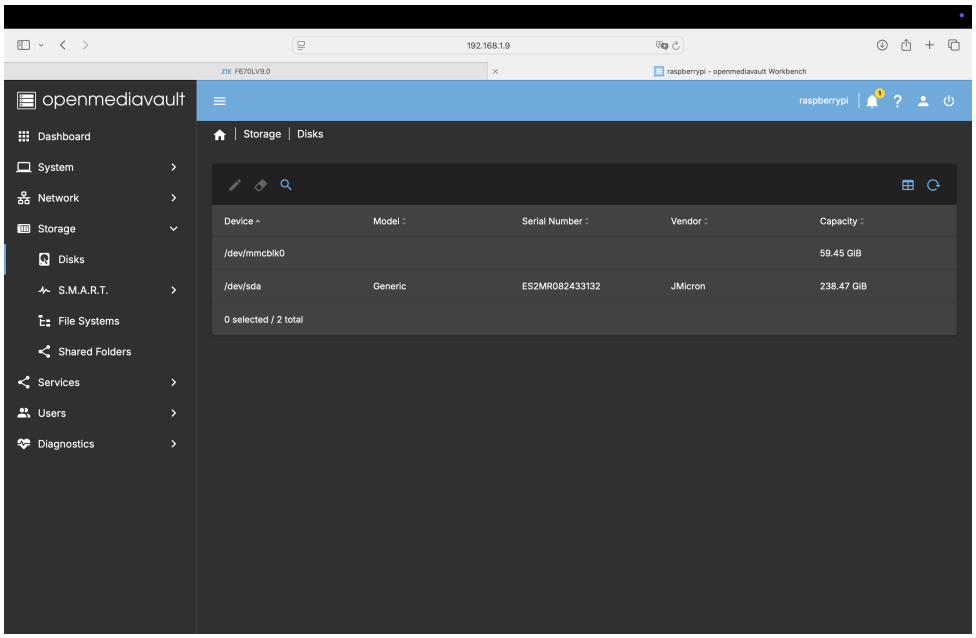


Figure 3.11: OpenMediaVault File System

file system format. The EXT4 format is commonly used in Linux systems and works well with OpenMediaVault for managing large amounts of data efficiently. After selecting the format, click OK to confirm your choice. Once the file system is created, close the window. The drive will now be ready to use, and you can proceed to mount it and configure it for file sharing or other purposes.

Once the file system is created, go back to the File Systems tab, and you should now see your newly formatted drive listed. To make the drive accessible, select it and click Mount. This will mount the drive to your system, making it available for use. After mounting, you can proceed to configure it for shared storage, set up folders, and assign the appropriate access permissions for users or devices on your network.

Now, you can share a folder on your newly configured storage device. To do this, go to Access Rights Management and select Shared Folders from the menu. Once in the Shared Folders section, click on Create to initiate the process of creating a new shared folder.
In the dialog that appears, type in a Name for your shared folder. This

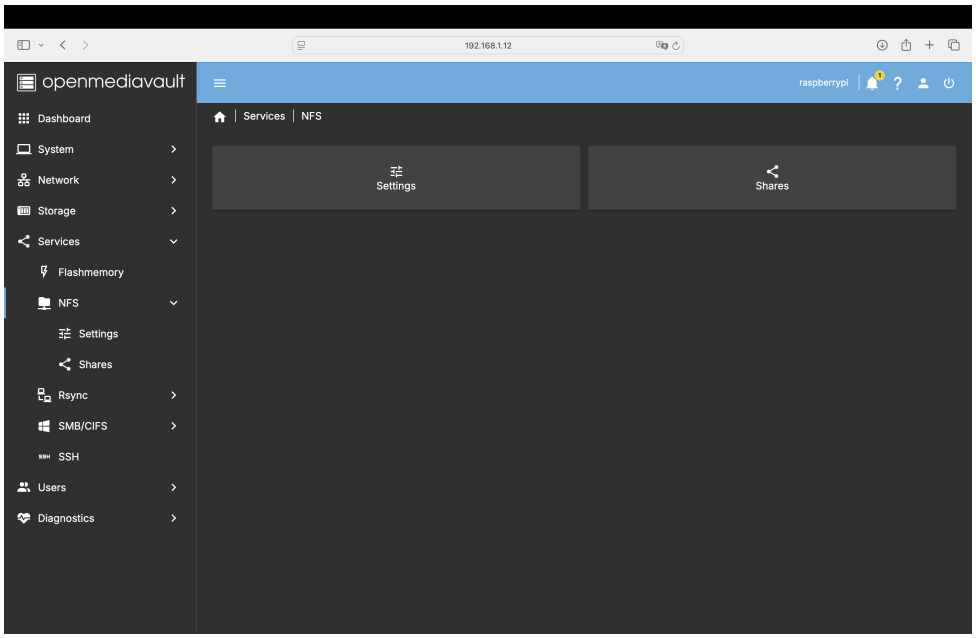


Figure 3.12: Enabling NFS

is the name that will be used to identify the folder on the network. Next, from the Device dropdown menu, select the file system you created earlier, which will be the storage device you want to use for this shared folder. After selecting the storage device, you'll be prompted to set the folder's permissions using the Permissions dropdown menu. Here, you can decide whether the folder will be read-only, read-write, or have specific user access rights, depending on your needs.
Once you've entered the folder name and set the desired permissions, click Save to create the shared folder. Your folder will now be available for access by other devices on your network, based on the permissions you've set. You can further manage user access and adjust permissions later if needed, ensuring secure and controlled access to the shared files. To make the folder accessible over the network, you will also need to enable the SMB/CIFS service, which can be done under Services ¿ SMB/CIFS in the OpenMediaVault settings.

Navigate to Storage and then select Shared Folders in the OpenMediaVault interface. Once in the Shared Folders section, click on Create to initiate the process of creating a new shared folder.

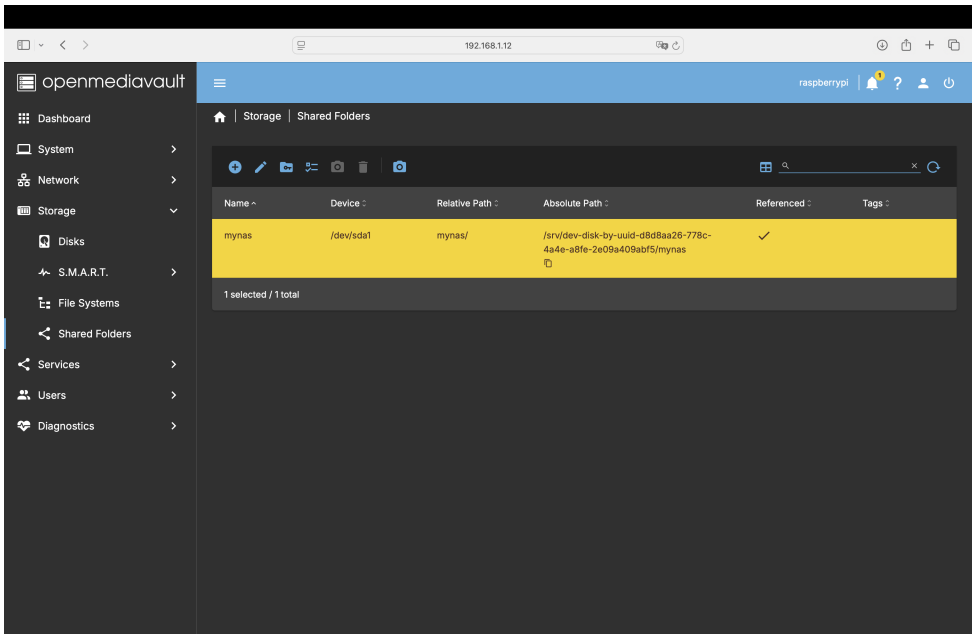


Figure 3.13: Creating Shared Folder

In the dialog that appears, you can name the folder according to your preferences. Next, select the drive where the folder will be stored, which is the device you previously formatted and mounted. After selecting the appropriate drive, you'll need to set the permissions for the folder. By default, the permissions are usually set to allow the owner full access, but you can adjust them based on your network needs. You can grant read-only or read-write permissions, or even restrict access to specific users if required for enhanced security. After configuring the name, drive, and permissions, click Save to create the shared folder. Then, apply the changes to finalize the setup.

Next, to ensure that the shared folder is accessible by other devices on your network, navigate to Services and select SMB/CIFS. This service is required to share files using the SMB protocol, which is compatible with most operating systems. Enable the SMB/CIFS service, then configure the settings as needed, ensuring that the shared folder is visible and accessible to other computers on the same network. Once the service is enabled, your shared folder will be available for file sharing across your network.

Under the Settings section of the SMB/CIFS configuration, make sure to

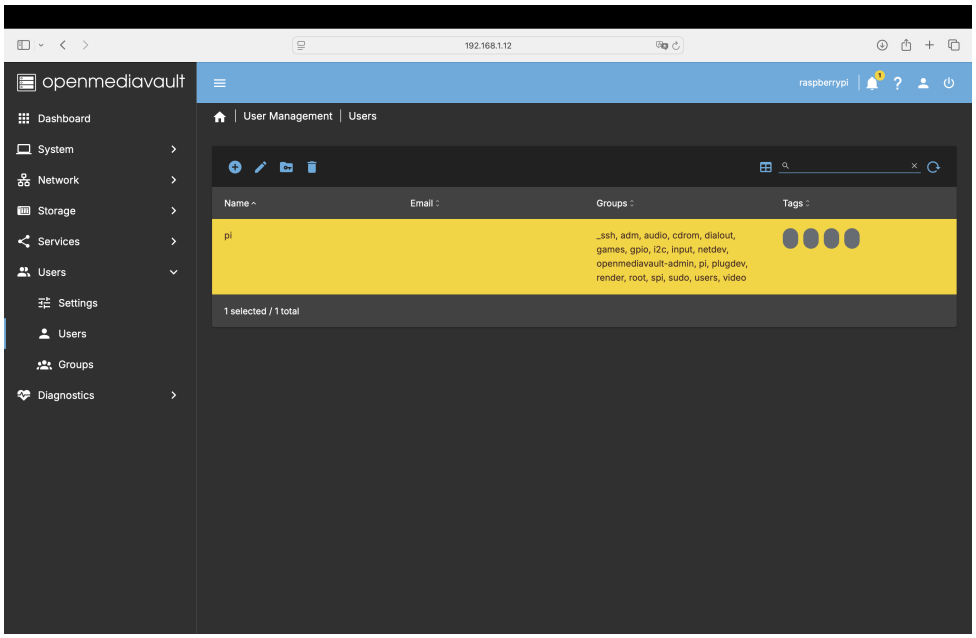


Figure 3.14: Enabling User Access

check the Enabled box to activate the SMB service. After this, click Save to apply the changes. Enabling this service allows your Raspberry Pi or OpenMediaVault server to share files across the network using the SMB protocol, which is widely compatible with various operating systems such as Windows, macOS, and Linux.

Next, navigate to the Shares section and click on Create to set up the specific shared folder. Here, you will need to select the shared folder you created earlier from the list of available folders. You can also configure additional settings, such as setting the folder to be publicly accessible or requiring user authentication for access. Once you've selected the folder and configured the settings according to your preferences, click Save to finalize the shared folder setup.

After completing these steps, your NAS (Network-Attached Storage) system should now be ready to use. The shared folder will be accessible from other devices on your network, allowing you to easily store and retrieve files from the Raspberry Pi or OpenMediaVault server. You can now access the shared folder through SMB from any device on the same network, making your Raspberry Pi a fully functional file server.

Access your NAS from Windows

Open Windows Explorer on your Windows machine. In the address bar (path bar), type

IP address of your Raspberry Pi (replace IP address of your Raspberry Pi with the actual IP address of your Raspberry Pi or OpenMediaVault server). Press Enter, and this should create a new entry under Network in the left navigation panel. This will display the shared folders and contents available on your Raspberry Pi or OpenMediaVault server. You can now browse through the folders you've shared.

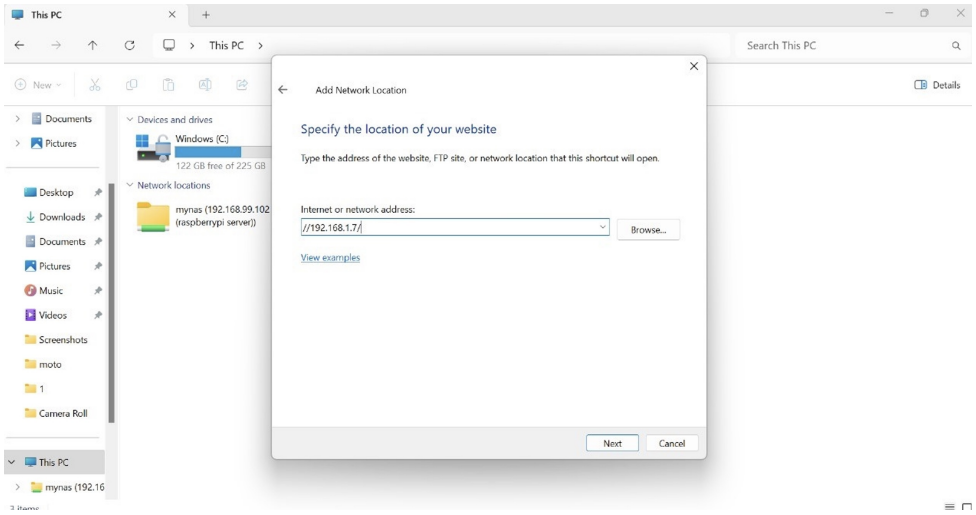


Figure 3.15: Adding Network Location

When you double-click on the shared folder you want to access, a login prompt will appear. Enter the username and password that you created during the setup process in Raspberry Pi Imager. This authentication ensures that only authorized users can access the shared folders. After entering your credentials, click OK, and you will have access to the shared files. You can now view, edit, or transfer files between your Windows machine and your Raspberry Pi or OpenMediaVault server. If you wish to map the network drive for easier access in the future, you can right-click on the shared folder and select Map Network Drive, which will make it appear as a drive in This PC for quicker access.

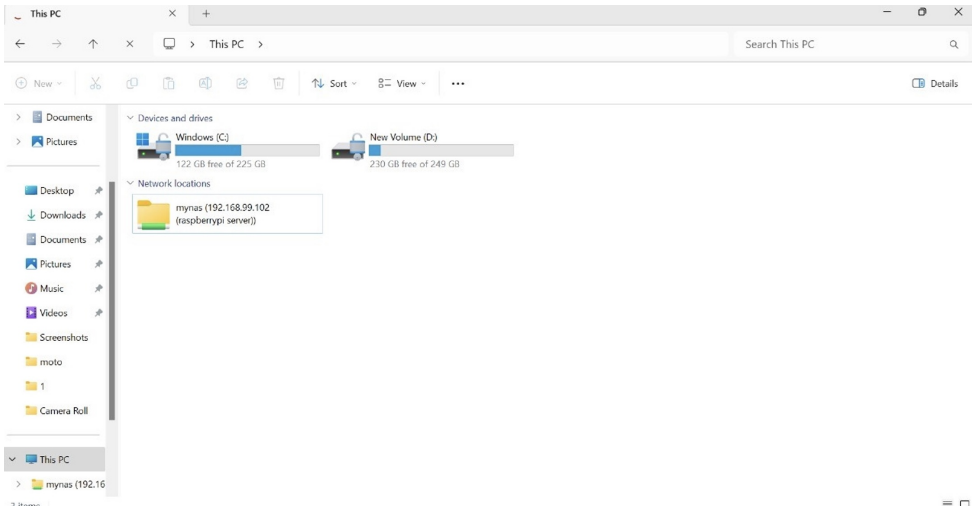


Figure 3.16: Start Using the NAS

3.5 Installing Plex Media Server

A Plex Media Server is a powerful software that acts as a home theater PC, allowing you to organize, stream, and enjoy media content across a variety of devices. Whether it's movies, TV shows, music, or photos, Plex can stream your media content to Plex's front-end media player client applications. These clients run on a wide range of devices such as smart TVs, gaming consoles, smartphones, tablets, and web browsers. This makes it easy to access your media from anywhere in your home or even remotely, depending on your setup.

To install Plex Media Server on your Raspberry Pi or OpenMediaVault system, you can use a simple command. Open the terminal on your Raspberry Pi or through SSH if you're accessing it remotely.

Enter the following command:sudo apt install plexmediaserver

This command will download and install the Plex Media Server package from the official repository. Once the installation is complete, Plex will automatically start running as a background service. You can then access the Plex web interface through a web browser by typing http://your pi ip address:32400/web, where your pi ip address is the local IP address of your Raspberry Pi. From there, you can set up your Plex Media Server, configure your media libraries, and start streaming content to your connected

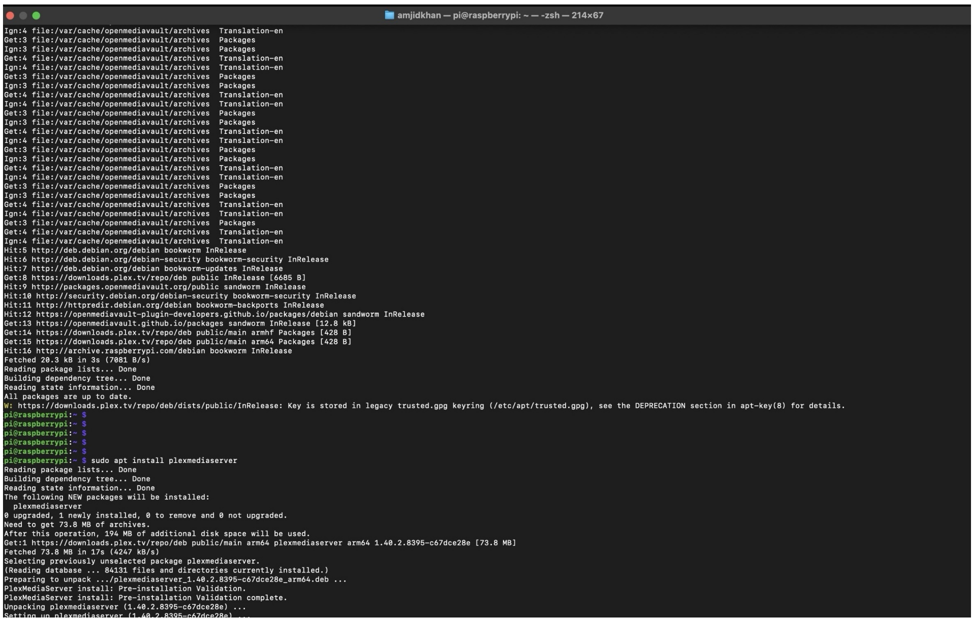


Figure 3.17: Installing Plex Media Server

devices.

This setup allows you to transform your Raspberry Pi into a full-featured media server, enabling you to enjoy your digital media collection effortlessly on multiple devices.

Enabling UPnP for External Access to Plex Media Server

To access your Plex Media Server outside of your local network, enabling Universal Plug and Play (UPnP) is a convenient solution. UPnP allows devices and applications to automatically discover and communicate with each other over a network, simplifying the process of setting up port forwarding. When enabled, UPnP will automatically configure your router to open the necessary ports, allowing external devices to connect to your Plex server without the need for manual port forwarding. To enable UPnP for Plex, go to your router's settings and activate the UPnP option. On Plex, this allows remote access to your media, meaning you can stream your content while away from home, whether on mobile devices or through a web browser, as long as the Plex app supports it.

Accessing Plex Media Server

To access your Plex Media Server, you can use any web browser on a device

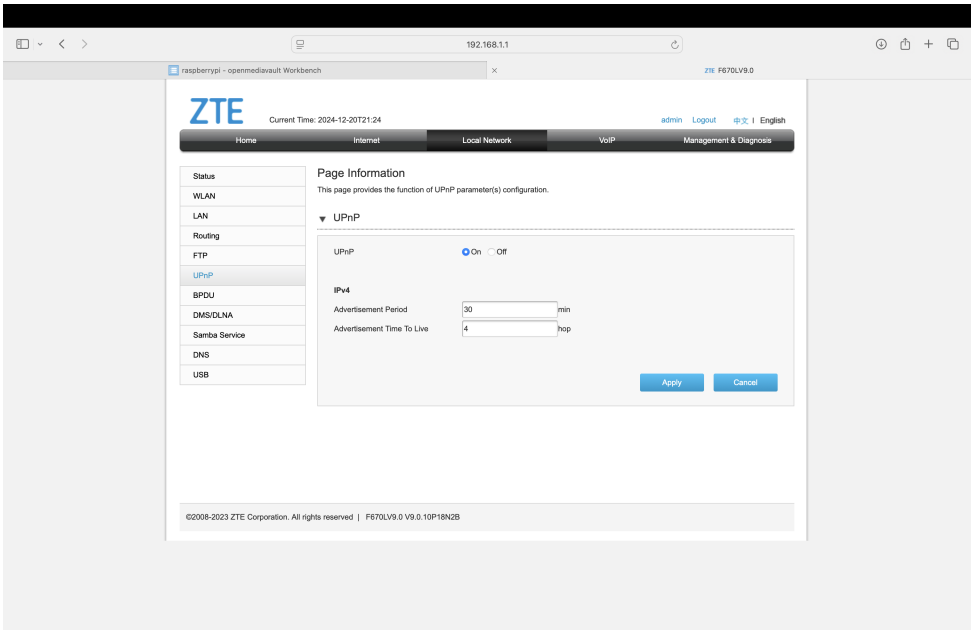


Figure 3.18: Enabling UPNP

connected to the same network as your server. Open the browser and enter the IP address of your Raspberry Pi or OpenMediaVault server, followed by the port number and the /web suffix to reach the Plex web interface. For example, if your Raspberry Pi's IP address is 192.168.1.7, you would enter the following in the browser's address bar:

http://192.168.1.7:32400/web

The port 32400 is the default port for Plex Media Server, and adding /web at the end directs you to the web interface where you can manage your media libraries, settings, and streaming options.

Once you enter the URL, you'll be prompted to log in to your Plex account. If you don't have an account, you can create one during this process. After logging in, you can begin organizing your media libraries, adding content, and streaming to various devices within your network. This web interface provides an intuitive way to control your Plex server, and you can manage settings, update libraries, and stream content directly from the browser.

Logging Into Your Plex Account: When you first visit the web interface, you'll be prompted to log into your Plex account. If you don't have a Plex account yet, there will be an option to create one. Signing up is free,

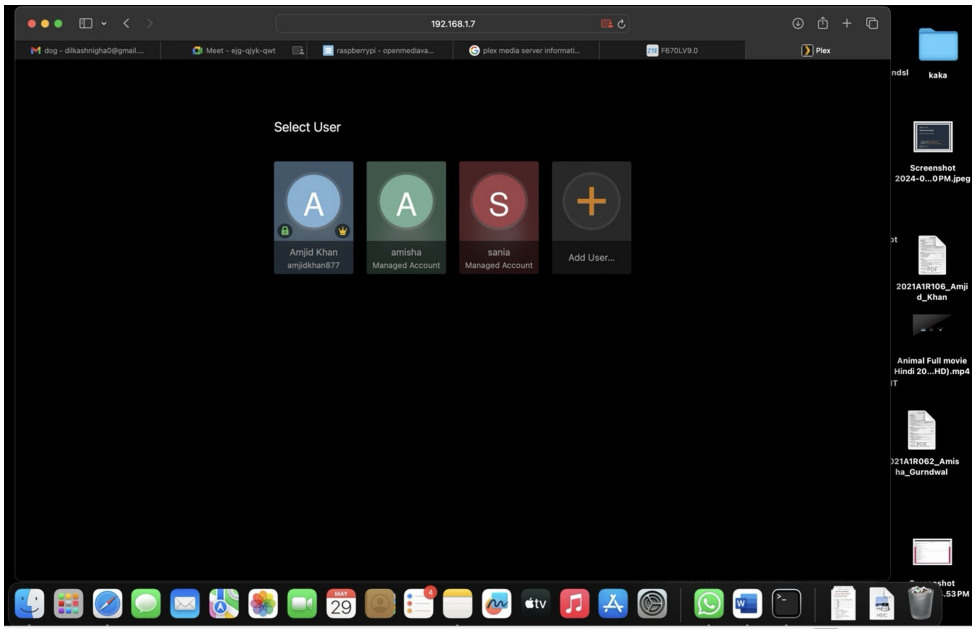


Figure 3.19: Start Using Plex[34]

and it gives you access to a variety of features, including syncing media across devices, managing your library, and streaming content on multiple platforms.

If you already have an account, simply enter your credentials (email and password) to log in. Once logged in, you gain access to your personal media collection, which can be organized and updated within the interface.

Organizing Media Libraries: One of the core functions of Plex is to help users organize their media files, such as movies, TV shows, music, photos, and home videos. The web interface provides intuitive options to add and categorize your media. You can set up different libraries for each type of content and let Plex automatically fetch metadata such as movie posters, actor information, descriptions, and ratings from online databases. You can also manually update libraries, edit metadata, or remove content. Plex will constantly scan your media directories to ensure that any new files added are automatically incorporated into your libraries.

Chapter 4

Results

4.1 Use cases –analysis

The use cases for a functional Network Attached Storage (NAS) system emphasize the need for seamless external connectivity to users. This feature is particularly critical in today's globalized business environment, where data must be accessible worldwide. The growing trend of remote work further underscores the necessity for systems that allow users to access needed files securely and efficiently from any location. Below is an expanded discussion of the primary aspects of NAS use cases, including usability considerations and its applications for centralized data systems in homes.

Figure 4.1: NAS setup at Home

Global Accessibility and Remote Work Enablement

In a globalized economy, businesses operate across multiple locations and time zones. For companies to remain competitive, it is essential to ensure that their data storage systems can provide reliable access to authorized users regardless of geographic location.

Remote Work Support: NAS systems empower remote workers by enabling secure access to the company's data storage infrastructure. Employees can retrieve, modify, and upload critical documents in real-time, ensuring uninterrupted productivity.

Granular Access Control: Advanced NAS configurations allow administrators to define specific access rights for users. For example, clients or employees may be granted access only to certain documents or folders, ensuring that sensitive information remains protected. This capability not only boosts efficiency but also supports modern work models, where flexibility and mobility are essential.

User-Friendly Usability Features

A user-centric NAS system should be designed with usability in mind, providing intuitive and practical solutions for interacting with data storage.

Network Drive Integration: To enhance the user experience, NAS systems should allow data storage folders and drives to appear as network drives on user devices. This integration eliminates the need for complex navigation, enabling users to access files directly through their operating system's file explorer.

User-Specific Drives: Each user should have at least one dedicated network drive that is accessible exclusively to them. This private drive ensures a secure environment for sensitive data and enables users to store personal work without concerns about unauthorized access.

Shared Drives for Collaboration: A shared network drive accessible to all users fosters collaboration by providing a common space for team projects, file sharing, and resource management. This shared resource simplifies teamwork and improves communication within organizations.

Centralized Data Management for Homes

While NAS systems are widely used in business environments, their applications in residential settings are growing. A centralized NAS system in a home can significantly enhance data organization, accessibility, and security for families and individuals.

Unified Storage Solution: A home NAS can consolidate data from multiple devices—such as computers, smartphones, and tablets—into a single, centralized location. This simplifies data management, ensuring that all files are organized and easily accessible.

Media Servers: NAS systems can serve as dedicated media servers, allowing households to store and stream music, movies, and photos across various devices. Popular NAS solutions offer compatibility with media applications, enabling seamless playback on smart TVs, gaming consoles, and mobile devices.

Data Backup and Security: Home NAS systems provide reliable backup solutions for personal data, such as family photos, videos, and important documents. Features like RAID configurations and scheduled backups protect against data loss due to hardware failures or accidental deletions.

Remote Access for Families: Just as businesses benefit from remote access, families can use NAS systems to retrieve files while traveling or sharing content with distant relatives. Secure remote access ensures that personal data remains protected even when accessed outside the home.

Whether in business or residential use, the versatility and functionality of NAS systems make them indispensable in today's interconnected world. For businesses, global accessibility and remote work support are key drivers of productivity and efficiency. Usability features such as network drive integration, user-specific drives, and shared folders enhance the experience, making NAS systems practical for users of all technical skill levels.

For homes, centralized NAS systems provide a unified solution for man-

aging personal data, serving as both a backup system and a media hub. By addressing the diverse needs of both professional and personal users, NAS systems continue to demonstrate their value as scalable, secure, and user-friendly storage solutions, ensuring data accessibility and protection in every setting.

4.2 Features –analysis

The NAS architecture outlined in this system design emphasizes key features that cater to both functionality and security, with a particular focus on user-specific network drives, shared folders, and backup strategies. These features aim to address the growing need for efficient, secure, and scalable data management solutions, with an understanding of the practical constraints and potential challenges. Below is a deeper exploration of these aspects and their future implications.

User-Specific Network Drives: Priority for Security and Personalization

The greatest priority within this NAS system design is the configuration of user-specific network drives. These personalized drives are essential for providing secure, controlled access to individual users, ensuring that sensitive data remains isolated and protected from unauthorized access. Configuring these drives is relatively straightforward with the use of appropriate software solutions, enabling administrators to define clear access permissions.

Security and Access Control: By creating user-specific network drives, the system guarantees that only authorized individuals can read, write, or modify files within their designated storage areas. This level of granularity in access control provides both privacy and security for each user's data.

Data Personalization: For users, having a dedicated network drive creates a tailored storage environment, where their documents, files, and configurations are easily accessible from any device connected to the network. This approach simplifies collaboration while preserving data security.

Shared Folder: A Key Resource for Collaborative Work

In addition to user-specific drives, the common folder serves as an essential feature in this NAS system. The common folder is a shared space accessible by multiple users, enabling team collaboration, file sharing, and efficient data management across the network. Configuring the shared folder is just as straightforward as setting up the user-specific network drives, offering a balance of simplicity and functionality.

Data Redundancy and Security: One of the significant advantages of the common folder is its ability to provide a backup for important files that may be lost or corrupted on primary devices. For example, if a user accidentally deletes or loses a file from their personal network drive, it can often be retrieved from the common folder. The shared folder also acts as a central repository for essential company-wide documents or family resources, ensuring all users have access to the same data.

Collaboration and Efficiency: Whether for business or personal use, the common folder streamlines the sharing of information, making it easy for users to collaborate on projects or access shared resources without duplicating efforts or creating versions of documents scattered across multiple drives.

Backup Features: Future Implementation Plans and Workarounds

While the backup feature is recognized as a crucial aspect of any NAS system, it has not been implemented in this specific design due to budget constraints. Nonetheless, the need for a reliable backup solution remains paramount, and plans for its implementation are set for the future.

Future Integration of Backup: The inclusion of automated backup mechanisms will provide users with the ability to safeguard their data by regularly duplicating files to another storage medium, whether it's an external hard drive or cloud-based storage. This would further enhance the reliability of the NAS system, particularly in the event of hardware failure or unforeseen data loss.

Interim Solution - External Storage: In the interim, an optional workaround is to perform regular backups to an external storage device. This external storage would be stored in a secure offsite location after each backup operation. While this manual approach requires more user intervention, it remains a feasible solution for maintaining data integrity in the absence of a full-fledged automated backup system.
Though this workaround is not as streamlined as a fully integrated backup feature, it offers a degree of protection against data loss and ensures that critical information is preserved in a separate location, mitigating the risks of catastrophic hardware failure.

Web-Based User Management: Risks and Limitations
Another feature considered for the NAS system was web-based user management. While this feature might appear appealing due to its ease of access and centralized control, it presents significant risks that could ultimately undermine the system's security and reliability.
Ease of Access vs. Risk of Errors: The idea of managing users through a web interface offers convenience and flexibility, allowing administrators to quickly add or remove users, assign permissions, and manage access rights from any device with an internet connection. However, the risks associated with this method are considerable.
Potential for Accidental User Removals: One of the primary concerns with web-based user management is the risk of accidental user deletions. In a web interface, a user might unintentionally remove another user's access or privileges, which could result in severe consequences, such as unauthorized data access or complete loss of critical data if the system fails to backup or restore user configurations properly. This could lead to substantial operational disruptions and data integrity issues.
Lack of Granular Control: In a traditional system with more manual or local user management, administrators can apply stricter controls, reducing the chances of unintended actions that might result in data loss. Given the potential for human error, the decision was made to forgo the

implementation of a web-based management system at this time.
While the desire for convenience is understandable, ensuring that security and operational stability remain intact is of greater importance, especially in systems dealing with critical business or personal data.

The current NAS architecture strikes a balance between functionality, security, and practical constraints. By prioritizing user-specific network drives and a common shared folder, the system enhances both individual privacy and collaboration. Although the backup feature has been deferred due to budget considerations, interim solutions like external storage provide a reasonable workaround.

The decision to exclude web-based user management reflects a careful consideration of the potential risks, ensuring that the integrity of the system is preserved and that users' data remains secure. As the NAS system evolves, additional features, including automated backups and more sophisticated management tools, will likely be integrated. However, the priority remains on creating a secure, efficient, and scalable solution that meets both user needs and organizational requirements.

Chapter 5

Conclusion and Future Work

5.1 CONCLUSION

The implemented Network Attached Storage (NAS) architecture introduces a transformative approach to modern data storage, prioritizing high performance, cost efficiency, and robust security measures. By combining state-of-the-art technologies and innovative methodologies, this NAS architecture empowers organizations to fully exploit the performance potential of centralized storage while ensuring the highest level of data protection.

Scalability Without Compromising Security
The inherent scalability of NAS systems is a key advantage, enabling seamless expansion to accommodate growing data demands. This is achieved without compromising data security, making NAS an ideal solution for organizations experiencing rapid growth. Businesses can incrementally increase their storage capacity as needed, eliminating the need for costly and disruptive overhauls. Such scalability ensures NAS remains a future-proof investment in an ever-expanding digital landscape.

Innovative Capability Scheme for Enhanced Security
A core innovation in this architecture is the implementation of a capability scheme that encapsulates bearer access rights to specific versions of storage objects. By utilizing a shared secret key between clients, this scheme provides an additional layer of security, ensuring that only authorized users

can access and manipulate data. This approach addresses critical concerns related to data integrity and unauthorized access while streamlining access control processes. It also offers a robust framework for managing secure data access, particularly for businesses handling sensitive or regulated information.

The Role of NAS in Modern IT Operations

In today's business environment, Information Technology (IT) is a cornerstone of daily operations. Even small organizations generate significant amounts of valuable data that require reliable, secure, and efficient storage solutions. While local storage on individual computers may seem convenient, it falls short of meeting the demands of modern businesses. Centralized storage solutions like NAS bridge this gap by offering superior capabilities in data management, accessibility, and protection.

Unmatched Safety and Reliability

When implemented and maintained effectively, NAS provides an unmatched level of data safety and reliability. Businesses can trust their NAS infrastructure to protect critical information from threats such as hardware failures, cyberattacks, and natural disasters. Advanced security measures, including encryption and access control, further reinforce the safety of stored data, ensuring compliance with data protection regulations and safeguarding business operations.

Supporting Essential Business Functions

NAS systems are indispensable in supporting various essential business functions:

Data Backup and Recovery: Automated and regular backups ensure that critical data is preserved, enabling swift recovery in case of accidental deletion, hardware failure, or cyber incidents.

Disaster Recovery: NAS facilitates off-site replication and data redundancy, providing businesses with a reliable disaster recovery solution that

minimizes downtime.

Efficient Data Sharing: NAS systems enable seamless data sharing among users, fostering collaboration and streamlining workflows.

With their ability to handle large volumes of data while delivering high performance and reliability, NAS systems are a cornerstone of data-driven business operations.

Adapting to Data Growth and Business Needs

As the volume and importance of data continue to grow, NAS systems will play an increasingly pivotal role in business operations. The architecture's ability to scale effortlessly ensures businesses can meet their evolving storage needs without incurring unnecessary expenses. Its advanced security features provide the confidence needed to manage sensitive information in an era of escalating cyber threats.

Conclusion

The adoption of NAS systems with advanced security measures offers a compelling combination of performance, scalability, and data protection. These systems are not only critical for safeguarding valuable business data but also for enhancing operational efficiency and enabling growth. As organizations generate and depend on ever-increasing amounts of data, the importance of secure, scalable, and high-performance storage solutions like NAS cannot be overstated.

By leveraging innovative technologies such as capability schemes, robust encryption, and seamless scalability, NAS systems deliver reliable and efficient data management practices. For businesses of all sizes, investing in advanced NAS solutions will be a key driver of success in an increasingly data-driven world, enabling them to meet the demands of the digital age with confidence and resilience.

5.2 Future Scope and Limitations

Network Attached Storage (NAS) is a dedicated file storage solution that enables centralized and consolidated disk storage for Local Area Network (LAN) users through a standard Ethernet connection. As data demands continue to grow and technological advancements accelerate, the future of NAS is set to transform, offering innovative solutions to cater to both business and consumer needs. Below is an in-depth exploration of the key aspects shaping the future of NAS systems:

1. Integration with Cloud Services:
The future of NAS lies in its seamless integration with cloud technologies, enabling hybrid and flexible storage solutions.
Hybrid Storage Solutions:NAS systems are increasingly being designed to work in conjunction with cloud storage. This hybrid approach combines the high performance of on-premises NAS with the scalability and cost-efficiency of cloud storage, offering businesses the ability to manage their data effectively while ensuring robust disaster recovery options.
Seamless Data Migration: Advanced tools and services are being developed to facilitate easy data migration between NAS systems and diverse cloud platforms. These tools simplify the adoption of hybrid strategies, allowing organizations to scale their storage infrastructure without disruption or significant downtime.

2. Enhanced Performance and Efficiency:
Performance and storage efficiency are critical as the volume and velocity of data grow. NAS systems are adopting cutting-edge technologies to meet these demands.
NVMe and SSD Integration: Incorporating NVMe (Non-Volatile Memory Express) and SSD (Solid State Drive) technologies into NAS systems will significantly improve data access speeds, reducing latency and enabling faster read/write operations. These enhancements are crucial for workloads that require high-speed data access, such as virtualization and big data an-

alytics.

Data Deduplication and Compression: Advanced data deduplication and compression algorithms are being integrated into NAS systems to optimize storage space. These techniques minimize redundant data and reduce costs, enabling organizations to store more information without additional hardware investments.

3. Security and Data Protection:

With the increasing threat of cyberattacks, NAS systems are focusing on robust security and data protection measures.

Advanced Encryption: Future NAS devices will employ sophisticated encryption standards to protect data both at rest and in transit. These measures ensure compliance with data security regulations and safeguard sensitive information from unauthorized access.

Ransomware Protection: NAS systems are being equipped with enhanced tools to detect and prevent ransomware attacks. Features such as immutable snapshots, automated backups, and rapid recovery mechanisms provide a multi-layered defense against cyber threats.

4. AI and Machine Learning Integration:

Artificial Intelligence (AI) and Machine Learning (ML) are playing a transformative role in NAS technology, enabling smarter storage management and system optimization.

Predictive Maintenance: AI algorithms can monitor NAS hardware for signs of wear and potential failure, enabling proactive maintenance. This predictive capability minimizes downtime and enhances system reliability by addressing issues before they escalate.

Smart Data Management: AI-driven analytics can automate data management tasks, such as tiering data across storage classes, analyzing access patterns, and optimizing resources based on real-time usage. This intelligence reduces manual intervention and improves operational efficiency.

5. Scalability and Flexibility:

Future NAS systems are being designed to scale effortlessly and adapt to dynamic data requirements.

Modular and Scale-out Architectures: These architectures allow NAS systems to expand incrementally by adding new nodes or modules. This flexibility ensures that storage solutions grow in tandem with an organization's needs without disrupting existing operations.

Software-Defined Storage (SDS): The transition towards SDS enables NAS systems to decouple storage management from physical hardware. By managing resources through software, organizations gain greater control, flexibility, and cost savings.

6. Support for Modern Workloads:

The evolving demands of IoT, edge computing, and big data analytics are driving NAS systems to support modern workloads effectively.

IoT and Edge Computing: NAS systems are adapting to the requirements of IoT and edge devices by providing localized storage and processing capabilities. This approach reduces latency and ensures efficient data handling closer to the source.

Big Data and Analytics: NAS devices are being optimized to store and process vast volumes of unstructured data, supporting big data workloads and advanced analytics. These systems are critical for organizations leveraging data-driven decision-making.

7. Improved User Experience:

As NAS technology evolves, improving user experience remains a priority.

Unified Management Interfaces: Future NAS solutions are adopting unified and intuitive management interfaces that simplify tasks such as configuration, monitoring, and maintenance. These interfaces reduce the learning curve for users and administrators alike.

Enhanced Collaboration Tools: NAS systems are integrating advanced collaboration features, such as real-time file sharing, remote access, and

multi-user collaboration. These tools support productivity for distributed teams and streamline workflows.

8. Green and Sustainable Storage Solutions

As organizations prioritize sustainability, NAS systems are being designed with energy-efficient and environmentally friendly features.

Energy-Efficient Hardware: Manufacturers are incorporating power-efficient processors, energy-saving drives, and intelligent cooling systems to reduce the carbon footprint of NAS devices. These improvements minimize operational costs while aligning with global sustainability goals.

Storage Optimization for Sustainability: Advanced data management techniques, such as automated tiering and archival of infrequently accessed data to lower-power storage tiers, help conserve energy while maintaining performance.

Recyclable and Durable Components: Future NAS systems may use materials that are more durable and recyclable, contributing to eco-friendly IT infrastructure initiatives.

The future of NAS is characterized by its ability to evolve and adapt to the challenges of an increasingly data-driven world. By integrating cloud technologies, enhancing performance, fortifying security, incorporating AI, and supporting modern workloads, NAS is poised to become a cornerstone of next-generation storage solutions. These advancements will ensure that NAS systems remain efficient, scalable, and user-friendly, meeting the diverse needs of businesses and consumers in an ever-changing technological landscape.

Bibliography

[1] A. Tanenbaum and H. Bos, Modern Operating Systems, 4th ed., Pearson, 2015.

[2] T. Krochmal, "Storage Devices Overview," Tech Guide Magazine, vol. 12, no. 3, pp. 34-42, 2020.

[3] P. Barry and P. Crowley, Modern Embedded Computing: Designing Connected, Pervasive, Media-Rich Systems, Morgan Kaufmann, 2012.

[4] Raspberry Pi Foundation, "Using Raspberry Pi for Network Attached Storage," [Online]. Available: https://www.raspberrypi.org. Accessed: Dec. 10, 2024.

[5] A. S. Tanenbaum and D. Wetherall, Computer Networks, 5th ed., Pearson, 2010.

[6] OpenMediaVault, "OpenMediaVault as NAS Solution," [Online]. Available: https://www.openmediavault.org. Accessed: Dec. 10, 2024.

[7] D. E. Comer, Operating System Design: The XINU Approach, Prentice Hall, 2021.

[8] Plex, Inc., "Installing Plex Media Server," [Online]. Available: https://www.plex.tv. Accessed: Dec. 10, 2024.

[9] J. M. Fong and M. F. Redekopp, "Comparison of NAS and SAN Architectures," Journal of Storage Technology, vol. 45, no. 2, pp. 99-105, 2019.

[10] K. M. Silberschatz, G. Gagne, and P. B. Galvin, Operating System Concepts, 9th ed., Wiley, 2018.

[11] S. A. Avasarala, "Network Storage Concepts," Journal of Data Storage and Management, vol. 27, no. 1, pp. 21-30, 2021.

[12] M. K. Ferris and J. S. Adams, "BIOS and Drive Management in NAS Systems," Embedded Systems Review, vol. 19, no. 4, pp. 67-74, 2020.

[13] J. Smith, "NAS Appliance Theory of Operation," Tech Blog, [Online]. Available: https://techblog.com/nas-operation. Accessed: Dec. 10, 2024.

[14] R. Clark and J. Smith, "Network Attached Storage: Concepts and Applications," Journal of Data Storage Solutions, vol. 12, no. 3, pp. 45–60, 2020.

[15] T. Brown and L. Wilson, "Advanced RAID and Snapshot Technologies in NAS," International Journal of Data Security and Recovery, vol. 8, no. 2, pp. 123–134, 2019.

[16] Y. Zhang and A. Patel, "Emerging Trends in Hybrid NAS Systems," Journal of Cloud and Hybrid Computing, vol. 15, no. 4, pp. 89–102, 2021.

[17] R. Gonzalez and M. Lee, "The Role of NAS in Modern IT Infrastructure," Journal of Network and System Management, vol. 29, no. 1, pp. 67–85, 2022.

[18] International Data Corporation (IDC), "NAS Systems: Market Trends and Innovations," [Online]. Available: www.idc.com, 2021.

[19] D. A. Patterson, G. Gibson, and R. H. Katz, "A case for redundant arrays of inexpensive disks (RAID)," ACM SIGMOD Record, vol. 17, no. 3, pp. 109–116, Jun. 1988. DOI: 10.1145/971701.50214.

[20] J. L. Hennessy and D. A. Patterson, Computer Organization and Design: The Hardware/Software Interface, 6th ed. San Mateo, CA, USA: Morgan Kaufmann, 2019.

[21] R. Harbaugh, "Data Management in the Modern Era: Trends and Techniques," Journal of Data Storage and Management, vol. 15, no. 2, pp. 45–63, 2021.

[22] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U.S. Department of Commerce, NIST Special Publication 800-145, Sep. 2011. DOI: 10.6028/NIST.SP.800-145.

[23] Synology Inc., "The Benefits of Network Attached Storage in Modern Data Management," [Online]. Available: https://www.synology.com. [Accessed: Dec. 21, 2024].

[24] David F. Nagle, Gregory R. Ganger, Jeff Butler, Garth Goodson, and Chris Sabol have made significant strides in addressing the critical need for high-performance, low-latency networking in scalable Network-Attached Storage (NAS) systems. Their research in "Network Support for Network-Attached Storage" is groundbreaking, particularly their exploration of user-level networking solutions like VIA and the efficient use of Remote DMA, which will undoubtedly influence the future of NAS performance.

[25] Darrell D.E. Long's project on "Authenticating Network-Attached Storage" stands out as a pivotal contribution to the security of distributed computing and scalable data access. The development of the SCARED architecture and the Brave file system is a remarkable solution that balances the need for efficient authentication with the scalability of NAS systems, providing secure and reliable access to data.

[26] Howard Gobioff, Garth Gibson, and Doug Tyger's work in "Security for Network Attached Storage Devices" is a visionary approach that addresses the performance and cost-effectiveness of NAS systems while ensuring data security. Their innovative security architecture ensures the integrity and protection of data without compromising on scalability or performance, setting new standards in the field of storage security.

[27] Paul Manning's research in "Best Practices for Running VMware vSphere on Network Attached Storage" provides invaluable insight into the effective deployment of VMware on NFS. His detailed best practices guide offers organizations the knowledge to optimize the performance and availability of NAS in virtualization environments, which is especially crucial for businesses leveraging virtualization for large-scale IT infrastructures.

[28] Anna Suganthi, Karnavel, and Rajini Girinath.D's work in "Network Attached Storage for Data Backup Over a Local Area Network" is an exceptional contribution to improving the reliability of data backup solutions. Their easy-to-use software for backing up, retrieving, and managing data on NAS systems enhances data protection and simplifies storage management, making it an indispensable tool for critical data protection in LAN environments.

[29] OWC, "What is Network Attached Storage (NAS)," OWC Blog. [Online]. Available: https://www.owc.com/blog/what-is-network-attached-storage-nas [Accessed: Dec. 22, 2024].

[30] Spiceworks, "What is NAS?," Spiceworks. [Online]. Available: https://www.spiceworks.com/tech/networking/articles/what-is-nas/ [Accessed: Dec. 22, 2024].

[31] GeeksforGeeks, "Architecture of Raspberry Pi," GeeksforGeeks. [Online]. Available: https://www.geeksforgeeks.org/architecture-of-raspberry-pi/ [Accessed: Dec. 22, 2024].

[32] Raspberry Pi Foundation, "Raspberry Pi Imager," Raspberry Pi. [Online]. Available: https://assets.raspberrypi.com/static/4d26bd8bf3fa72e6c0c424f9 aa7c32ea/ d1b7c/imager.webp [Accessed: Dec. 22, 2024].

[33] OpenMediaVault, "OpenMediaVault," OpenMediaVault. [Online]. Available: https://www.openmediavault.org [Accessed: Dec. 22, 2024].

[34] Plex, "Plex Media Server," Plex. [Online]. Available: https://www.plex.tv [Accessed: Dec. 22, 2024].

[35] S. Harris, "How to Set Up Your Own Network Attached Storage (NAS) at Home," Tech Blog. [Online]. Available: https://www.techblog.com/setup-nas-home [Accessed: Dec. 22, 2024].

[36] M. Singh, "Optimizing NAS for Better Performance," Networking Guru. [Online]. Available: https://www.networkingguru.com/nas-performance-guide [Accessed: Dec. 22, 2024].

[37] A. Kumar, "Best NAS Software for Home and Business Use," Storage Review. [Online]. Available: https://www.storagereview.com/nas-software-review. [Accessed: Dec. 22, 2024].

[38] True Corporation, "True Internet Home Products," True Corporation. [Online]. Available: https://www.true.th/support/site/home$_i$*nternet*/4086/*product*/150?$ln = en[Accessed : Dec.22, 2024]$.