

Contents

[Task 1: Operating System Definitions and Services 2](#_Toc200726105)

[Arguments FOR including applications: 3](#_Toc200726106)

[Arguments AGAINST including applications: 3](#_Toc200726107)

[Process Management 4](#_Toc200726108)

[Memory Management 4](#_Toc200726109)

[File System Management 5](#_Toc200726110)

[Device Management 6](#_Toc200726111)

[Security and Access Control 6](#_Toc200726112)

[Task 2: Windows Operating System Evolution 7](#_Toc200726113)

[Touch & Hybrid Computing: Windows 8 Failure and Windows 10 Recovery 8](#_Toc200726114)

[Windows as a Service' Model 8](#_Toc200726115)

[Task 3: Linux System Administration (Smart City Project) 9](#_Toc200726116)

[Task 4: Windows/macOS System Administration 11](#_Toc200726117)

[Windows Implementation: 11](#_Toc200726118)

[Task 5: AI Integration in Modern Operating Systems 18](#_Toc200726119)

[Task 6: Virtualization and Containerization 19](#_Toc200726120)

[Question 1: Definition of Virtualization and Containerization 19](#_Toc200726121)

[Question 2: OS Support for Virtualization 20](#_Toc200726122)

[Question 3: Hybrid Approach Benefits 21](#_Toc200726123)

[Task 7: Memory Management and Paging Calculations 22](#_Toc200726124)

[Task 8: Cybersecurity and Data Privacy in Modern OS 23](#_Toc200726125)

[Question 1: Open-Source vs Proprietary OS in National Cybersecurity 23](#_Toc200726126)

[Question 2: AI-Driven Threat Detection in Modern OS 23](#_Toc200726127)

# Task 1: Operating System Definitions and Services

What is OS? Is a system software that manages and control all resources and operations (programs and applications and the other system software) in my computer as also it acts as a interface for the software and the diff parts of my computer, and the OS in my computer is Windows. There are other OS’s (Linux, macOS, Android, iOS).

**Question 1: Should operating systems include applications like web browsers and mail programs?**

## Arguments FOR including applications:

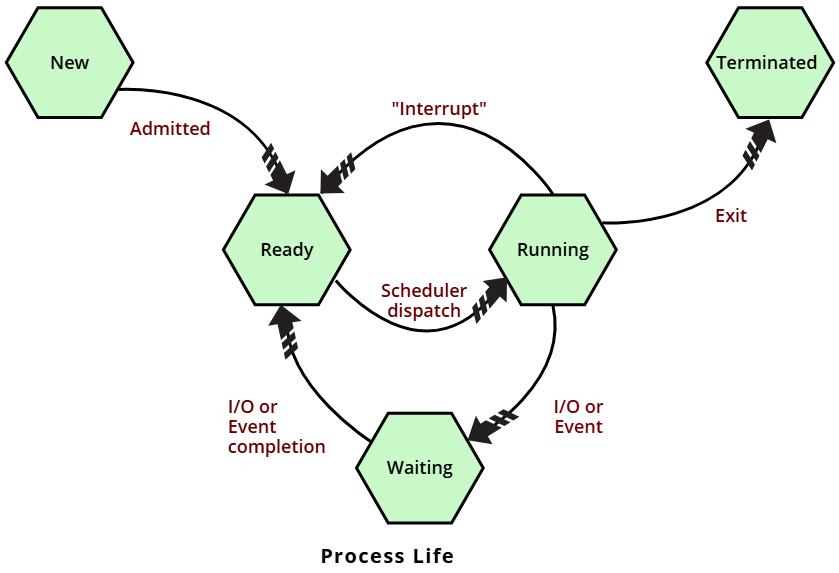
Actually it depends on, is the browser technicaly part of the OS? No actually it does runs at a layer above the OS, but what if OS does really include web browser as like Haiku, as they are now necessary component of contemporary computer infrastructure as well the web browsers are a basic rendering engine that allows users to interact with web-based content and services as much like OS systems package essential networking features and user interface elements and practically speaking the majority of users anticipate that their system will be operational right away after installation and web browser access to the internet is today as fundamental as text editing or file management. Linux distributions illustrate this idea by integrating browsers with mail apps and other networking tools, acknowledging that these programs are necessary for the system to function. A universal interface for accessing data, services, and applications is provided by the browser, making it a logical component of the complete system package that users purchase and install. User Convenience, by bundling essential applications provides users with a complete, ready-to-use system without requiring separate installations, System Integration: Builtin applications can be deeply integrated with OS services, providing better performance and security. Consistent User Experience, an applications designed as part of the OS maintain consistent UI/UX standards, Security Benefits: OS-integrated applications can leverage kernel-level security features more effectively

## Arguments AGAINST including applications:

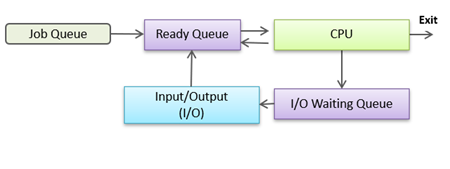
But in the other side operating systems have to come with web browsers since they are now a necessary component of contemporary computer infrastructure as well the web browsers are a basic rendering engine that allows users to interact with web-based content and services, much like OS systems package essential networking features and user interface elements. Practically speaking, the majority of users anticipate that their system will be operational right away after installation, and web browser access to the internet is today as fundamental as text editing or file management. Linux distributions illustrate this idea by integrating browsers with mail apps and other networking tools, acknowledging that these programs are necessary for the system to function. A universal interface for accessing data, services, and applications is provided by the browser, and here I did divide this to thse components effected, OS should focus on core system services; applications are separate concerns and as well the bundled applications increase the attack surface and complexity of the OS and as well the users should be free to choose their preferred applications without being forced to use bundled ones and for the maintenance including applications makes OS updates more complex and frequent and for the fairness bunding applications might create unfair competitive advantages and the minimal OS installations are more suitable for servers and embedded systems.

**Question 2: Five OS Services and Their Benefits**

## Process Management



What it does? Creating the process and also it does scheduling them and terminating processes as we know the users can run multiple programs simultaneously without manual resource allocation and as well user programs cannot directly access CPU scheduling mechanisms or kernel process tables



And for the job schedular, is a tool that helps automate IT tasks based on a set time and it is usually designed for specific systems or applications, allowing certain processes, like database management, to run automatically lets take this as an examples, include the Windows Task Scheduler and CRON for Linux and UNIX systems so these tools handle tasks during a designated time period and often outside of regular working hours. Automation administrators create job scheduling packages to manage how these tasks are carried out and reducing the need for manual involvement.

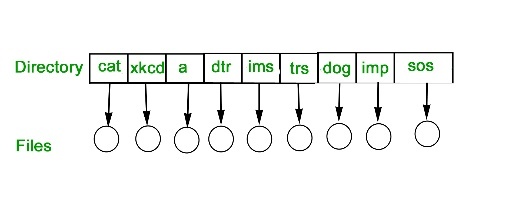
## Memory Management

Memory management is mainly about handling the main memory of a computer. In a system that runs multiple programs at the same time, the operating system sits in part of the main memory, while the rest is shared among various processes. The process of dividing memory among different programs is known as memory management. This function is crucial for efficiently managing the information that moves between the main memory and the disk while a process is running but what make it really important is that its able to reserve and free up memory before and after a program runs and to monitor which parts of memory are being used by which processes and to reduce issues related to memory fragmentation and to make the best use of the available main memory and to ensure data remains consistent and reliable while processes are running.

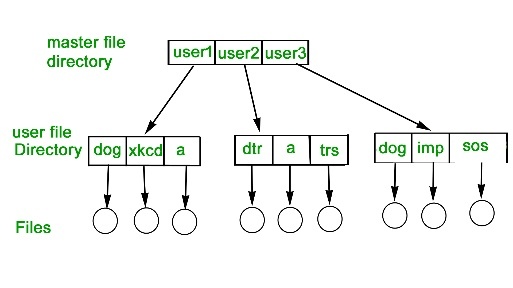
## File System Management

Its work is about file creation, deletion, reading, writing, and organization *and it p*rovides abstracted, hierarchical storage without requiring knowledge of disk hardware. Direct disk I/O and hardware controller access requires kernel privileges

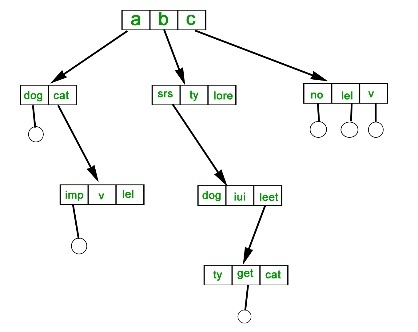
Where we have a single level directory is maintained for all the users



And also we have the 2-level one whetre each user is maintained



And as well the tree-structured directory it's an efficient search, and the ability to group is also available. We have an absolute or relative pathname for the file



As well we have three types of allocation, the indexed one and linked and continuous where it’s a set of blocks.

|  |  |  |
| --- | --- | --- |
|  |  |  |

## Device Management

*Service* is to Managing I/O devices through device drivers and *user convenience* where programs can use devices without knowing hardware-specific details *and the* Hardware device access requires privileged instructions and interrupt handling

## Security and Access Control

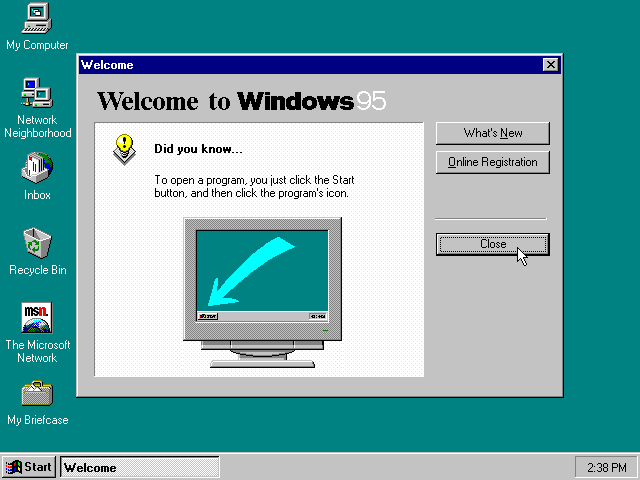
Its service is to user authentication, authorization, and resource protection and for the user convenience it does provides secure multi-user environment with automatic permission enforcement and as well for the security enforcement requires kernel-level privileges to prevent circumvention

Linux as they say Maximum Control is widely considered the most secure operating system, thanks to its multi-layered defense system. It uses three types of access control working together🡪 discretionary (DAC) and mandatory and RBAC. The famous file permission system operates at the kernel level, making it extremely difficult for malicious software to gain access and as well mooost Linux systems come hardened by default and are transparent by design - security flaws get spotted and fixed quickly by the open-source community so the catch? Linux is only as secure as you configure it to be.

Windows and as well they say the Enterprise Ready faces unique challenges as the most targeted operating system, but modern versions pack serious security features. NTFS permissions provide granular control, while User Account Control blocks dangerous actions before they happen. The real strength lies in enterprise integration with Active Directory and other business tools and as well windows relies heavily on real-time protection through Defender and automatic updates to stay ahead of threats. While this works well for most users, the platform's popularity makes it a constant target for cybercriminals.

macOS the Elegant Protection is built on Unix foundations, macOS combines robust security with Apple's signature simplicity. Features like sandboxing, Gatekeeper, and System Integrity Protection work quietly in the background to keep threats at bay and the user-friendly interface makes security accessible to everyone, though this simplicity can sometimes hide important configuration details. While less targeted than Windows, Mac users aren't immune to phishing attacks and social engineering.

# Task 2: Windows Operating System Evolution



**GUI Innovations: Windows 95 Start Menu Revolution**

Revolutionary Aspects: We can find that the Start Menu provided a single location for accessing all programs, settings, and documents and also the programs were organized in logical folders, making navigation intuitive for the search integration it was a really quick access to recently used items and documents and as well we had a combined with the taskbar to provide persistent access and program switching

Legacy in Modern Windows: As well as we know that the Windows 10/11 still use the Start Menu concept with tiles and traditional menu options and the search functionality has been enhanced with Cortana and cloud integration and the live tiles in Windows 10 expanded the original concept and also the paradigm of centralized system access remains fundamental

Internet & Cloud Integration Evolution

Internet Explorer Era: For this the IE integration in Windows 98 did have made web browsing a core OS function and as well we have the ActiveX which controls enabled rich web applications. Created security vulnerabilities due to deep system integration.

Microsoft Edge Development: the tools, resources, and processes used to create and improve websites and web applications for the Microsoft Edge browser as it replaced IE with modern web standards support and does have a better security through sandboxing and modern architecture and have a good integration with Microsoft services (OneDrive, Office 365)

Cloud Services Impact: For the cloud the OneDrive integration provides seamless file synchronization and the Microsoft Account integration enables cross-device continuity mean while the Azure integration for enterprise environments and the Windows as a Service relies on cloud-based update delivery

Security Enhancements

User Account Control (UAC) and For this the Impact of it shows the it Reduced privilege escalation attacks by requiring explicit permission for administrative actions and it have lot of Benefit such as how does it protects against malware that attempts to gain system-level access and its refined in later versions to reduce false positives while maintaining security

Windows Defender where it does have an amazing evolution from basic antispyware to comprehensive endpoint protection and it does built-in real-time protection with cloud-based threat intelligence its impact is that its eliminated need for third-party antivirus for many users

Trusted Platform Module (TPM) as it is a specialized security chip built into modern computers and devices that provides hardware-based protection for sensitive data and cryptographic operations so for the security enhans the hardware-based cryptographic security and its application for example BitLocker encryption and secure boot and credential protection and in the future the Windows 11 requires TPM 2.0 that making hardware security standard.

## Touch & Hybrid Computing: Windows 8 Failure and Windows 10 Recovery

### Windows 8 Failures:

We start with the flaws in Windows 8, the first of which was a radical change in the user interface, which removed the Start menu and imposed a touch interface on desktop users. The desktop experience was also poor, as the traditional desktop became a secondary interface, containing confusing dual interfaces. Metro apps and desktop programs created an inconsistent experience. There was also a lack of user training due to the lack of a gradual transition from the familiar Windows 7 interface.

### Windows 10 Corrections:

Moving on to Windows 10 improvements, such as the return of the Start menu, combining the traditional menu with live tiles, and the Continuity feature, such as automatic switching between tablet and desktop modes. It also includes universal apps, such as individual apps that adapt to different form factors. Touch features are available but not mandatory for desktop users.

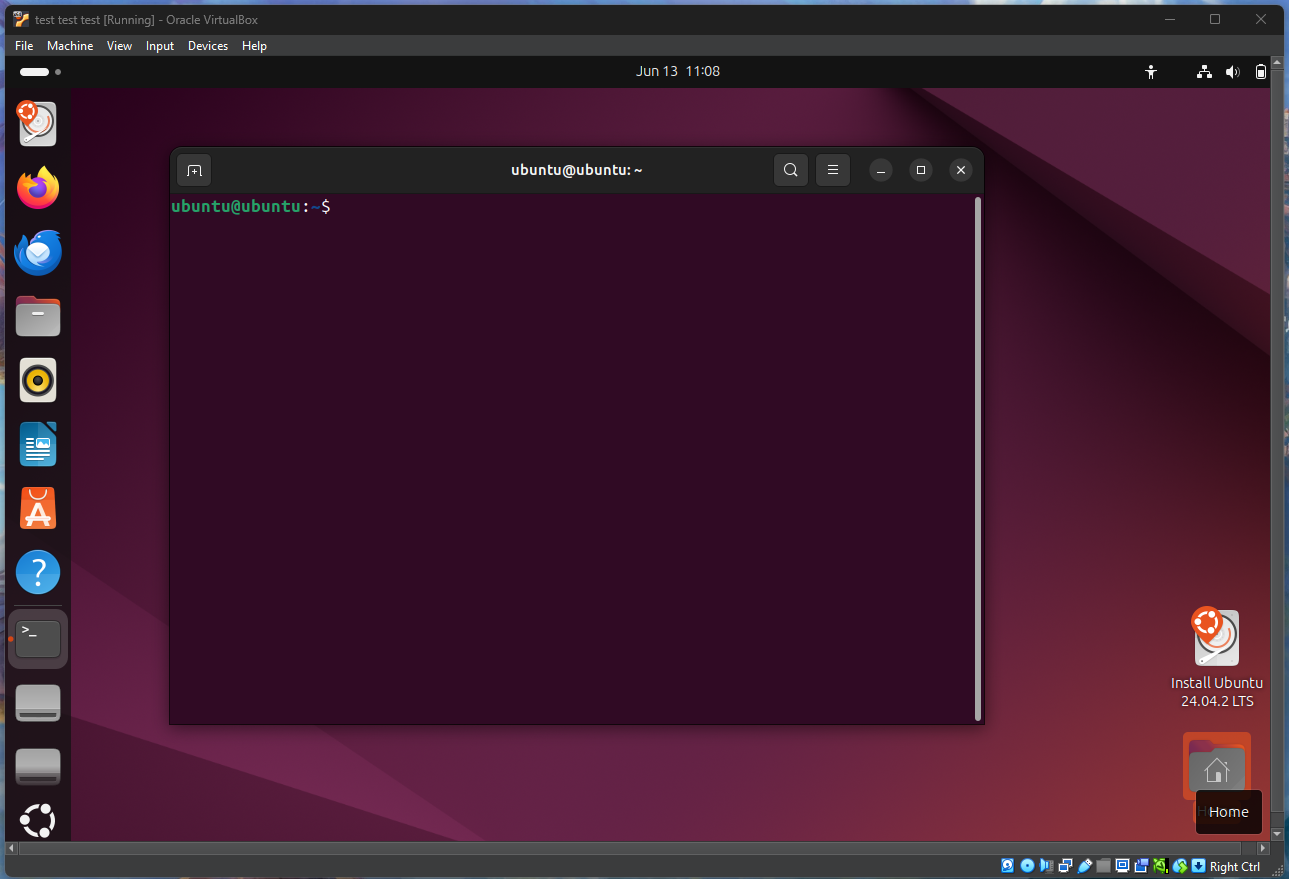
## Windows as a Service' Model

**Advantages and Disadvantages**

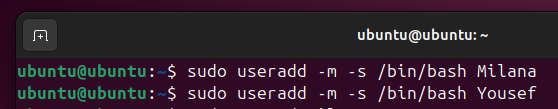
It has many distinct advantages, including continuous security updates and regular patches that reduce Windows vulnerabilities. It also includes feature updates, providing new capabilities without waiting for major releases. It also reduces support complexity, such as fewer operating system versions to maintain. It also offers cloud integration, which provides better integration with Microsoft's cloud services. Costs are also predictable, as the subscription model provides predictable revenue. However, it also has drawbacks, such as forced updates, as users lose control over the timing of updates. It also has compatibility issues, as frequent updates can break existing software. Furthermore, it raises privacy concerns, such as the constant collection of data to improve the service. Worse still, it relies on the internet for updates, and finally, it is a testing burden, as organizations must constantly test compatibility.

# Task 3: Linux System Administration (Smart City Project)

**Step-by-Step Implementation Commands:**



**Now lets start the implementation**

****

**A screenshot of a computer program

AI-generated content may be incorrect.**

**A black background with white text

AI-generated content may be incorrect.**

**A screenshot of a computer

AI-generated content may be incorrect.**

**A computer screen shot of white text

AI-generated content may be incorrect.**

**A screenshot of a computer screen

AI-generated content may be incorrect.**

**A screen shot of a computer

AI-generated content may be incorrect.**

**A computer screen shot of a program

AI-generated content may be incorrect.**

**A computer screen with white text

AI-generated content may be incorrect.**

**A screen shot of a computer program

AI-generated content may be incorrect.**

**A computer screen shot of a computer code

AI-generated content may be incorrect.**

**A computer screen shot of a program

AI-generated content may be incorrect.**

**A computer screen shot of a program

AI-generated content may be incorrect.**

# Task 4: Windows/macOS System Administration

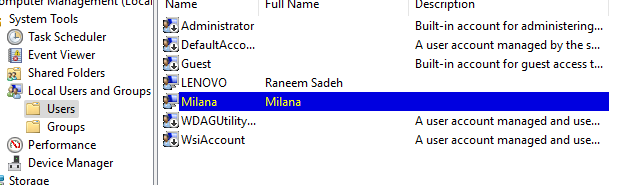
## Windows Implementation:

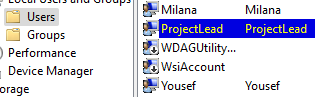
Use Computer Management → Local Users and Groups

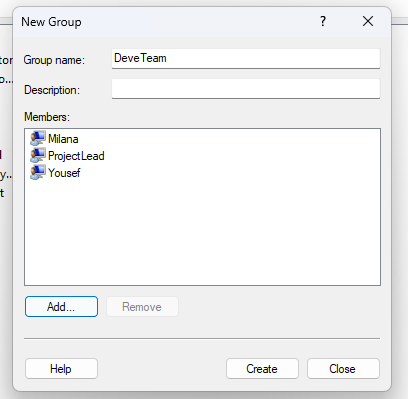
A screenshot of a computer

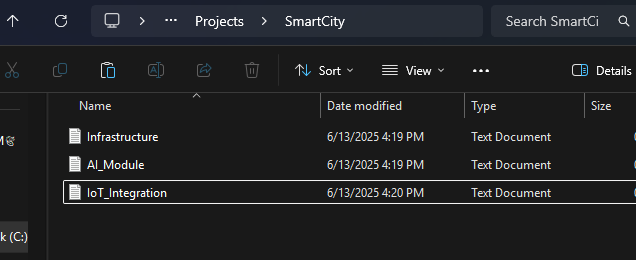
AI-generated content may be incorrect.

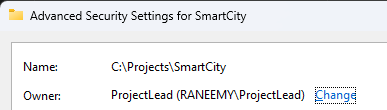
Create users through User Accounts control panel

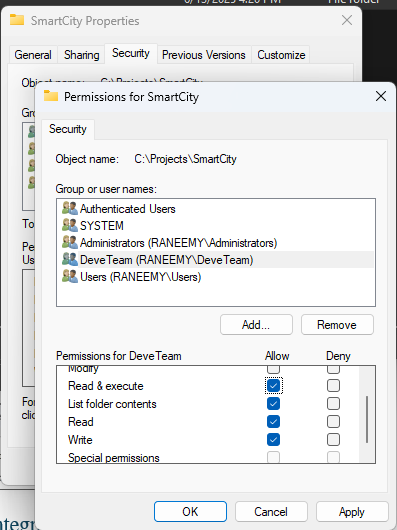




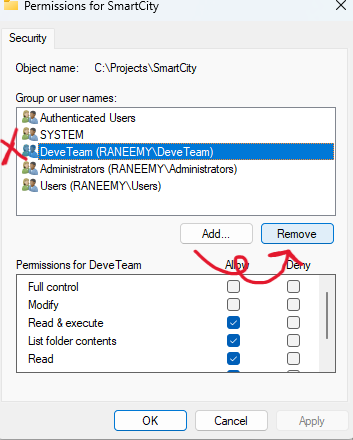




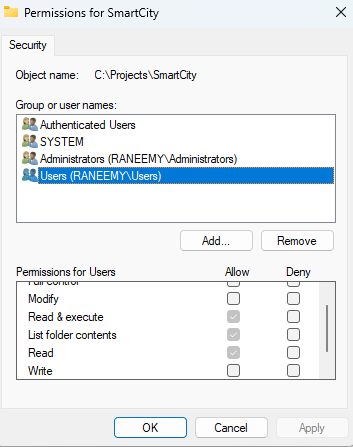


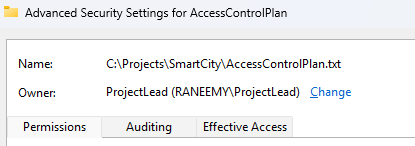


Deleting

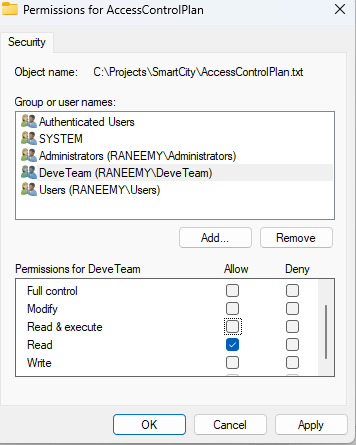


Users can only read and excute











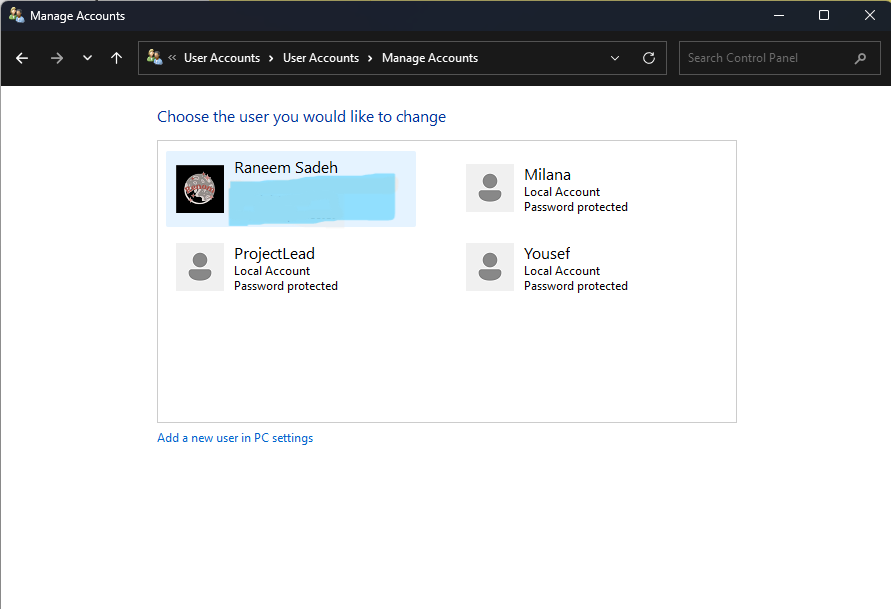
Full control for the ProjectLead

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



Deleting all the accounts

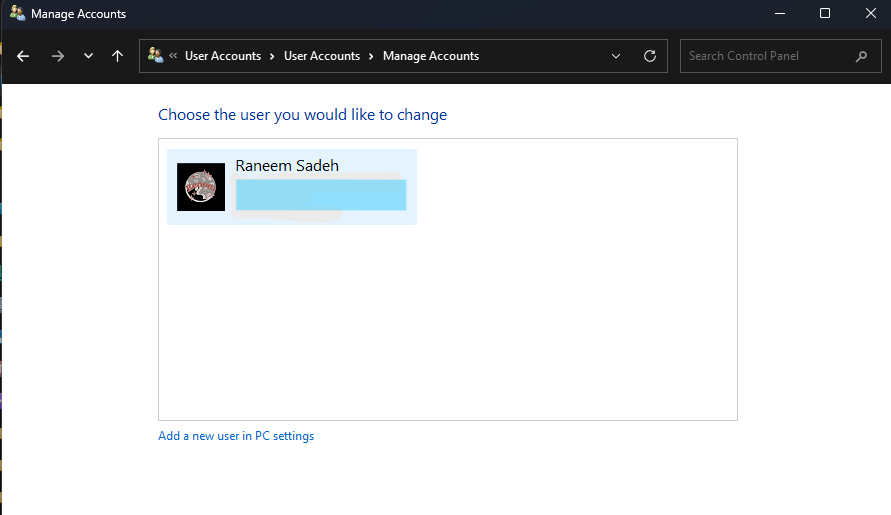
A screenshot of a computer error

AI-generated content may be incorrect.

A screenshot of a computer error

AI-generated content may be incorrect.

Now there is no accounts



And as we know there are more than one type of OS, so let me show the diff of windows and macOS and Linux

For the user creation

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Linux Command-Line | Windows GUI | macOS GUI |
| Add user | sudo adduser username | Control Panel → User Accounts | System Settings → Users & Groups |
| Set password | Prompted during adduser, or use passwd | Done during user creation | Done during user creation |
| View users | cat /etc/passwd | net user (CMD) or view in GUI | dscl . list /Users or view in GUI |

**For the creating the groups and adding the user to it**

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Linux Command-Line | Windows GUI | macOS GUI |
| Create group | sudo groupadd DevelopersTeam | Computer Management → Local Users & Groups | Users & Groups → Create Group |
| Add user to group | sudo usermod -aG DevelopersTeam username | User Properties → Member Of tab | Drag user to group in GUI |
| View group memberships | groups username | net localgroup groupname | id username or check group panel |

**For creating the dir and files**

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Linux Command-Line | Windows GUI | macOS GUI |
| Create directory | mkdir SmartCity | Right-click → New → Folder | Finder → File → New Folder |
| Create file | touch Infrastructure etc. | Right-click → New → Text Document | Finder → File → New Document (TextEdit) |

**For setting file per**

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Linux Command-Line | Windows GUI | macOS GUI |
| Set read/write/execute | chmod 770 filename | Right-click → Properties → Security tab | Right-click → Get Info → Sharing & Permissions |
| Change ownership | sudo chown user:group filename | Advanced Security Settings | Use GUI or chown in Terminal |
| View permissions | ls -l | Properties → Security → Advanced | Get Info → View under Sharing & Permissions |

**For deleting**

|  |  |  |  |
| --- | --- | --- | --- |
| Task | Linux Command-Line | Windows GUI | macOS GUI |
| Delete user | **sudo userdel -r username** | **Computer Management → Delete User** | **Users & Groups → Select user → Remove** |
| Remove group | **sudo groupdel groupname** | **Computer Management → Local Groups** | **Use GUI or Terminal** |

# Task 5: AI Integration in Modern Operating Systems

**Question 1: AI Transformation in OS Development**

Artificial intelligence has transformed operating systems development, as one of its fundamental transformations is that AI algorithms predict resource needs and improve system performance. They also include self-healing systems that automatically detect and fix problems, perform dynamic customization based on usage patterns and predictions, and AI-powered threat detection and response systems, as well as adaptive interfaces that learn user preferences and behaviors.

**Question 2: Key AI Technologies in Modern OS**

It integrates dramatically with modern operating systems, using machine learning algorithms to recognize patterns in system behavior and security threats. It can process natural language by integrating voice assistants (Cortana, Siri) into the operating system. With CV, it can perform facial recognition for authentication (Windows Hello, Face ID). With predictive analytics, it can anticipate system maintenance needs and improve performance. We also have deep learning neural networks for malware detection and behavior analysis.

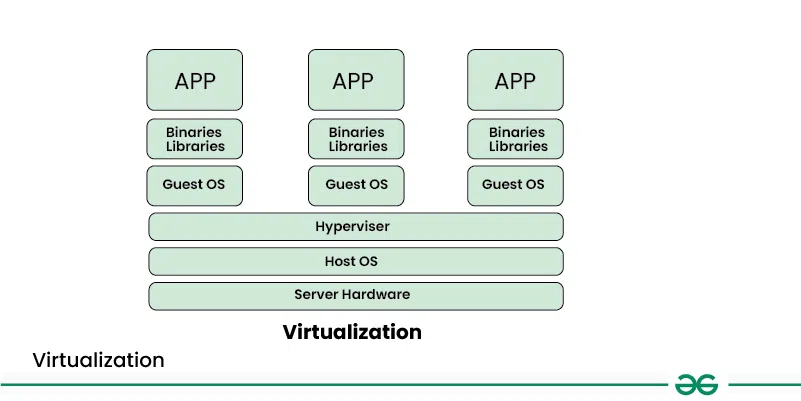
**Question 3: AI-Powered Voice and Natural Language Interfaces**

It has been able to replace traditional interaction with AI-powered voice and natural language interfaces that work efficiently, so that natural language commands can be faster than navigating through menus. Voice control enables hands-free operation while performing other tasks. AI also understands intent and context, reducing the need for precise commands and privacy concerns. Constantly listening devices raise privacy issues, but it faces challenges with accuracy. Speech recognition still struggles to handle accents and background noise. Graphical user interfaces (GUIs) are still superior for detailed visual work, and users need to learn optimal voice command patterns.

# Task 6: Virtualization and Containerization

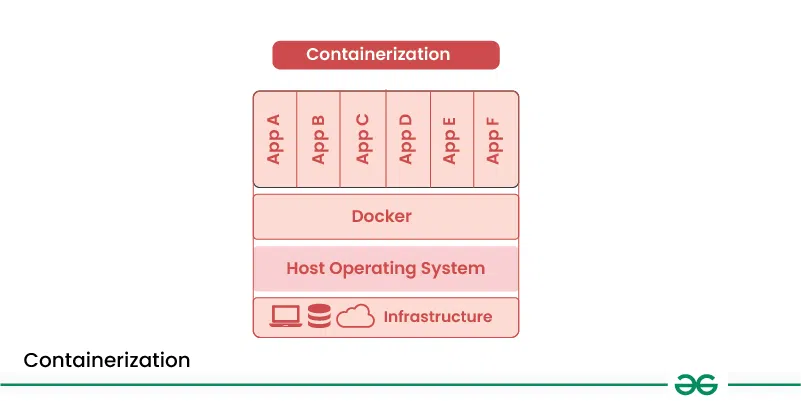
## Question 1: Definition of Virtualization and Containerization

**Virtualization:**

****

This technology creates virtual copies of computer resources, such as operating systems, storage devices, hardware platforms, and network resources. It's like creating a software copy of a physical machine, but it allows multiple isolated environments to run on the same machine or across a distributed system. Let me simplify this for you: Imagine you have a powerful computer, but you only use a small portion of its resources. Virtualization allows you to divide this machine into multiple virtual machines, each operating as a separate machine with its own operating system and applications. Each virtual machine will also be isolated from the others, meaning that problems with one virtual machine won't affect the others. It also improves resource utilization, allows you to run multiple applications on a single machine, and improves scalability by easily adding or removing virtual machines as needed.

**Containerization:**



It is a lightweight form of virtualization that allows you to run applications and their dependencies in isolated containers. Each container shares the same operating system kernel but is isolated from other containers, providing a portable and consistent running environment for applications. Containers provide process isolation, ensuring that applications running in one container do not affect those running in other containers. Containers encapsulate all the dependencies and configurations necessary to run an application, making them portable across different environments. Of course, compared to traditional virtual machines (VMs), these containers are much lighter because VMs share the host operating system kernel. They are designed to be scalable, allowing you to quickly expand or shrink them on demand. Containers enable developers to build, test, and deploy applications more efficiently, leading to faster release cycles and improved collaboration between development and operations teams.

|  |  |  |
| --- | --- | --- |
|  | Containerization | Virtualization |
| Running legacy applications | No | Yes |
| Building microservices architecture | Yes | No |
| Lifting and shifting existing applications to the cloud | No | Yes |
| Maximizing resource utilization | Yes | No |
| Rapid development and deployment (CI/CD) | Yes | No |
| Isolating applications from one another | No | Yes |

## Question 2: OS Support for Virtualization

**Hardware Virtualization Support:**

Modern processors now include specialized features that improve virtualization performance and security through hardware-assisted virtualization, such as Intel VT-x and AMD-V. These CPU extensions enable near-native performance for guest operating systems while maintaining strict isolation between virtual machines. Hardware manages critical operations, such as privilege level transitions and interrupt handling, significantly reducing overhead and improving security.

Technologies such as Extended Page Tables (EPT) in Intel processors and Rapid Virtualization Indexing (RVI) in AMD systems address memory management challenges in virtualized environments. These technologies implement nested page tables, allowing the virtualization driver to control physical memory allocation while guest operating systems seamlessly manage their memory mappings.

Input/Output virtualization has also seen significant improvements with technologies such as Single-Root I/O Virtualization (SR-IOV). This allows a single physical device to directly provide multiple virtual functions to guest operating systems, reducing virtualization driver intervention and thus improving performance and resource utilization.

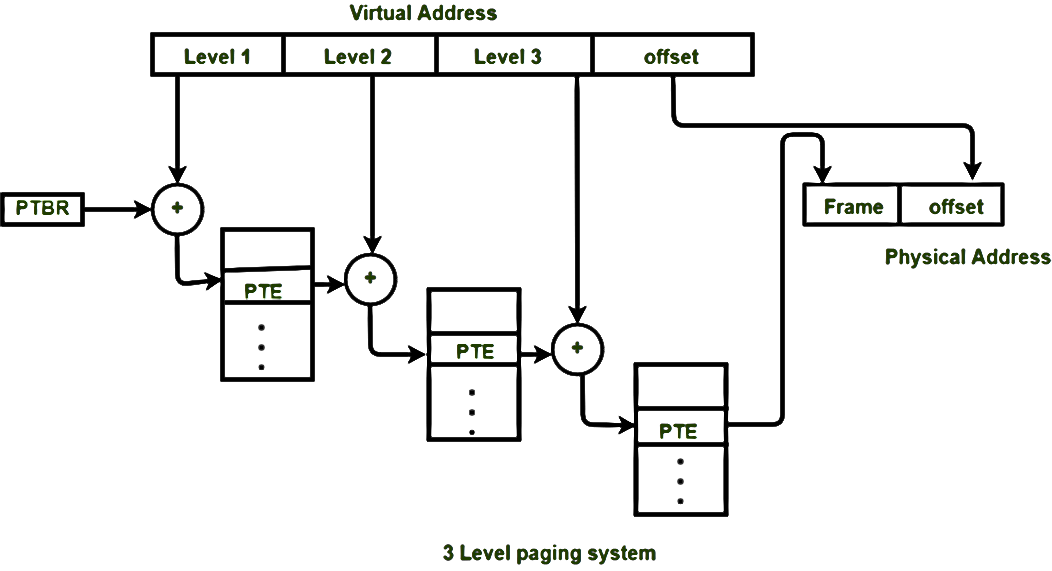
**OS-Level Support:**

Operating system support for virtualization goes beyond running on virtual machines. It is deeply integrated with virtualization drivers and resource management. First-generation virtualization drivers, such as VMware ESXi and Microsoft Hyper-V, replace traditional operating systems, enabling maximum performance and efficiency. These drivers also enhance features such as live migration and dynamic resource allocation through specialized drivers and interfaces. Over time, modern operating systems, particularly Linux, have evolved to better support containerized environments such as Docker and Containerd, which use kernel namespaces and control groups for simple isolation without the cost of running full OS instances. This integration allows for features such as process isolation, network virtualization, and efficient resource management. Resource management in virtual environments involves complex coordination to ensure optimal performance across virtual machines and containers. The host operating system manages CPU scheduling, memory allocation, and I/O resource prioritization, often using Quality of Service (QoS) mechanisms. Security measures operate on multiple layers, with the host operating system providing isolation and access controls to prevent interference between virtual workloads. Advanced features include secure boot, encrypted virtual disks, and audit logging for security analysis and compliance.

## Question 3: Hybrid Approach Benefits

Why choose hybrid virtualization plus containers? Because they are simply amazing. They offer flexibility in virtual machines for different operating system requirements, containers for application deployment, and containers provide efficiency. Virtual machines provide isolation, security layers, and multiple isolation levels for different security requirements. They are easy to move and load between environments. Not to mention their enhanced scalability and security. Due to the microservices architecture, containers enable precise scaling of application components. Furthermore, a virtual machine failure does not affect other virtual machines; a container failure does not affect the host machine. Due to cloud integration, this enables seamless scaling across on-premises and cloud environments.

# Task 7: Memory Management and Paging Calculations



|  |  |
| --- | --- |
|  |  |
|  | |

# Task 8: Cybersecurity and Data Privacy in Modern OS

## Question 1: Open-Source vs Proprietary OS in National Cybersecurity

**Open-Source Advantages & Disadvantages**

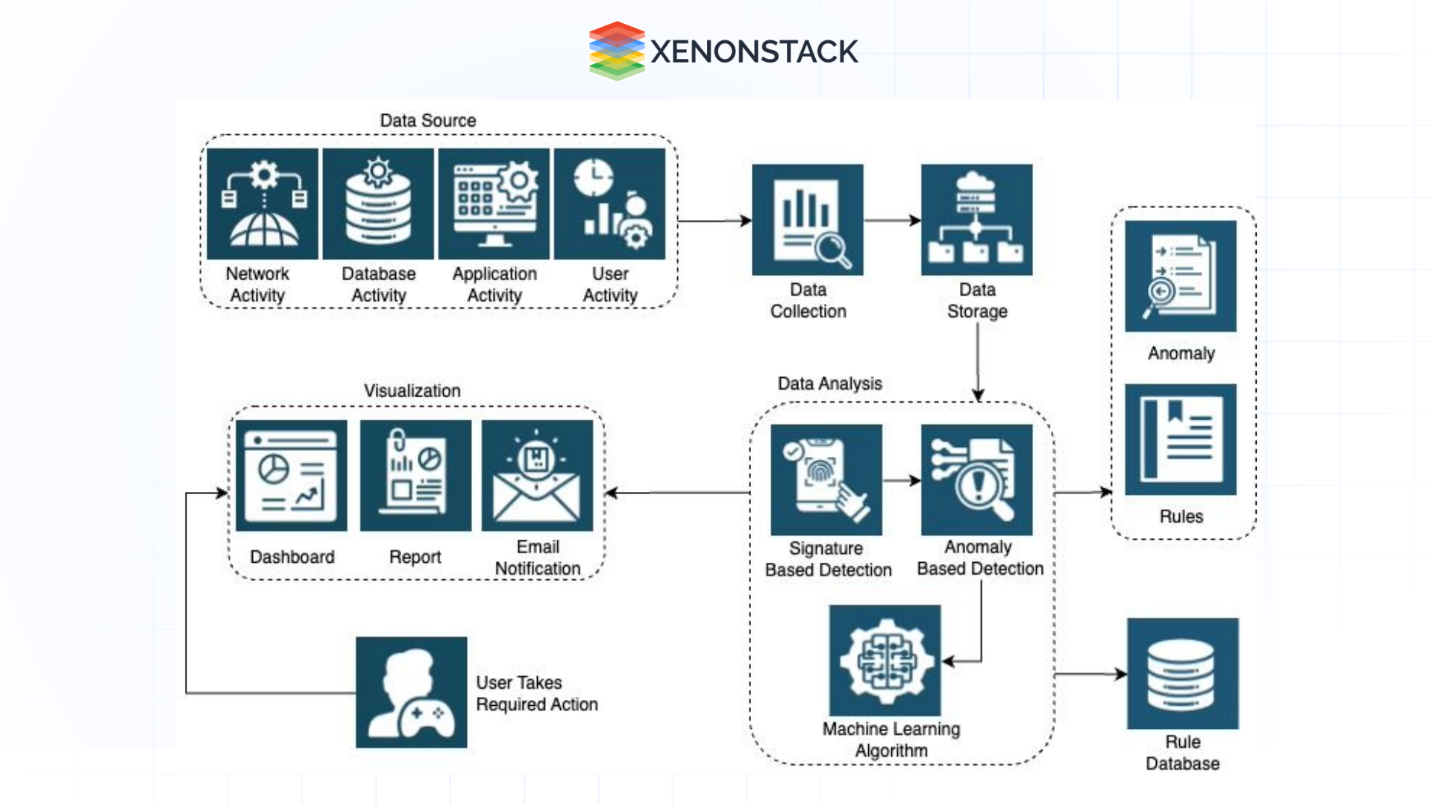
One of the most important advantages of open source systems is their transparency, as the source code can be audited for security vulnerabilities. Also, because of the large developer community, they quickly identify and fix security issues. The absence of backdoors reduces the risk of surreptitious surveillance. They are designed to be modifiable to meet specific national security requirements. Their independence reduces dependence on foreign technology suppliers. However, alongside these advantages, there are also disadvantages, including vulnerability to security vulnerabilities, as vulnerabilities are visible to both defenders and attackers. Unfortunately, they may lack comprehensive support from vendors for critical systems, as well as for maintenance and security, which requires significant expertise. Furthermore, because of the multiple distributions, this leads to consistency and compatibility issues.

**Proprietary Advantages & Disadvantages**

As for proprietary systems, they have professional support, as this support is allocated by the suppliers, and regular and consistent security updates are provided. They contain unified applications across deployments, and the suppliers are held responsible for security issues and patches. They also offer better integration with existing enterprise systems. Despite all these advantages, they also have drawbacks, as they are a black box, as they cannot be verified for backdoors or security vulnerabilities. Unfortunately, they must rely on foreign companies (suppliers) for critical infrastructure, and unfortunately, there is the potential for the supply chain, its components, and even its updates to be compromised.

Given all this, we find that the best approach to national cybersecurity is a hybrid approach. This is because open source solutions can be used with national-level code reviews, enhanced customization, and proprietary solutions evaluated with strict supplier oversight. These solutions also have custom-designed solutions built on solid open source foundations, ensuring transparency and public trust.

## Question 2: AI-Driven Threat Detection in Modern OS



In fact, this can be solved through behavior analysis, where AI learns natural user patterns and detects any anomalies. By monitoring process behavior, it can identify suspicious process activity and system calls. By analyzing network traffic, it can detect unusual network connections and data leaks. Through machine learning security, it can detect malware using AI models trained on malware signatures and behaviors. Its intelligence allows it to identify previously unknown threats before they occur, and without sending anything, it can respond on its own. For example, AI can automatically isolate threats and take countermeasures. As for predictive security, AI can predict potential security vulnerabilities before they are exploited, and by integrating with global threat databases for proactive protection (it's as if it's studying whether this can also be done in the same way). It can also dynamically and effectively assess these risks. Let's look at examples of this. Windows Defender ATP already exists, as it uses machine learning for advanced threat detection. We also have macOS XProtect, which detects and blocks malware using AI. Linux security modules are capable of AI-enhanced access control and intrusion detection. We can imagine future developments, such as quantum-resistant security, where AI will help develop post-quantum encryption solutions. What about autonomous security (self-protecting systems that automatically adapt to new threats? Federated learning can be described as collaborative AI security without sharing sensitive data.

References

Digital Citizen, 2023. *The geek’s way of managing user accounts and groups in Windows*. <https://www.digitalcitizen.life/geeks-way-managing-user-accounts-and-groups>

Microsoft Learn, 2023. *How do I set up user accounts and manage permissions?* <https://learn.microsoft.com/en-us/answers/questions/1389054/how-do-i-set-up-user-accounts-and-manage-permissio>

YouTube, 2023. *Linux Commands for Beginners | Introduction to Linux Command Line Interface*. <https://www.youtube.com/watch?v=xzEjychfD1Y>

GeeksforGeeks, 2024. *File Systems in Operating System*. <https://www.geeksforgeeks.org/operating-systems/file-systems-in-operating-system/>

HAT University, 2025. *Security Commands Lecture Recording (Meeting Recording - 2025/06/06)*. <https://hatuniversity.sharepoint.com/sites/operatingsystems40spring25/_layouts/15/stream.aspx?id=%2Fsites%2Foperatingsystems40spring25%2FShared%20Documents%2FGeneral%2FSecurity%20Commands%2D20250606%5F032852%2DMeeting%20Recording%2Emp4>

Ubuntu, 2025. *Ubuntu Server Download*. <https://ubuntu.com/download/server>

TechTarget, 2024. *Operating system (OS)*. <https://www.techtarget.com/whatis/definition/operating-system-OS>

VirtualBox, 2025. *Downloads*. <https://www.virtualbox.org/wiki/Downloads>

IBM, 2023. *What is an Operating System?* <https://www.ibm.com/think/topics/operating-systems>

Quora, 2024. *Should operating systems include applications such as web browsers and mail programs?* <https://www.quora.com/Keeping-in-mind-the-various-definitions-of-operating-system-consider-whether-the-operating-system-should-include-applications-such-as-web-browsers-and-mail-programs-Argue-both-that-it-should-and-that-it-should-not>

GeeksforGeeks, 2023. *Virtualization vs Containerization*. <https://www.geeksforgeeks.org/system-design/virtualization-vs-containerization/>

MrPCSS, 2023. *Windows 95 – A Revolution in Personal Computing*. <https://mrpcss.com/windows-95-a-revolution-in-personal-computing/>

GeeksforGeeks, 2023. *Operating Systems Overview*. <https://www.geeksforgeeks.org/operating-systems/operating-systems/>

GeeksforGeeks, 2023. *Process Schedulers in Operating Systems*. <https://www.geeksforgeeks.org/operating-systems/process-schedulers-in-operating-system/>