Experiment No.8

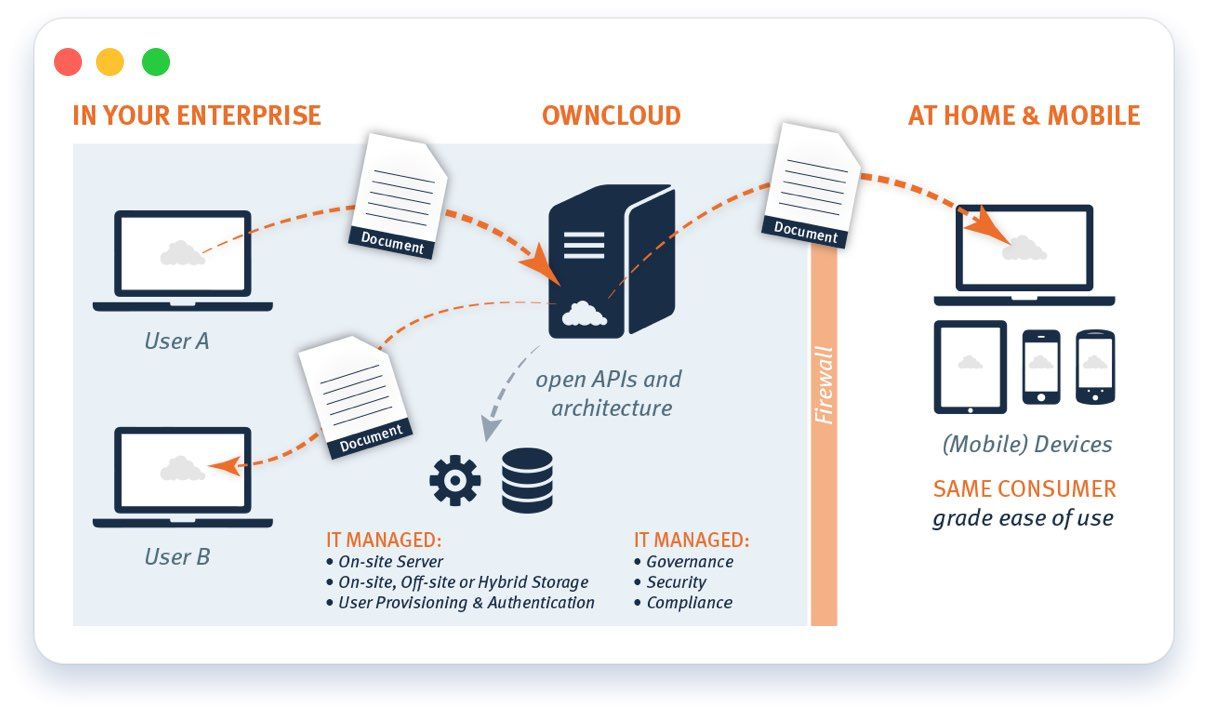
**AIM:** To study securing servers feature in cloud using ownCloud.

**Theory:**

**1] Fileshare**

As a busy knowledge worker, you may be in the airport when you have an urgent request from one of your executives to send a critical file ASAP. Your flight is about to board and you don’t have time to fire up your laptop, access the internet, access the VPN, start email, attach the file, sync the client all just to send the file. But, your mobile phone with the ownCloud app lets you go to the file and share it. Done.

Whether in SharePoint, on a Windows network drive or in cloud storage, users have a single interface from which they can access, sync and share files on any device, anytime, from anywhere. Users can quickly find and share the files they need whether shared by others or created themselves. With features like password protection, link expiration, anonymous and full access sharing, files are managed accordingly. And, administrators can easily track and audit file sharing activities.



**2] Syncing**

You are working on the final presentation for your big product launch. You save the last version on your desktop, grab your iPad and run for the airport. As you taxi for takeoff you open the ownCloud app, the latest file, which has conveniently synced from your PC to the laptop, is there waiting for your final touches. With a sync client that keeps the web, desktop and mobile device on the same page, users don’t have to question if they have the latest file version. Running seamlessly in the background, ownCloud actively monitors any file changes and pushes the latest version to all devices and all relevant users wherever they are.

**3] External Storage**

Your IT project doesn’t start with a blank slate. There are storage systems, servers, private cloud management tools, log managers, backup tools, and more already deployed in the enterprise. ownCloud delivers choice. If storage can be mounted on Linux, ownCloud can use it SAN, NAS, direct attached, virtual, software defined – whatever is needed. Further, with the ownCloud file system abstraction layer, API based storage, such as S3 or Swift compliant gateways are simple to integrate. And on the off chance a different object store interface is required, it can easily be added.

With ownCloud, you can also leverage storage that already exists; FTP, Swift, S3, Dropbox and more. Administrators can decide to store the most sensitive data on-premises and less sensitive data in the cloud while making all of your files available through a single interface and enabling compliance with your chosen security and governance policies.

**4] Encryption & Security**

OwnCloud is software provided to you, to install in your data center; managed by you, to your policies, following your procedures. Encryption at rest secures your files on the server and still allows sharing among users. The File Firewall ensures all access requests meet rules set by the administrator, and existing infrastructure – such as intrusion detection and log management can provide added layers of security. With WebDAV, mobile libraries and the ownCloud API as well as several enterprise-only apps, secure file sharing is in your control.

**5] Storage API**

The new storage API not only offers better scalability, but it also enables ownCloud to leverage storage that has, until now, been unheard of in file access solutions – such as tape. In this manner, ownCloud can leverage the most cost effective storage possible, while still providing employees, partners and suppliers the frictionless experience they seek in accessing their files.

**6] Data Infrastructure Modernization**

You work in IT at an organization that has unstructured data spread across multiple data silos such as Windows networks drives, Microsoft SharePoint, FTP servers, object storage (e.g. S3) or public cloud services (e.g. Google Drive, Dropbox or other WebDAV-enabled services). Having previously created policies and set permissions at the user, file, application, storage or cloud level, you want the ability to preserve and reuse those same policies and permission. With ownCloud, you can provide users with a single point of access to all of their unstructured data where permissions, ACLs and compliance requirements are respected and can be met and/or configured at a file, object store or user level. Files stored in data silos are made available within ownCloud securely and benefit from ownCloud feature portfolio. Data Infrastructure Modernization is realized by a common file access layer to bundle information, regardless of where the data lives – in applications, object stores, on-premises storage or in the cloud. Users can access company files on any device, anytime, from anywhere completely managed, secured and controlled by IT. Data is kept where it is, while IT is able to manage sensitive information and business risk, leveraging existing data management, security, governance tools and processes.

**7] Flexible API**

ownCloud open architecture, mobile libraries and APIs allow IT to rapidly extend core functionality and enhance the solution to meet user needs. Extend ownCloud with custom functionality through REST APIs that expose ownCloud user management, file management, file sharing and activity events, allowing you to customize ownCloud as needed. ownCloud sharing API enables third-party apps to set and query files shared within ownCloud. ownCloud also leverages the WebDAV standard for file access, enabling other software to interact with ownCloud and manage files. ownCloud is highly extensible, enabling the addition of new APIs quickly via plug-in applications. ownCloud gives you to the power to integrate apps that customize your deployment.

**8] Federated Cloud Sharing**

You are collaborating with another research center on sensitive data but they are on the other side of the world. Your organization has very strict usage guidelines around data sharing...and so does your collaborator. With Federated Cloud Sharing from ownCloud, both organization can maintain their individual control while sharing designated files and folders across time zones and geographies all while maintaining the access at any time, from any device. With Federated Cloud Sharing, users on one ownCloud installation can collaborate with users on other ownCloud installations while each server maintains its respective security and governance protocols. Files shared between users are no longer confined to a single shared folder or ownCloud instance; users can access the latest file versions and selectively sync the most critical shared files. And, when sharing with users on other ownCloud instances, their names will appear as an option for sharing if they have been configured as a trusted server. To the end user, it appears as if they are using a single ownCloud instance, even though the users are distributed across multiple ownCloud instances. This also means that mobile and desktop users can take advantage of these sharing capabilities, providing a seamless, frictionless way to collaborate with their files inside and outside the organization.

**9] Ransomware Protection new**

Ransomware attacks are an ever-present malware risk, both for large enterprises as well as for private users. Once affected, whole hard drives or parts of it can become encrypted leading to unrecoverable data loss that directly translates to significant effort and cost. For this exact purpose the ownCloud Ransomware Protection App protects companies by blocking uploaded files known to originate from ransomware to preserve original, unaffected files in ownCloud. Additionally it can lock user accounts when ransomware has been detected in order to prevent further damage. As not all ransomware attacks can be detected nor prevented, smart mechanisms for the restoration of original files are also included in the application.

**10] Guests new**

File Sharing with external parties can be quite a challenge. While a public link might be enough to share a single file, this becomes rather complicated for use cases with various files, folders and documents, for example working together on a project over the course of some time. The ownCloud Guests feature solves this by allowing to create ownCloud Guest accounts with very limited access rights. Simply share with external users just by entering an email address in the sharing dialog.

Recipients receive an email containing an activation link. They can log in using their email address as username and the password they chose during activation. Guests may even use the ownCloud desktop clients and mobile apps to connect to ownCloud and work on shared contents. Guest users do not have storage space and can only work in contents that are shared with them. To make this experience fully transparent, Guests are of course fully logged and auditable with the ownCloud Logging and Auditing functionality.

**Conclusion:**

Thus the securing servers features in cloud using ownCloud.