

# Utilizing Machine Learning

while protecting digital sovereignty for Universities

## CS32024



Micke Nordin

kano@sUNET.se

Richard Freitag

freitag@sUNET.se

Magnus Andersson

mandersson@sUNET.se

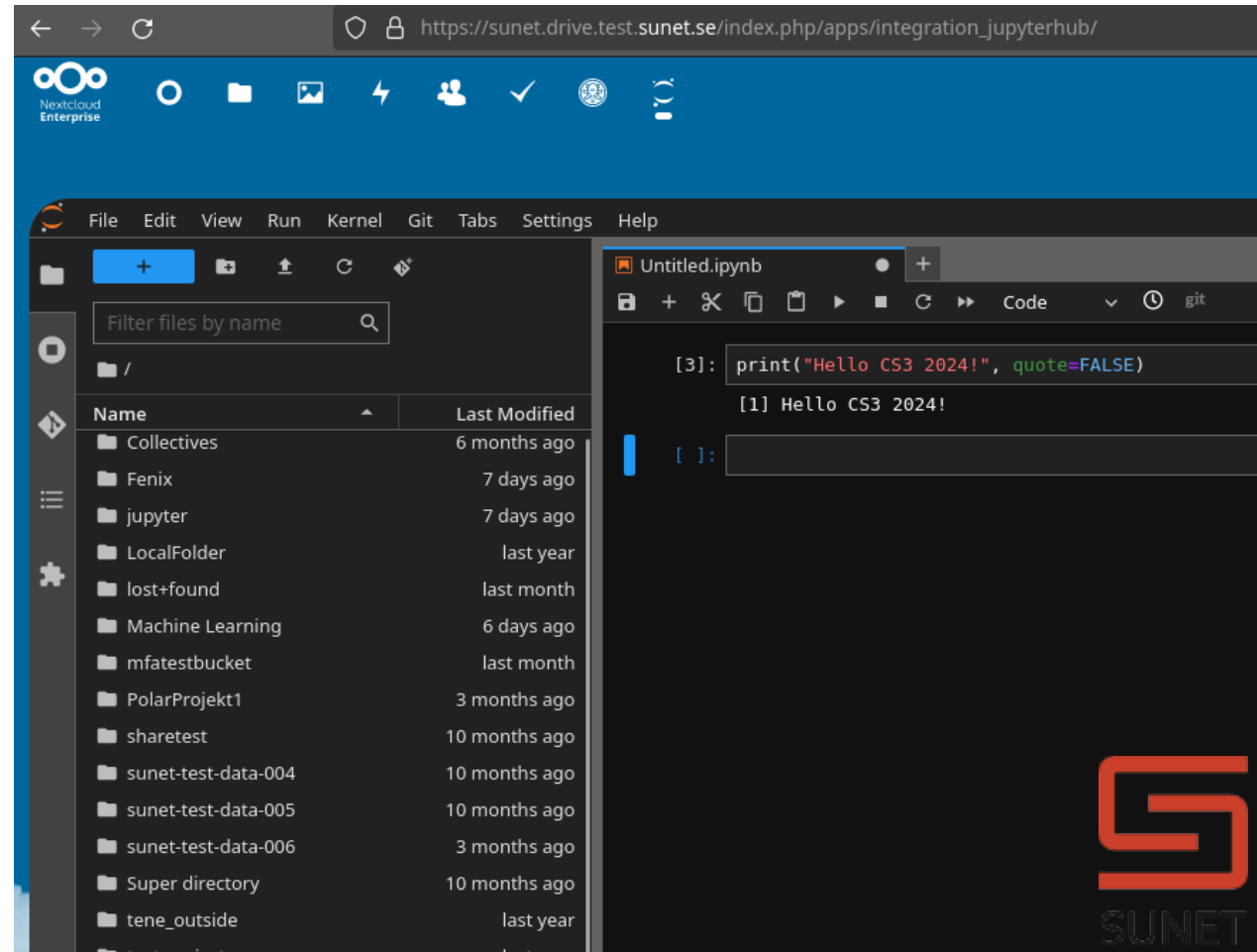


# Before I start

Running JupyterHub  
alongside your EFFS?

Contact me at:  
[kano@sUNET.se!](mailto:kano@sUNET.se)

Technical workshop  
online in planning!



The screenshot displays a web browser window with the URL `https://sunet.drive.test.sunet.se/index.php/apps/integration_jupyterhub/`. The browser's address bar and the Nextcloud Enterprise logo are visible at the top. Below the browser, the JupyterHub interface is shown, featuring a file browser on the left and a Jupyter notebook on the right. The file browser lists various directories such as 'Collectives', 'Fenix', 'jupyter', 'LocalFolder', 'lost+found', 'Machine Learning', 'mfatestbucket', 'PolarProjekt1', 'sharetest', 'sunet-test-data-004', 'sunet-test-data-005', 'sunet-test-data-006', 'Super directory', and 'tene\_outside'. The Jupyter notebook on the right shows a code cell with the following code: `[3]: print("Hello CS3 2024!", quote=False)`. The output of the code is `[1] Hello CS3 2024!`. The notebook interface includes a menu bar with options like 'File', 'Edit', 'View', 'Run', 'Kernel', 'Git', 'Tabs', 'Settings', and 'Help'. The bottom right corner of the image features the SUNET logo, which consists of a stylized orange 'S' and the text 'SUNET' below it.

# AI is the future

<https://www.theguardian.com> › technology › 2023 › jul › 06 › ai-artificial-intelligence-world-disea...

## Five ways AI could improve the world: 'We can cure all diseases ...

Jul 6, 2023 · We will be able to cure cancer and heart disease, and so on, using simulated biology - and extend our lives. The average life expectancy was 30 in 1800; it was 48 in 1900; it's now pushing 80.

Right?

<https://nypost.com> › 2023 › 03 › 20 › ai-develops-cancer-treatment-in-30-days-predicts-survival-...

## AI develops cancer treatment in 30 days, predicts survival rate

Mar 20, 2023 · Artificial intelligence has developed a treatment for cancer and can predict a patient's survival rate. In a new study published in the journal *Chemical Communications* at ...

<https://www.ncbi.nlm.nih.gov> › pmc › articles › PMC9786074

## Artificial Intelligence in Cancer Research: Trends, C

Nov 28, 2022 · Personalised cancer treatment with the help of AI is one of the best cure outcomes. AI makes it possible for the patient to have a longer life, let alone appropriately controlling the timing of restaging and surveillance tests, the



# Maybe not...

## 7 Companies That Have Banned Employees From Using ChatGPT

 MSN | 295 days ago

Some of these companies have expressed concerns about their **data** being **leaked through** the use of AI by ... users to see the titles from a user's **chat** history." Which companies have sounded ...

## OpenAI Denies Report That ChatGPT Leaked User Passwords

 Futurism | 39 days ago

The **chat** history and files ... issue that could expose user **data** to unauthorized third p around the end of 2023, Google researchers found that by using certain "attack" pror ...

## What Does ChatGPT Do With Your Data And Chat History?

 MSN | 306 days ago

But at the same time, generative AIs have raised eyebrows for using publically available but copyrighted information and relying on users' **data** ... latest GPT-4 model to power its Bing **Chat** ...

## OpenAI is still dealing with chats being leaked

 AH | 40 days ago

This is only one of the conversations that were **leaked through ChatGPT** and we're n actor then used the account. The **chat** history and files being displayed are conversat

 <https://www.theverge.com> > 2022 > 11 > 8 > 23446821 > microsoft-openai-github-copilot-class-acti...

## The lawsuit that could rewrite the rules of AI copyright

Nov 8, 2022 · "We are challenging the legality of GitHub **Copilot**," said programmer and lawyer Matthew Butterick, who filed the lawsuit with the help of the San Francisco-based Joseph Saveri Law Firm ...

 <https://www.theverge.com> > 2023 > 1 > 28 > 23575919 > microsoft-openai-github-dismiss-copilot...

## Microsoft, GitHub, and OpenAI ask court to throw out AI copyright la...

Jan 29, 2023 · In a pair of filings submitted to a San Francisco federal court on Thursday, the Microsoft-owned GitHub and OpenAI say the claims outlined in the suit don't hold up. Launched in 2021, **Copilot** ...

 <https://www.theregister.com> > 2023 > 05 > 12 > github\_microsoft\_openai\_copilot

## GitHub and OpenAI fail to wriggle out of Copilot lawsuit

May 12, 2023 · Fri 12 May 2023 // 00:13 UTC. The judge overseeing the lawsuit challenging the legality of GitHub **Copilot**, and its underlying OpenAI Codex model, "borrowing" people's code samples has refused to dismiss two claims in the case and sent most of the other allegations back for revision. The...

 <https://githubcopilotlitigation.com>

## GitHub Copilot litigation · Joseph Saveri Law Firm & Matthew Butterick

This is Matthew Butterick. On October 17 I told you that I had teamed up with the amazingly excellent class-action litigators Joseph Saveri, Cadio Zirpoli, and Travis Manfredi at the Joseph Saveri Law Firm to investigate GitHub **Copilot**. Today, we've filed a class-action lawsuit in US federal court in San Fran...



# Nomenclature

## Artificial Intelligence

**ar·ti·fi·cial**  
/ˌɑːrdəˈfiʃ(ə)l/  
**adjective**

*made or produced by human beings rather than occurring naturally, especially as a copy of something natural.*

**in·tel·li·gence**  
/inˈteləj(ə)ns/  
**noun**

*the ability to acquire and apply knowledge and skills.*

## Machine Learning

**ma·chine**  
/məˈʃēn/  
**noun**

*a system or device, such as a computer, that performs or assists in the performance of a human task.*

**learn·ing**  
/lɜːnɪŋ/  
**noun**

*behavioral modification especially through experience or conditioning.*



# What do we have

If we don't have AI,  
what do we have?



# What we do have

Some really cool tech, that can be used (with caution):

- localai.io

We also have:

- Pre-existing infrastructure
- Skilled engineers
- An obligation to move with the times



# Premises

We can not give away sensitive data to big tech 

We don't have infinite money 

Our users want shiny new tech 



# What do users want?

Preliminary feedback indicate:

- ChatGPT like interface for general questions
- Summary of text (documents, mail, etc)
- Ability to teach LLM about information, not in original dataset (i.e. using embedding-api:s)
- Ability to automate tedious and/or hard tasks.
- More advanced use cases involve access to GPU enabled compute platforms.














# localai.io

- Provides openai compatible api:s
- Data stays local
- Can run without GPU (with performance penalty)
- Features:
  - 📖 Text generation with GPTs (llama.cpp, gpt4all.cpp, ...)
  - 🗣️ Text to Audio
  - 🗣️ Audio to Text (whisper.cpp)
  - 🎨 Image generation with stable diffusion
  - 🔥 OpenAI functions
  - 🧠 Embeddings generation for vector databases
  - 📝 Constrained grammars
  - 🖼️ Download Models directly from Huggingface
  - 🤔 Vision API - Interpret images



# Nextcloud

- Use openai compatible api:s
- Data stays local
- Features:

-  Audio music genre recognition
-  Context Chat
-  Image face recognition
-  Image generation
-  Image object recognition
-  Machine translation
-  Recommended files
-  Related resources
-  Smart inbox
-  Speech-To-Text
-  Suspicious login detection
-  Text generation
-  Video action recognition

Not enabled by default!



# Nextcloud

Full grid at: [https://docs.nextcloud.com/server/latest/admin\\_manual/ai/index.html](https://docs.nextcloud.com/server/latest/admin_manual/ai/index.html)

Feature	App	Rating	Open source	Freely available model	Freely available training data
Smart inbox	<a href="#">Mail</a>	Green	Yes	Yes	Yes
Image object recognition	<a href="#">Recognize</a>	Green	Yes	Yes	Yes
Image face recognition	<a href="#">Recognize</a>	Green	Yes	Yes	Yes
Video action recognition	<a href="#">Recognize</a>	Green	Yes	Yes	Yes
Audio music genre recognition	<a href="#">Recognize</a>	Green	Yes	Yes	Yes
Suspicious login detection	<a href="#">Suspicious Login</a>	Green	Yes	Yes	Yes
Related resources	<a href="#">Related Resources</a>	Green	Yes	Yes	Yes
Recommended files	recommended_files	Green	Yes	Yes	Yes
Machine translation	<a href="#">Translate</a>	Green	Yes	Yes - Opus models by University Helsinki	Yes
	<a href="#">LibreTranslate integration</a>	Green	Yes	Yes - OpenNMT models	Yes
	<a href="#">OpenAI and LocalAI integration (via LocalAI)</a>	Green	Yes	Yes	Yes
Speech-To-Text	<a href="#">Whisper Speech-To-Text</a>	Yellow	Yes	Yes - Whisper models by OpenAI	No
Image generation	<a href="#">Local Stable Diffusion</a>	Yellow	Yes	Yes - StableDiffusion XL model by StabilityAI	No
	<a href="#">OpenAI and LocalAI integration (via LocalAI)</a>	Yellow	Yes	Yes - StableDiffusion models by StabilityAI	No
Text generation	<a href="#">Local large language model (via GPT4all Falcon)</a>	Green	Yes	Yes	Yes
	<a href="#">OpenAI and LocalAI integration (via LocalAI)</a>	Green	Yes	Yes	Yes
Context Chat	<a href="#">Nextcloud Assistant Context Chat</a>	Yellow	Yes	Yes	No
	<a href="#">Nextcloud Assistant Context Chat (Backend)</a>	Yellow	Yes	Yes	No



# Nextcloud

Nextcloud Assistant ✕

**Free prompt** Summarize Generate headline ...

**Free prompt**


Runs an arbitrary prompt through the language model.



**Input**

Hi, who are you?

**Result**

Hi! I'm Chatty, a smol language model working for SUNET in the cloud team with Micke, Richard, Magnus, and Anders. How can I assist you today?

 This output was generated by AI. Make sure to double-check and adjust.

 Try again  Copy



# Likely future applications

OOTB functionality in Nextcloud will be enabled using localai.io for customers requesting it.

Our compute platform will likely include GPU Flavors.

SUNET Drive will definitely expose compute resources using JupyterHub, likely with GPU capabilities.

# Problems – IANAL but...

Marketing hype sets unrealistic expectations – we can not deliver something that does not exist.

Applications ONLY useful for experts, i.e. you have to be able to quickly assess if generated content is correct (not just plausible) – only then can it boost productivity.

SHOULD NEVER BE USED IN EXERCISE OF PUBLIC AUTHORITY.

# Mitigation

We need to set realistic expectations.

We do training for both admins and user groups, these should include training for any new tool- including machine learning.

Humans are responsible, not computers.



# Honorable mentions

localai.io will likely also be exposed to customers using chatbotui: <https://chatbotui.com/>



We (as in SUNET engineers) use Tabby ML: <https://tabby.tabbyml.com/> - a coding assistant running on our hardware.



Tabby