Deck

ALEPH.IM hackathon 2024

Team 13

Problem

Confidentiality

Integrity

Availability

Netflix faces a privacy disaster

This incident took place back in 2006 when the information about movies rented by Netflix subscribers was shared for research but third parties were able to recover user details including watching history, personal preferences, and behaviors.

Target knows you better

Target's intrusive advertisers turned a purchase history into pregnancy prediction algorithm to send coupons to future mothers. It unpleasantly confused families as the organization knew about their child-bearing in advance.

Facial recognition is subverted by protesters

In Hong Kong, protesters have grown increasingly concerned that police abuse facial recognition software to make arrests. To avoid detection, many of them used scarfs, masks, 3D-printed glasses, and even hairstyling and makeup as a disguise.

Microsoft's AI chatbot learns racism from Twitter

Pretty soon after Microsoft launched a Twitter bot Tay, people started tweeting the bot with all sorts of misogynistic, racist, and Donald Trumpist remarks. Tay assimilated the internet's worst tendencies into its personality.

Autopilot keeps crashing Tesla cars

2016 was notorious for Tesla due to their car crash when the car didn't recognize a van stopped in the lane as an obstacle. There were also two other similar Tesla's autopilot accidents in 2016 and 2019 resulting in human deaths.

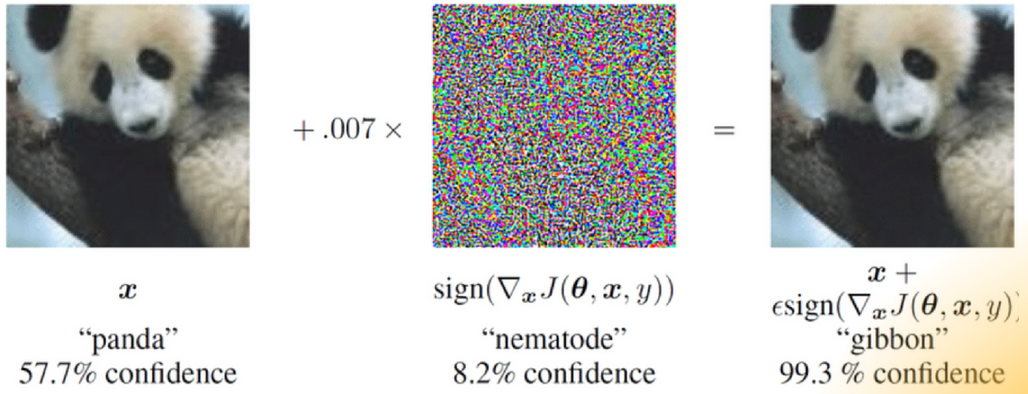
LG robot Cloi fails publicly

Cloi, LG's smart home assistant, was supposed to demonstrate the use of kitchen appliances. Instead, it became unresponsive and left the LG executives red-faced.

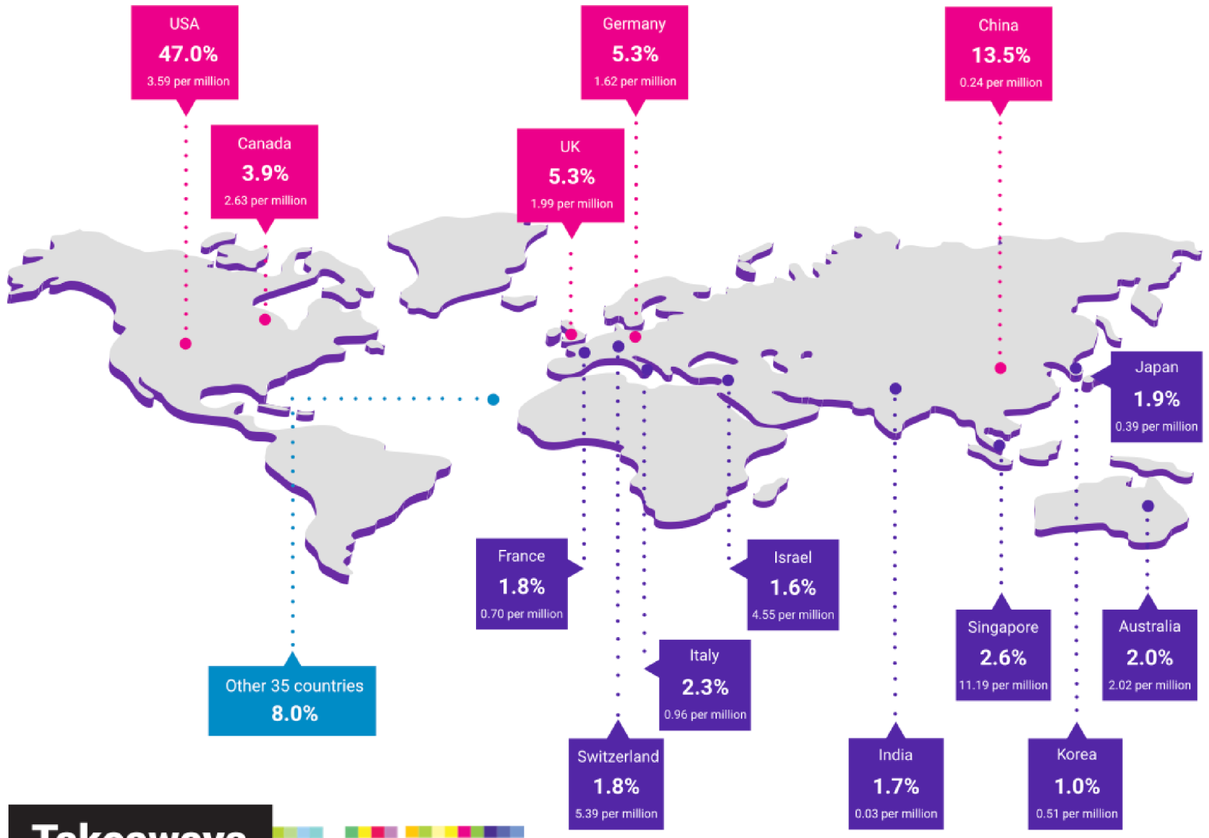
AI datasets are under attack

Attacked AI datasets	Share
Image	60.8%
Text	10.0%
Record	5.5%
Binary	4.3%
Audio	4.1%
Graph	3.2%
Signal	3.0%
Agent	2.8%
3D	2.2%
Traffic	2.1%
Video	1.9%

- The dominance of attacks against AI systems with image processing shouldn't mislead you into thinking that other AI applications are less vulnerable.
- Traditional storage system are not transparent, private and trustworthy, but still more than 50% of OpenAI dataset are stored on AWS. This makes potential attackers jobs much easier



Market Opportunity



Takeaways

AI Security Research by Country

222.66B $

Cyber Security (2023)
(CAGR) of 12.3%

22.80B $

Big Data Security (2023)
(CAGR) of 12.3%

2.19B $

Legal AI Software (2024)
(CAGR) of 14.1%

Solution

Decentralized Protected Dataset Storage

All-in-one Model Training using Decentralized Computing

Verified Dataset and Model marketplace

Benefits

01

Make decentralized computing easily accessible and scalable

02

Considerably reducing attacks vectors. Improve Personal data protection.

powered by ALEPH.IM

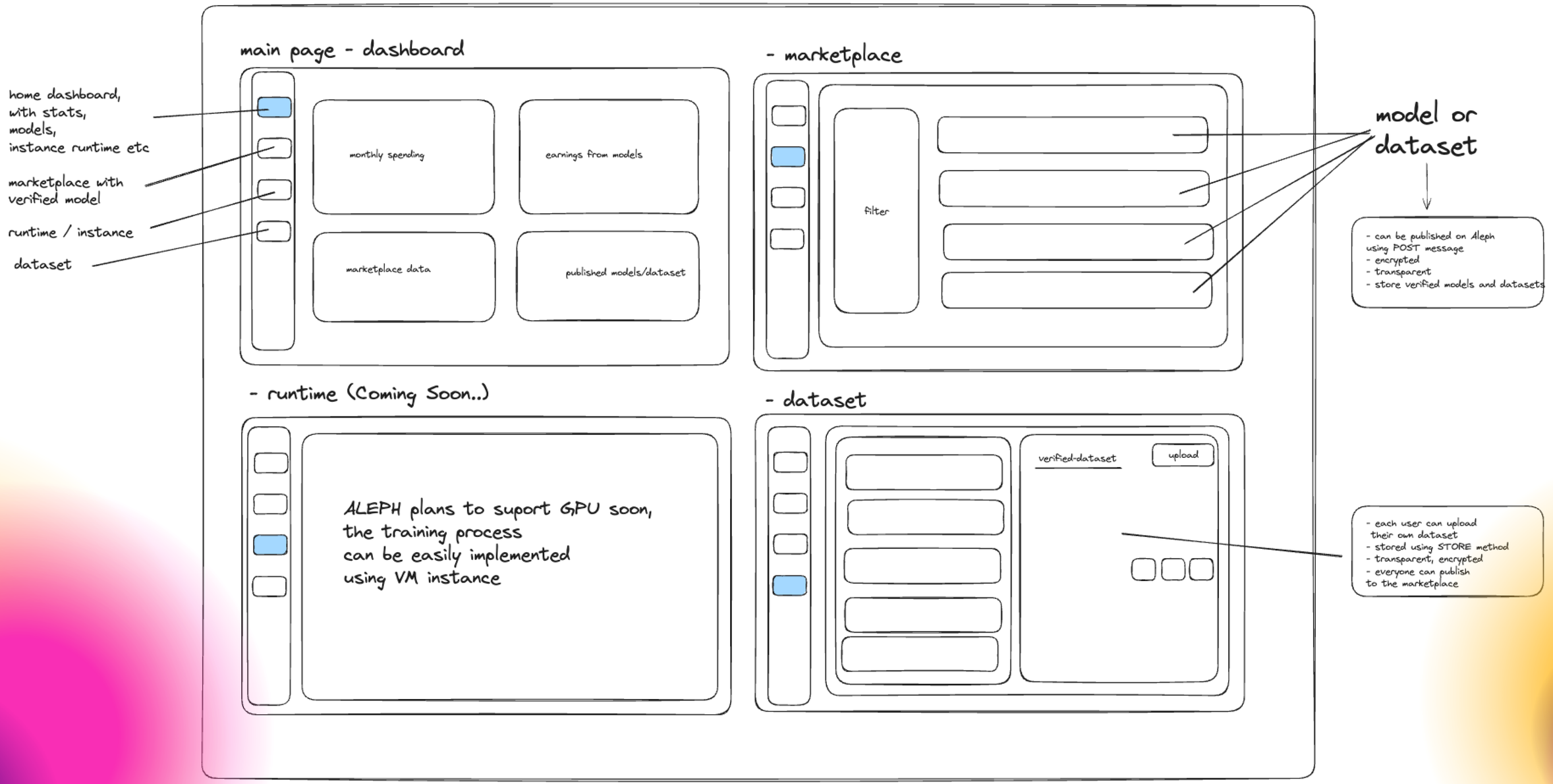
03

Grow Aleph.im communauty, scale the solution globaly and lead the future of Cloud Computing

04

Communauty of marketplace, and rewards system. Anyone can earn money by fine-tuning models

Structure


home dashboard,
with stats,
models,
instance runtime etc
marketplace with
verified model
runtime / instance
dataset
main page - dashboard
monthly spending
earnings from models
marketplace data
published models/dataset
- marketplace
filter
model or
dataset
- can be published on Aleph
using POST message
- encrypted
- transparent
- store verified models and datasets
- runtime (Coming Soon..)
ALEPH plans to suport GPU soon,
the training process
can be easily implemented
using VM instance
- dataset
verified-dataset
upload
- each user can upload
their own dataset
- stored using STORE method
- transparent, encrypted
- everyone can publish
to the marketplace

Roadmap

01

runtime & GPU support

- aleph.im runtime support
- gpu support
- dedicated pre-loaded instance

02

token rewards system

- Token reward for contributors
- active communauty
- make easily shareable model and SDK loaders

03

verified dataset & model

- AI Act compliant dataset
- first platform with gov verified models
- leverage Aleph and blockchain for a more secure system