Deep Tensor

Securing Tomorror's AI/ML, Today!

Mormor Karl

Reliable ML / AI

Xuan-Son (Sonny) Vu (PhD.)

Assistant Prof. at RSS, CS Department, LTH
Founder at DeepTensor AB
CTO at WASP Media & Language, UMU

Email: xuan-son.vu@cs.lth.se / s.vu@deeptensor.ai

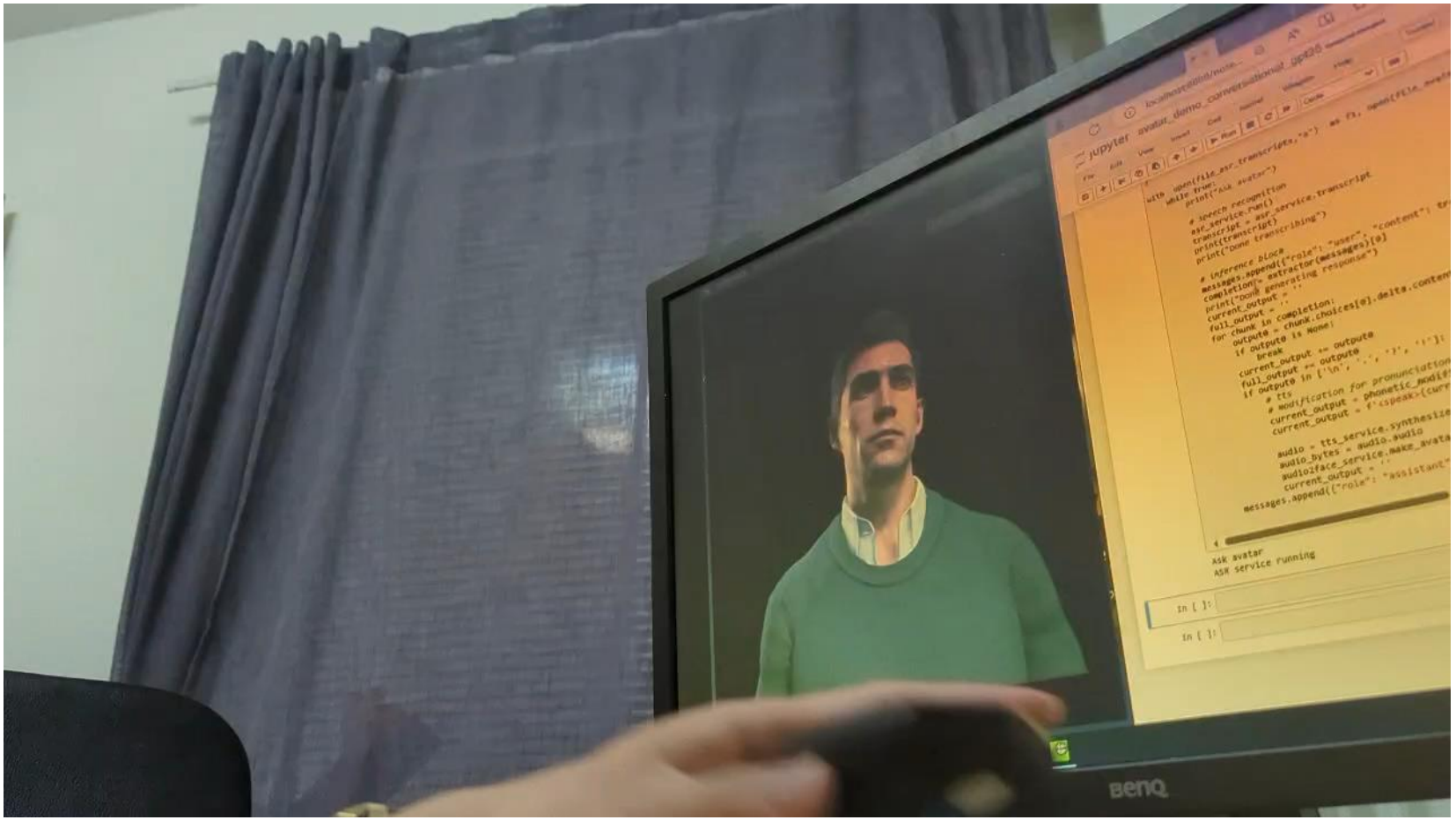
LUNDS UNIVERSITET

Xuan-Son (Sonny) Vu

Assistant Prof. at RSS, CS Department, LTH
CTO at WASP Media & Language
Founder of DeepTensor AB

- Profile:
  - PhD. in privacy-preserving ML
  - MSc. in natural language processing + ML
  - BSc. in opinion mining
- Research interests:
  - Trustworthy ML/DL, graph learning in NLP/**multimodal data**, meta learning
- Research contributions:
  - Co-authored different neural models - e.g., ppRNN (faster version of RNN), MGTN (modular model), SGTN (privacy-preserving), Cformer (meta pseudo labels).
  - Published at top conferences: AAAI, WWW, ACMMM, EMNLP, COLING, CICLING
- Founders:
  - MLOPs.VN, AIHUB.ML, and DeepTensor AB (securing AI/ML solutions)
- Long-term research:
  - Reliable ML/AI, acquiring knowledge from multimodal data, and using structured knowledge to power downstream applications (AI/IoT, Robotics, Healthcare).
  - Knowledge to solve: ML + data science

VIRTUAL AVATAR (KEVIN)

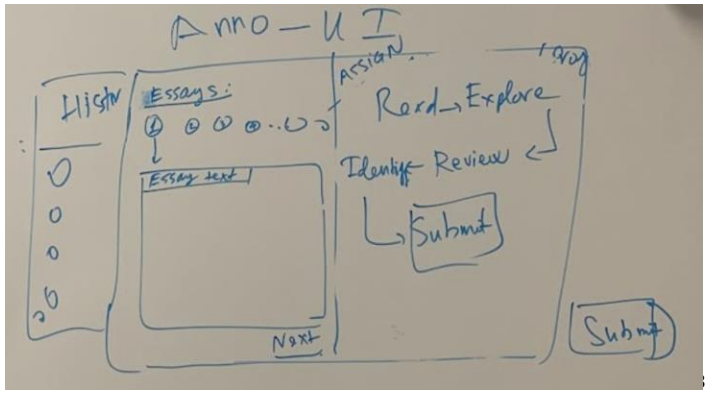


VIRTUAL AVATAR (JADE)

LUNDS UNIVERSITET

PROJECTS

- AI-operator (1-3 students)
  - Supervisors: Sonny Vu, Johanna Björklund
  - Work with Virtual Avatar framework
  - Enhance it with screen operation
  - Write report
- Motiviated Intruder (NLP) (1-2 students)
  - Supervisors: Sonny Vu, Elena Volodina, Therese, Simon
  - Questions:
    - How well do we protect writer's identities by applying pseudonymization?
    - How does the profile of "motivated intruders" facilitate/impede re-identification?
    - How many pseudonym groups are necessary to protect writers? Which ones?
  - TODO:
    - Design GUI for the motivated Intruder tests
    - Experiment
    - Write report



LUNDS UNIVERSITET

LUNDS UNIVERSITET