Xiaopeng Ke

Portfolio: https://sites.google.com/view/xiaopeng-ke
Github: github.com/mezereonxp
Email: mezereonxp@gmail.com
Mobile: +86-130-3249-4890

Education

- **Northeastern University** Shenyang, China
  Bachelor of Engineering - Software Engineering; GPA: 3.82 *July 2015 - June 2019*
  Courses: *Operating Systems, Data Structures, Analysis Of Algorithms, Networking, Databases*
- **Nanjing University** Jiangsu, China
  Master of Engineering - Computer Science; GPA: 4.45 *July 2019 - Present*
  Courses: *Advanced Machine Learning, Distributed System, Cryptography, Introduction to the Theory of Computation*

Experience

- **Xiaomi Inc.** Beijing, China
  Middleware Engineer (Intern) *March 2018 - Oct 2018*
  - **Zander - A tracing system for analyzing service status**: Created a unsupervised anomaly detection module with multiple algoirthms such as LOF, Isolation Forest, and HoltWinter.

Projects

- **Automation Slicing and Testing for in-App Deep Learning Models**: We propose a framework to automatically slice and test numerous in-app deep learning models. In our framework, we propose two reconstruction methods to convert the in-app model to the trainable model with correct preprocesss and postprocess procedures. With that framework, we study 100 commercial in-app models and find 56% of in-app models are vulunerable to robustness issues.
- **Privacy-Preserving and Robust Federated Deep Metric Learning**: We propose a new paradigm to train the deep metric learning model under the federated training scenario. We also make proofs on the convergence of the training process. To protect the participants' training data, we apply the differential-privacy technique to the training process.
- **Practical Long Video Summary**: We observe that current SOTA video summary techniques rely on the Kernel Temporal Segmentation (KTS) method. Since KTS takes heavy computation under long videos, it is time-consuming to do the video summary on long videos. To tackle this problem, we propose a practical long video summary pipeline to reduce the complexity of KTS by analyzing the long-tail distribution characteristic of video shots.
- **Adversarial Robust Deep Metric Learning**: We study the Adversarial Robustness of Deep Metric Learning and discover the Mix-Up defenses are all failed in Deep Metric Learning under adversarial examples. We also propose an Ensemble Adversarial Training to enhance the robustness of Deep Metric Learning.
- **Inference Data Protection for BlackBox Deep Learning Service**: Users always upload their data to enjoy the deep learning service. These input data could be used for other tasks. Thus, we propose an algorithm to remove unnecessary information from the inference data by serval queries. These inference data sanitized are hard to exploit on other tasks.

Publications

- **Conference Paper: GAPter: Gray-box Data Protector for Deep Learning Inference Services at User Side** : Wu Hao, Bo Yang, Xiaopeng Ke, Siyi He, Fengyuan Xu, and Sheng Zhong. (ICASSP-2023)
- **Conference Paper: Privacy-Preserving and Robust Federated Deep Metric Learning** : Yulong Tian, Xiaopeng Ke, Zeyi Tao, Shaohua Ding, Fengyuan Xu, Qun Li, Hao Han, Sheng Zhong, Xinyi Fu. (IWQoS-2022)
- **Conference Paper: Towards Efficient and Practical Long Video Summary**: Xiaopeng Ke, Boyu Chang, Hao Wu, Fengyuan Xu, and Sheng Zhong. (ICASSP-2022)
- **Conference Paper: Efficient Architecture Paradigm for Deep Learning Inference as a Service.**: Jin Yu, Xiaopeng Ke, Fengyuan Xu, and Hao Huang. (IPCCC-2020)

Honors and Awards

- ATEC Competition Season-II: Digital Currency Transaction Fraud Identification (Rank 4), 2021
- ACM MM2021 AIC Phase VII: Robust defense competition for e-commerce logo detection (21/36489), 2021
- Outstanding Graduate, 2019
- National Second Prize in Mathmatical Modeling Competition, 2018
- Huawei Named Scholarship, 2018
- First Class Award of NEU Mathematical Modeling Competition, 2017
- First Prize of "ZhongTian" Iron and Steel Mathematical Modelling Challenge, 2016

Granted Patent

- CA-2022105476061:Mobile Device Collaborative Inference System for Deep Learning Transformer Models

Opensource Experience

- **AnomalyDetectTool**
  Release a tool project "AnomalyDetectTool" for detecting anomaly points at github with 74 stars. *Jan 2019*