AVSS Workshop

PPSS: Privacy-Preserving Surveillance Systems

AVSS 2023 Workshop Proposal

1. Workshop Title

PPSS: Privacy-Preserving Surveillance Systems

2. Organizers

Sung Whan Yoon
Assistant professor, AI Graduate School & Department of Electrical Engineering – Ulsan National Institute of Science and Technology (UNIST)
Ulsan, South Korea
shyoon8@unist.ac.kr

Short Bio: He is currently an assistant professor at Graduate School of AI & Department of Electrical Engineering at Ulsan National Institute of Science and Technology (UNIST) since Mar. 2020. He received a Ph.D. degree from School of Electrical Engineering at Korea Advanced Institute of Science and Technology (KAIST), in Aug. 2017, under the supervision of Prof. Jaekyun Moon. Before joining UNIST, he was a postdoctoral researcher at KAIST from Sep. 2017 to Mar. 2020. His research interests are in the area of artificial intelligence, distributed learning systems, and intelligence communications. When focusing on the machine learning field, he has been dedicated to meta-learning algorithms for few-shot image recognitions (the results were published in ICML 2019 & NeurIPS Meta-Learning Workshop 2018). Also, he is interested in implementing algorithms for incremental/continual learning (the work was published in ICML 2020). In the further direction, he has suggested a domain generalization algorithm across diverse image domains (the related work was published in AAAI 2023). He is also interested in federated learning systems for training deep models in a decentralized/private way (a recent work that combines meta-learning and federated learning was presented at AAAI Privacy-Preserving AI Workshop 2023).

Jonggyu Jang
Postdoctoral researcher, Department of Electrical Engineering – Pohang University of Science and Technology (POSTECH)
Pohang, South Korea
jgjang@postech.ac.kr

Short Bio: He is currently a postdoctoral researcher in Department of Electrical Engineering at Pohang University of Science and Technology (POSTECH). He received the B.S. and Ph.D. degrees in electrical engineering from the Ulsan National Institute of Science and Technology (UNIST), Ulsan, Republic of Korea, in 2017 and 2021, respectively. From March 2021 to March 2023, he was a Postdoctoral Researcher at the Future IT Innovation Laboratory, Pohang University of Science and Technology (POSTECH). His research interests include theories and applications for wireless communication and deep learning privacy.

Hosung Joo
Ph.D. Student, Department of Electrical Engineering – Pohang University of Science and Technology (POSTECH)
Pohang, South Korea
zxcqa123@postech.ac.kr

Short Bio: He is currently pursuing on Ph.D. in the Department of Electrical Engineering in Pohang University of Science and Technology (POSTECH). He received B.S. from the School of Electrical Engineering and the minor degree from the School of Computer Science from Korea Advanced Institute of Science and Technology (KAIST) in 2019. He worked as a researcher at Electronics and Telecommunication Research Institute (ETRI) from Mar. 2019 to Feb. 2021. His research interests are based on integrated sensor applications including radar, X-ray imaging, 3D meta-structure design, 3D image and point cloud reconstruction, artificial intelligence, and modern wireless communication with localization by information fusion.

3. Workshop and Challenge Introduction

The sensor is a fundamental component for next-generation services such as smart cities, autonomous driving, and telemedicine. These services are expected to generate a significant amount of data, as numerous sensors will be used to monitor daily activities. However, with the increased use of sensors, concerns about privacy violations become more pronounced. Visual data privacy is one of the most crucial privacy concerns for individuals. Moreover, the importance of privacy protection is becoming increasingly relevant due to regulatory frameworks such as the European Union's General Data Protection Regulation (EU GDPR) and the California Consumer Privacy Act (CCPA), which focus on safeguarding data privacy at the national level. In this workshop, we aim to engage with researchers from diverse backgrounds to explore innovative strategies for preserving the privacy of data. We seek to share advanced concepts and ideas on this topic, and to foster new perspectives on how privacy preservation can be achieved in this context. By doing so, we hope to identify promising research directions that will address the critical privacy issues surrounding the use of sensors in emerging technologies.

4. Workshop Topics

We conduct an extensive investigation of privacy-protecting methodologies for the surveillance and monitoring applications. Moreover, we explore not only direct information protection but also theoretical protection methods against learning model attacks such as inversion attacks, membership inference attacks. We will invite speakers with professional knowledge and experience about the topics:

- Privacy protection methods for 2D/3D visual data (RGB images, 2D/3D key points or features, point clouds, Deep steganography, and others)
- Privacy threats on text generation model
- Privacy-preserving LiDAR, RADAR image/signal applications
- Privacy-preserving voice signal applications
- Theoretical foundations against model inversion attacks, membership inference attack
    - Differential Privacy
    - Homomorphic Encryption
    - Federated Learning

5. Expected Schedule

Program	
Opening Remarks	13:00 – 13:15
Invited Talk 1,2,3	13:15 – 15:00
Coffee Break	15:00 – 15:40
Oral presentations	15:40 – 17:40
Concluding Remarks	17:40 – 18:00

6. Program Description

We collect surveys or brief technical contributions about the privacy-preserving surveillance systems (PPSS). Authors are expected to submit extended abstract of the paper containing more than 300 words for each submission. If their contributions were accepted, the authors will give a 15-minute oral presentation at the workshop. The accepted contributions will be combined into a single merged workshop paper which will be included and published to the proceedings of IEEE AVSS 2023.

7. Important Dates

Proposal	
Workshop Site Open	July 20, 2023
Contribution Paper Deadline	September 10, 2023
Acceptance Notification	October 1, 2023
Workshop date	November 6, 2023

* Abstracts submitted to the merged survey will be considered for publication of the workshop paper after editorial modifications.