Derin Cayir

+1 (786) 301-4952 | Miami, Florida, US | derin.cayir@gmail.com

PROFESSIONAL SUMMARY

My research focuses on leveraging advanced machine learning techniques to address security and privacy concerns in emerging technologies particularly in AR/VR devices. I am especially interested in AI, machine learning, signal processing, AR/VR, and security/privacy. In addition to my core research, I have industry experience that includes various roles where I applied machine learning to tackle complex, real-world challenges across different domains. Additionally, I contribute as an active reviewer to Springer Nature's Virtual Reality journal, Elsevier Computer Networks, and ACM SIGCSE, where I leverage my knowledge in cybersecurity to help advance the field.

EDUCATION

Doctor of Philosophy in Computer Science, Florida International University — December 2022 — June 2026

- GPA 4.00

Master of Science in Computer Science, Florida International University — December 2022 — December 2024

- GPA 4.00

Bachelor of Science in Electrical and Electronics Engineering, Bilkent University — August. 2018 — June 2022

- GPA: 3.1

PROFESSIONAL WORK EXPERIENCE

Graduate Research Assistant — December 2022 — July 2026
Florida International University — *Miami, Florida*

- Conducted a data-driven approach and implemented ML models to analyze privacy risks and malicious effects of benign-looking apps on emerging technologies, i.e. AR/VR.
- Published academic papers in top-tier venues, contributing new knowledge on AR/VR device security and privacy.
- Developed and led 11 hands-on labs focusing on IoT security, monitoring more than 10 graduate students and enhancing their practical and theoretical knowledge.
- Served as a Teaching Assistant for Graduate Level courses in Network Security, and IoT Security and Privacy, and Computer Data Analysis mentoring students and designing course content.

Researcher — December 2021 — August 2022
Tubitak — *Ankara, Turkey*

- The Scientific and Technological Research Council of Turkey.
- Developed machine learning algorithms to automatically detect anomalies in satellite data.

Software Engineering Intern — Aug 2021 - Aug 2022
Arcelik — *Anakara, Turkey*

- Engineered a control feedback system for a solar-powered refrigerator, optimizing energy consumption and improving system responsiveness.
- Conducted simulations and real-world testing to validate the efficiency of the solar energy system under varying environmental conditions.

Software Engineering Intern — Jun 2021 - Aug 2021
Havelsan — *Turkey*

- Engaged in the development of autonomous vehicle systems, including traffic sign recognition projects.
- Performed data augmentation and model training using thousands of images to achieve high accuracy and reliability in sign detection under diverse conditions.

Software Engineering Intern — Jun 2020 - Aug 2020
Integrated Systems and Systems Design (ISSD) — *Ankara, Turkey*

- Employed image processing techniques and machine learning to accurately count and report available parking spaces.

SELECTED PUBLICATIONS

- [**IEEE S&P Magazine '24**] Augmenting Security and Privacy in the Virtual Realm: An Analysis of Extended Reality Devices. **D. Cayir**, A. Acar, R. Lazzeretti, M. Angelini, M. Conti and S. Uluagac. IEEE Security & Privacy, Jan. 2024. *Accepted* **Received 2023 Best Paper Award**.
- [**NDSS '25**] Speak Up, I'm Listening: Extracting Speech from Zero-Permission VR Sensors. **D. Cayir**, R. Aburas, B. Celik and S. Uluagac. *Accepted*.
- [**USENIX '25**] What Moved My Cursor? Inaudible Acoustic Attacks in Virtual Reality. **D. Cayir**, R. Aburas, B. Celik and S. Uluagac. *Under Review*.
- [**PETS '25**] Does the HIPAA Security Rule Hinder Patient Care? Perspectives from Healthcare Workers in a Real Hospital Setting. **D. Cayir**, M. Angee, A. Acar, and S. Uluagac. *Under Review*.

SKILLS

Programming Languages	Python, SQL, Matlab, C/C++, Swift
Technologies	TensorFlow, Pandas, Pytorch, Git, OpenCV, Unity, Unreal Engine, Wireshark, XCode

SELECTED PROJECTS

Speech Extraction from VR IMU Sensors(Python, PyTorch, Machine Learning, SQL, C++, Time Series Analysis)

- Found that through a benign-looking malicious app, the data collected from accelerometer and gyroscope sensors can reveal the speech content such as digits said, SSN, birthdate, and the gender of the user with 90% accuracy.
- Analyzed different time and frequency domain features with Machine Learning models as well as CNN-LSTM Mel-spectrogram-based image classification.
- Fine-tuned Generative AI text-to-speech models (Style TTS and Tacotron 2) to enhance the dataset.
- Proposed a novel defense solution that mitigates such attacks by levereging the frequency band of non-audible sounds to craft frequency-swept noise to the IMU sensors, reducing potential eavesdropping threats by over $\simeq 80\%$.

Cursor Hijacking Attack and Mitigation Through Acoustic Noise Injection(Python, TensorFlow, Machine Learning, C++)

- Found that IMU sensors are susceptible to acoustic noise injection attacks which results in an attacker being able to control the cursor of the user through the on-device speakers of AR/VR devices.
- Developed and tested mitigation techniques using machine learning models to distinguish between genuine user inputs and noise-induced manipulations, enhancing system security.

Facial Feature Analysis and Re-Identification in Online Photos Using Computer Vision(Python, Swift, Computer Vision, Machine Learning)

- Investigated the feasibility of using anonymized facial features extracted by VR apps to identify individuals in online photo datasets, highlighting potential privacy vulnerabilities and the capabilities of modern computer vision techniques.
- Developed a proof-of-concept application in VisionPro that employs machine learning algorithms to match extracted facial features with publicly available online photos, demonstrating how attackers could potentially compromise user anonymity.

Healthcare Workers' Perception of Security Rules(Statistics, Data Analysis, Python, SQL)

- Conducted comprehensive research on HIPAA compliance in healthcare by analyzing the survey data from 70 healthcare workers, demonstrating skills in data analysis and technical problem-solving.
- Identified key factors in the data where certain behavioral characteristics of healthcare workers tend to predict their behavior and attitude toward security.
- Utilized Ordinary Least Squares (OLS), factor analysis, and Hierarchical Linear Regression methods for data analysis.

Extended Reality Device's Security and Privacy

- Published a Systematization of Knowledge (SoK) paper on the prestigious journal IEEE Security and Privacy's Special Issue on Security and Privacy for the Metaverse.
- Analyzed the literature on the attacks and defenses on security and privacy and suggested future research directions. Analyzed the current Extended Reality devices on the market for their security and privacy properties.