Replay Attack Detection in Multimedia of Things (MoT)

Khalid Malik, PhD; Brandon Kujawa

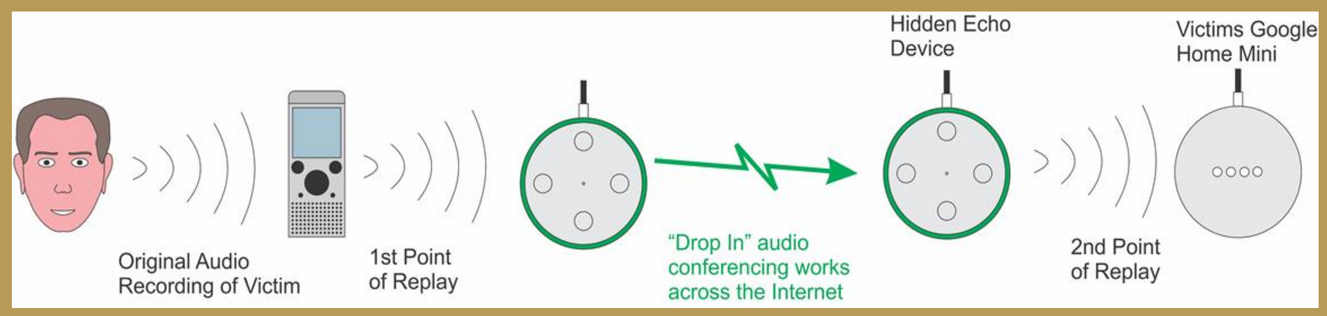
http://secs.oakland.edu/~mahmood/

The Goal of this project is to develop a framework for digital audio forensic analysis, to study the impact of anti-forensic attacks on detector performance, replay and cloning attacks on speaker recognition systems, and to design such a benchmarking testbed.

This digital audio forensic project aims to solve these problems by doing the following:

- Creating an extensive dataset consisting of audio samples taken from many environments and speakers, replaying these samples through multiple replay attack scenarios to get a variety of genuine and spoofed audio samples.
- Developing and testing different audio analysis methods for detecting different spoofing attacks such as replay and cloning attacks.

Example of multi-order replay attack scenario:



This diagram demonstrates a common way an attacker could compromise an end-user's device by using a multiple devices to relay the attack to target device.

Detection and analysis methods:

- 40 features are extracted from each audio sample MFCC, GTCC, Spectral features
- Using high correlation analysis via Pearson Correlation Coefficient we were able to take the number of necessary features down from 40 to 23. Using Variance Inflation factor to further narrow the features down to the 10 most important.

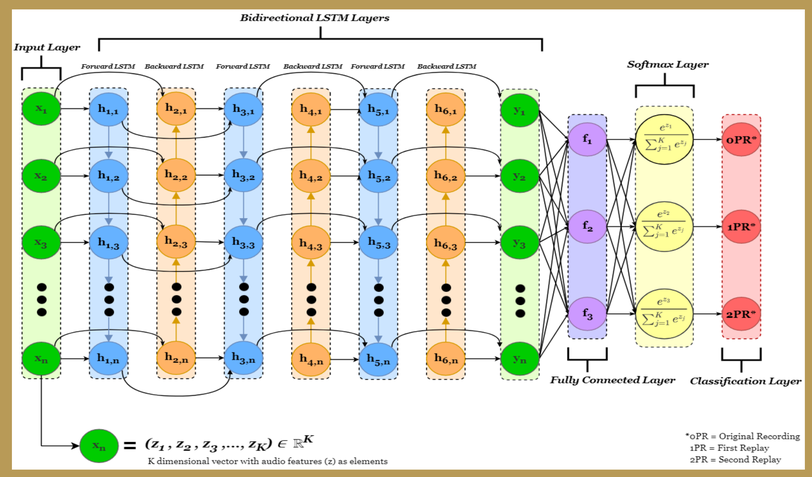
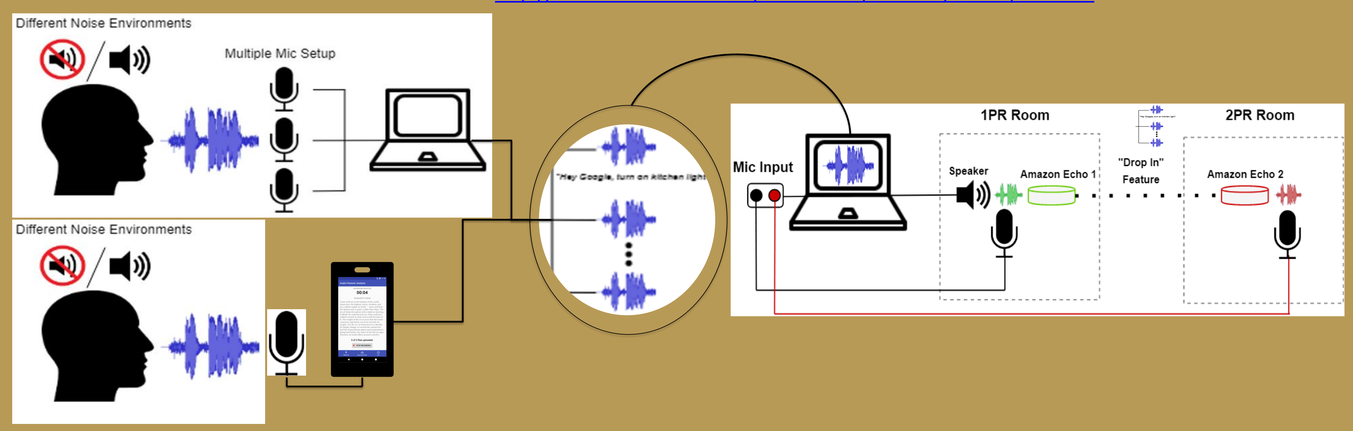


Fig. 4 A visual representation of our deep learning algorithm.

Dataset creation for multi order replay attacks:

Dataset link: http://www.secs.oakland.edu/~mahmood/datasets/audiospoof.html



Results for SVM vs. Deep Learning:

Broader Impact:

- The broader impacts of the proposed research are envisioned in several areas including digital forensics, national security, fintech industry, law enforcement, cyberspace, voice-activated services, and the entertainment industry.
- The project is likely to benefit society at large in areas including civil and criminal proceedings, media, politics, business, and science.
- Research products such as a dataset for benchmarking audio forensic algorithms, consisting of thousands of real-world audio recordings made across the globe using thousands of microphones, and the *ForensicExaminer* system will be valuable to researchers to "crowdsource" audio forensics research, analysis, and performance evaluation on real-world data.

Education and Outreach:

- Increase the number of student participation in areas of STEM and the study of the next generation of digital technologies, both theoretical and practical applications.
- The iDetect challenge, is based on a set of hands-on activities involving multimedia data generation, manipulation, and analysis. This serves as a way to reach out in the community to interest more young high school and undergraduate students in STEM.
- From a scientific and educational standpoint, this field of study is particularly timely, given the ubiquity of media generation and sharing in the mobile computing and social-networking age.

Scientific Impact and Contributions:

- SMILES Lab dataset created for use in this research. This dataset has been made publicly available and has the potential to be used in many different kinds of research regarding the analysis of audio files and speech verification. Sensors or ECU fingerprint modeling and extraction algorithms for IoT and Vehicle Forensics
- Linking generated data to the originating Sensor/ECU IoT and Vehicle Forensics.
- Impact of anti-forensic attacks on existing deep fake and other forgery detectors
- Analyzing performance of existing and new algorithms under selected anti-forensics attacks on CPS forgery detectors