EE/CprE/SE 491 BI-WEEKLY REPORT

10/11/2021-10/25/2021

Group number: 13

Project title: Adversarial AI to Prevent Microarchitectural Website Detection Attacks

Client &/Advisor: Berk Gulmezoglu

Team Members/Role: Ege Demir, Sean McClannahan, Aaron Anderson, Thane Storley

- **Bi-Weekly Summary** These past two weeks we have worked on saliency maps and cache noise creating code as two different groups.

- **Past 2 week accomplishments·**

Ege Demir: Implemented SmoothGrad saliency map technique on dataset and DL model.

- **Aaron Anderson:** beginning modifying prime and probe code for noise injection
- **Sean McClannahan:** Helped Ege with research on saliency maps.
- **Thane Storley:** worked on a plan for noise injection pending proper data collection

- **Pending issues**

- **Ege Demir:** We need to create the saliency mean of all samples to get better understanding of which zones DL model focuses more. We also need to test the findings with artificially induced noise on data samples.

Aaron Anderson: Need to figure out how to effectively access array to adversely affect AI

- **Sean McClannahan:** Gaining a clear understanding of saliency maps.
- **Thane Storley:** Using Saliency data to our advantage

○ **Individual contributions**

NAME	**Individual Contributions** *(Quick list of contributions. This should be short.)*	**Hours this bi-week**	**HOURS cumulative**
Ege Demir	Research & Implementation of Saliency Map	8	41
Aaron Anderson	JS coding and Research	5	35
Sean McClannahan	Research and theory	6	32
Thane Storley	Design, research	5	29

○ **Plans for the upcoming week**

- **Ege Demir:** We need to create the saliency mean of all samples to get better understanding of which zones DL model focuses more. We also need to test the findings with artificially induced noise on data samples.

- **Aaron Anderson:** Use saliency map to assist with noise insertion JS code
- **Sean McClannahan:** Continue working with Ege on saliency maps and how to apply them to our project.
- **Thane Storley:** Produce noise injection method with saliency data

Meeting with Advisor: We discussed progress on the javascript and saliency map.