Eduard Josep Bel Ribes

LEVERAGING INTER- AND INTRA-CLASS DISTANCES FOR POISONING ATTACKS

MASTER'S THESIS

Directed by Dr. Alberto Blanco Justicia

Master's Degree in Computer Security Engineering and Artificial Intelligence

UNIVERSITAT ROVIRA i VIRGILI

Tarragona
2023

Acknowledgements

I want to thank...
blablabla

Resum

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat.

Resumen

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna.

Abstract

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna.

Contents

List of code snippets

List of Figures

List of Tables

1 Introduction

intro to what we are going to talk about in this section, long text

1.1 Motivation

motivation of the project

1.2 Objectives

what we aim to find out

1.2.1 Text examples

Example text example text

2 Background

intro to the section, what are we going to talk about?

2.1 Federated Learning

What is it? where can it be found? pros?

Federated Learning (FL, McMahan et al., 2017a) has emerged as a promis- ing paradigm for training machine learning (ML) models using decentralized data.(MODIFICAR)

2.2 Security attacks on Federated Learning

blabla

2.2.1 Example subsubtitle

2.2.2 Text examples

Example text example text

3 Architecture

intro to the section, what are we going to talk about?

3.1 Project's architecture

architecture of Najeeb's code, where are my functions? scheme on how the system (server, epochs, peers, peer rounds) works

3.2 Security attacks on Federated Learning

blabla

3.2.1 Example subsubtitle

3.2.2 Text examples

Example text example text

4 Implementation

intro to the section, what are we going to talk about?

4.1 Creating the flipping functions

What is it? where can it be found? pros?

4.1.1 Example subsubtitle

5 Results

intro to the section, what are we going to talk about?

5.1 Results for entropy-based label flipping

What is it? where can it be found? pros?

5.2 Security attacks on Federated Learning

blabla

5.2.1 Example subsubtitle

6 Example title

6.1 Example subtitle

6.1.1 Example subsubtitle

7 Text examples

Example text example text

7.1 Bold & italic text

Bold text

Italic text

7.2 In document refernces

Equation 1

7.3 Other documents refernce

referenced text[2] test cite [1]

7.4 Acronyms & footnotes

ACRONYM[1]

Footnote[2]

7.5 Hyperlinks / URLs

Exemple of named hyperlink

[1] Acronym text
[2] Footnote text

8 Example lists

8.1 Unordered list

- Item
- Item
- Item

8.2 Ordered list

1. Item
2. Item
3. Item

9 Equation example

$$a^b = c \tag{1}$$

10 Table example

	API Disponible	API Obsoleta	Dificultat	Característiques avançades
Camera	1	21	Senzilla	No
CameraX	21	N/A	Senzilla	Sí[3]
Camera2	21	N/A	Complexa	Sí

Table 1: Comparativa d'APIs de càmera

As we can see in Figure 1, it works

11 Image example

Figure 1: Logo URV

12 Code snippet example

For all minted listings is required to enable *-shell-escape* on the LaTeX executable and have pygments installed

```
import numpy as np

def incmatrix(genl1,genl2):
    m = len(genl1)
    n = len(genl2)
    M = None #to become the incidence matrix
    VT = np.zeros((n*m,1), int)  #dummy variable

    #compute the bitwise xor matrix
    M1 = bitxormatrix(genl1)
    M2 = np.triu(bitxormatrix(genl2),1)
...
```

Code 1: Code example

13 Diagram examples

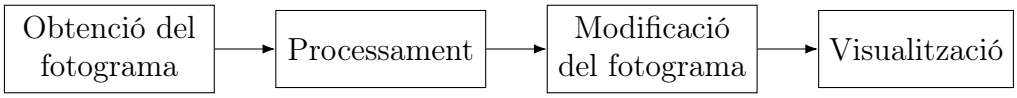

Figure 2: Projecte workflow

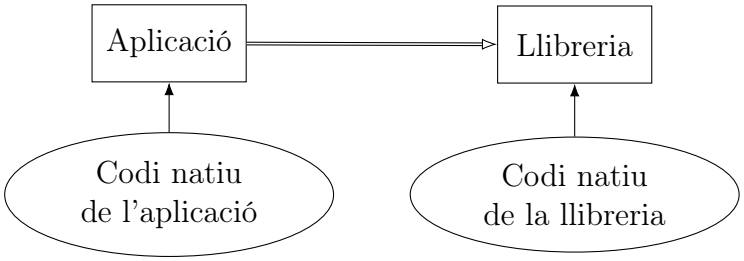

Figure 3: Module dependency

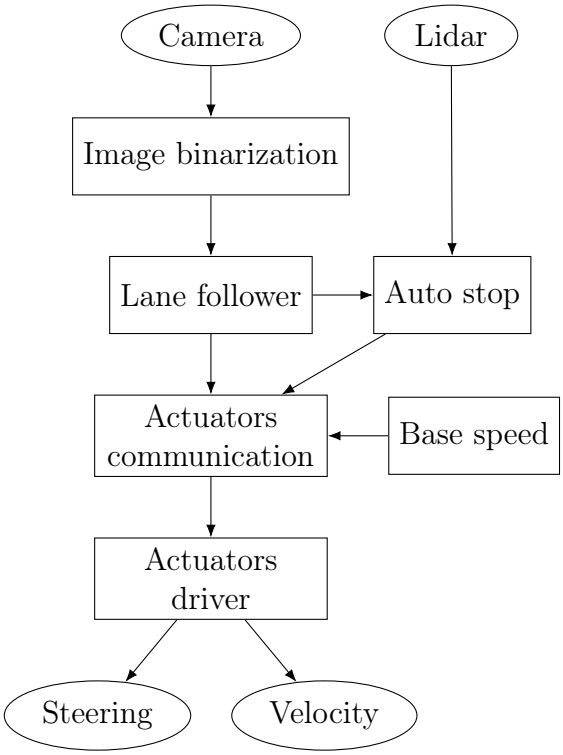

Figure 4: Car nodes layout

References

[1] Dirac, Paul Adrien M.: *The Principles of Quantum Mechanics*. Clarendon Press, 1981 (International series of monographs on physics). – ISBN 9780198520115

[2] test: *Online Title*. 2021. – URL https://www.example.com

Appendix A:
Apendix example