**Notice 1: The execution times are under the effect of other running applications on the system!**

**Important 1: The final decision unit is in the trustworthy part of the cellphone that the client is not able to make any intrusion into it. 🡪 TrustZone**

**Important 2: An attacker does not have any information about the system architecture. So, he/she needs to assume different recognition system architectures and launch multiple attacks in order to perform a successful malign operation.**

**Notice 2: Since the CNN is pre-trained and it does not always provide the same results, the most common values are reported.**

**Fingerprint Experiment 1 (Feature Extractor = CNN; SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0117 | 0.9883 |

**Execution Time = 632.048221 (s)**

**Fingerprint Experiment 2 (Feature Extractor = CNN; Infected SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

**Insider Attack: Manipulation of 12.5% of the Training Labels**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9922 | 0.0078 |
| Fake Fingerprint | 0.0156 | 0.9844 |

**Execution Time = 638.267665 (s)**

**What Happened? Unauthorized Access and Denial of Service!**

**Fingerprint Experiment 3 (Feature Extractor = CNN; Infected SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

**Insider Attack: Manipulation of 25% of the Training Labels**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0234/0.0273 | 0.9766/0.9727 |

**Execution Time = 641.317955 (s)**

**What Happened? Unauthorized Access!**

**Fingerprint Experiment 4 (Feature Extractor = CNN; Infected SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

**Insider Attack: Manipulation of 50% of the Training Labels**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 0.9961 | 0.0039 |
| Fake Fingerprint | 0.0352/0.0508 | 0.9648/0.9492 |

**Execution Time = 676.267665 (s)**

**What Happened? Unauthorized Access!**

**Fingerprint Experiment 5 (Feature Extractor = CNN; Point of Attack: Communication Channel; SVM = Classifier) Confusion Matrix**

**CNN Layer to Extract Features = Fully Connected 7**

**Attack:**

1. **Positively rectify the outputs of a number of neurons during the verification phase.**
2. **Forcing the outputs of a number of neurons to zero value (power gating neurons!) during the verification phase.**
3. **Negatively rectify the outputs of a number of neurons during the verification phase.**

|  |  |  |
| --- | --- | --- |
|  | True Fingerprint | Fake Fingerprint |
| True Fingerprint | 1.0000/0.9883 | 0/0.0117 |
| Fake Fingerprint | 0.0391/0.0273 | 0.9609/0.9727 |

**Execution Time = 637.720319 (s)**

**What Happened? Unauthorized Access and Denial of Service!**