Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Компьютерных сетей и систем

Кафедра Информатики

ЛАБОРАТОРНАЯ РАБОТА №11
«Реализация криптографических атак с помощью машинного обучения на физически неклонируемые функции»

БГУИР 1-40 81 04

Магистрант:
гр. 858642
Кукареко А.В.

Проверил:
Стержанов М. В.

Минск, 2019

ХОД РАБОТЫ

Задание.

Физически неклонируемые функции (ФНФ) часто используются в качестве криптографических примитивов при реализации протоколов аутентификации.

В данном случае устройство А, содержащее реализацию ФНФ, может быть аутентифицировано с помощью набора запросов (challenge) и проверки ответов на них (response). При этом использованные пары запрос-ответ удаляются из базы данных устройства.

1. Изучите классическую работу У. Рурмаира о криптографических атаках с помощью машинного обучения на ФНФ. U. Ruhrmair et al., “Modeling attacks on physical unclonable functions,” in Proc. ACM Conf. on Comp. and Comm. Secur. (CCS’10), Oct. 2010, pp. 237–249. https://eprint.iacr.org/2010/251.pdf
2. Сформулируйте задачу в терминах машинного обучения.
3. Обучите модель, которая могла бы предсказывать ответы по запросам, которых нет в обучающей выборке.
4. Применить как минимум 3 различных алгоритма (например, метод опорных векторов, логистическая регрессия и градиентный бустинг).
5. Какая метрика наиболее подходит для оценки качества алгоритма?
6. Какой наибольшей доли правильных ответов (Accuracy) удалось достичь?
7. Какой размер обучающей выборки необходим, чтобы достигнуть доли правильных ответов минимум 0.95?
8. Как зависит доля правильных ответов от N?
9. Ответы на вопросы представьте в виде графиков.
10. Развернутые ответы на вопросы оформите в виде отчета.

Результат выполнения:

2. Сформулируйте задачу в терминах машинного обучения.

Задача предсказания ответов ФНФ основываясь на запросах относится к классу задач классификации. Каждый бит запроса может быть рассмотрен, как последовательность признаков. Количество признаков равно длине запроса N. Классами в данной задаче являются значения ответов {0, 1}. Следовательно задача является задачей бинарной классификации.

3. Обучите модель, которая могла бы предсказывать ответы по запросам, которых нет в обучающей выборке.

```
X_16b_train, X_16b_test, y_16b_train, y_16b_test = train_test_split(X_16b_der, y_16b)

lr_model = LogisticRegression()
lr_model.fit(X_16b_train, y_16b_train)
y_16b_test_pred = lr_model.predict(X_16b_test)

print(f'Accuracy: {accuracy_score(y_16b_test, y_16b_test_pred)}')
print(f'f1: {f1_score(y_16b_test, y_16b_test_pred)}')
```

```
Accuracy: 0.9933333333333333
f1: 0.9935350400827515
```

4. Применить как минимум 3 различных алгоритма (например, метод опорных векторов, логистическая регрессия и градиентный бустинг).

```
lr_model = LogisticRegression()
svm_model = SVC()
gb_tree_model = GradientBoostingClassifier()

lr_model.fit(X_train, y_train)
svm_model.fit(X_train, y_train)
gb_tree_model.fit(X_train, y_train)
```

5. Какая метрика наиболее подходит для оценки качества алгоритма?

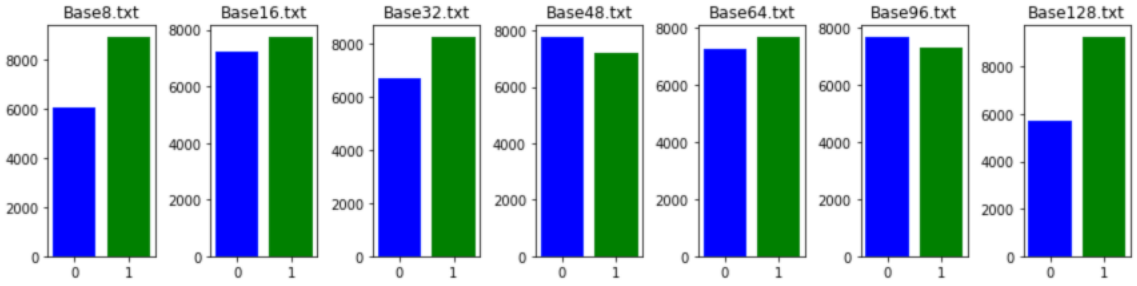

Рисунок 1 – баланс классов в разных файлах.

Как видно из рисунка 1, не все файлы содержат сбалансированные датасеты. Например в файлах Base8 и Base128 видно, что классов «0» содержится почти на треть меньше чем классов 1. Лучше метрикой для оценки моделей была бы “f1-score”. В датасетах с примерно равным распределением классов можно использовать «accuracy».

6. Какой наибольшей доли правильных ответов (Accuracy) удалось достичь?.

Доля правильных ответов варьируется от сложности «challenge», например если challenge составляет N=8, то все алгоритмы показали accuracy = 0.99 (99%), в тоже время при N=128 «логистическая регрессия» достигла точности accuracy = 0.975 (97.5%), а «градиентный бустинг» только accuracy = 0.8 (80%).

7. Какой размер обучающей выборки необходим, чтобы достигнуть доли правильных ответов минимум 0.95?

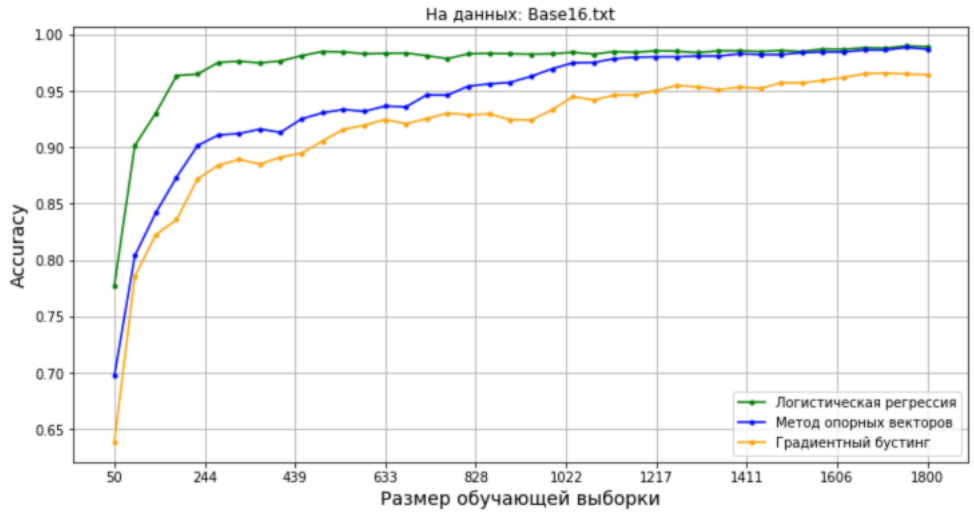

Рисунок 2 – зависимость точности от размера обучающей выборки при N=16.

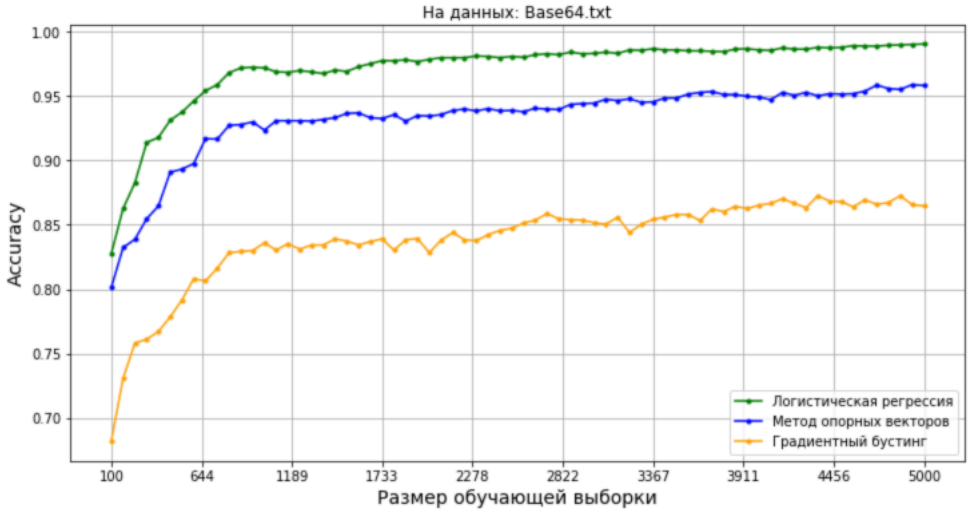

Рисунок 3 – зависимость точности от размера обучающей выборки при N=64.

Если посмотреть на рисунки 2 и 3, то можно составить данные в таблицу.

Таблица 1 – Размер выборок необходимые для достижения точности 95%

Алгоритм	N	Размер m
Логистическая регрессия	16	~ 200
	64	~ 650
Метод опорных векторов	16	~ 830
	64	~ 4500
Градиентный бустинг	16	~ 1200
	64	точность не достигнута

Если посмотреть на таблицу 1, то можно сделать вывод, что наилучшим алгоритмом для решения данной задачи среди 3х представленных является «логистическая регрессия», ей нужно меньше данных для достижения заданной точности.

8. Как зависит доля правильных ответов от N?

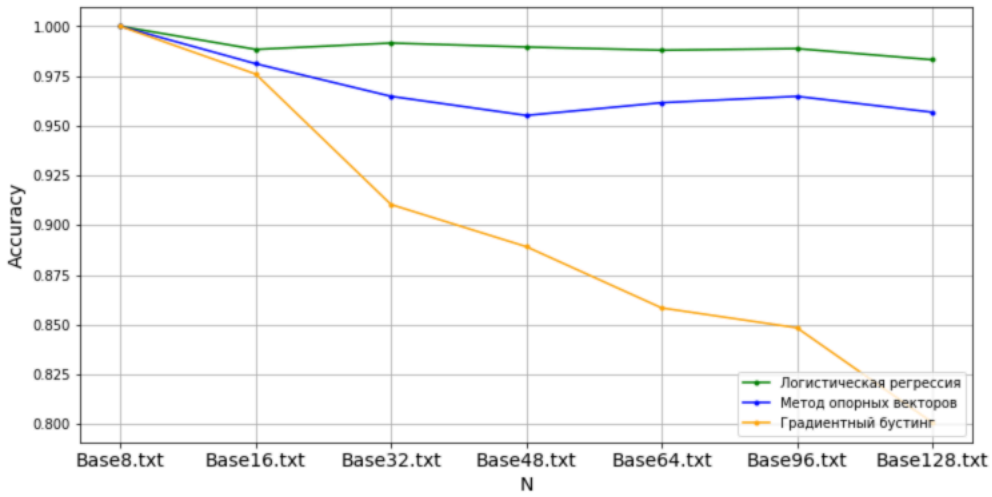

Рисунок 4 – зависимость точности от размера challenge N.

По рисунку 4 видно, что с возрастанием N, точность алгоритмов снижается. Можно заметить, что алгоритм «градиентный бустинг» уже не дает точность 95% при увеличении N. При этом «логистическая регрессия» очередной раз себя зарекомендовала, показав лишь незначительное падение точности при увеличении N.

Вывод.

В ходе выполнения лабораторной работы я ознакомился с концепцией «физически неклонируемые функций» (ФНФ), а так же ознакомился с методами атаки на ФНФ с помощью машинного обучения.

В результате мной были созданы модели для предсказания ответов ФНФ по запросам с помощью следующих алгоритмов: логистическая регрессия, метод опорных векторов, градиентный бустинг. Логистическая регрессия показала наилучшую эффективность как в точности предсказания, так и в скорости работы.