МЕСЕЦ НА НАУКАТА 2022

ФИТА

ИЗСЛЕДВАНЕ НА МЕТОДИ ЗА МАШИННО ОБУЧЕНИЕ ЗА КРИПТИРАНЕ НА ДАННИ

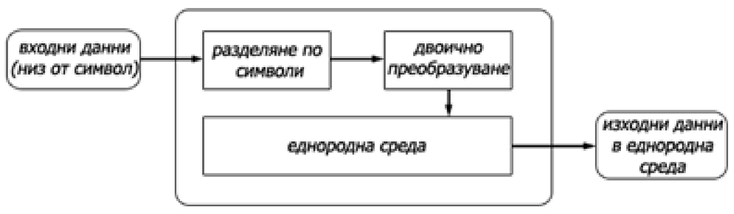
Ръководител на проекта доц. д-р Милена Карова, катедра КНТ
д-р инж. Димитър Георгиев Тодоров, катедра КНТ

Въведение

Основно предимство при асиметричното криптиране се явява бързината на шифриране и дешифриране. Недостатък обаче е необходимостта от споделяне на ключа между подател и получател, което води след себе си осигуряване начин за предаване, а в последствие и съхранението му. Основното решение на този проблем е хибридните системи, които комбинират двата вида криптиране – синхронно и асинхронно. Това разбира се е свързано с усложняване на всяка една система с внедрено хибридно криптиране. Конкретно усилията на колектива бяха насочени към:

- проучване на съществуващите методи и алгоритми за машинно обучение за извличане на знания и анализ на масиви от данни;
- анализиране и подбор на подходящ по тип, вид и обща големина обучаващи данни;
- проектиране и разработка на софтуерен модел (приложение), което да се използва за провеждане на експериментални проучвания, както за целите на дисертацията, така и за бъдещи потребности в учебните процеси.

Фиг. 1 Взаимодействие между алгоритмите



Фиг. 2 Общ вид на алгоритъма за поставяне на данни в еднородна среда

Заключение

Създаването на методика за предварителната обработка на криптографски данни посредством предложения алгоритъм за поставянето им в еднородна среда, ще даде възможност за постигането на модел на многопрофилно криптиране или криптиране с различни алгоритми в единна среда и на модел на криптографска комуникация от типа „подател - получател“ без предварителна уговорка за използвания криптографски ключ.

Разработения алгоритъм дава възможност за динамично представяне на данните от гледна точка на използваните алгоритми и техните изисквания.

Резултати

Разгледани са следните алгоритми от контролираното машинно обучение – kNN, SVM, Linear Regression, Naive Bayes, Decision Tree. Разгледани са различни синхронни криптографски алгоритми, като AES, DES, TripleDES, RC2, IDEA, CAST, Blowfish и ГОСТ 28147-89.

Предварителната обработка на данните е ключов момент и най-важен за постигане на целта на разработката и решаването на поставените задачи. Този етап се реализира от предложения алгоритъм за поставяне на данните в еднородна среда (Фиг. 2). Чрез него се постига търсената универсалност по отношение на възприятията на алгоритмите от машинно обучение и еднаквост по отношение на критериите към начина на изразяване на данните.

При изпълнение на заложените по проекта научноизследователски задачи бяха създадени ресурси в т.ч. бази от тренировъчни данни за алгоритмите от машинно обучение, софтуерна изследователска платформа, с чиято помощ са проведени експерименталните постановки. Постигнати са следните научни резултати:

-доказана е възможността от използването на алгоритми от машинно обучение за увеличаване на устойчивостта на синхронните криптографски алгоритми;
-избрани и определени са типа на данните, които се използват;
-избран е вида на съхранение на базовите данни;
-дадено е определение за еднородна среда;
-предложен е алгоритъм с методология за представяне на данни в подходящ вид и размер за работата на алгоритмите на машинно обучение.

Таблица 3: Резултатите за kNN

Algorithm	Key size	Correctly recognized	Incorrectly recognized	%	Load known keys, ms	Recognition, s
AES	256	82	28	75	5	0,198
DES	64	110	0	100	5	0,199
TripleDES	128	53	57	48	5	0,217
RC2	128	51	59	47	5	0,218
					Total time, min	
Total (average)		296	144	67	10,120	

Таблица 4: Резултатите за SVM

Algorithm	Key size	Correctly recognized	Incorrectly recognized	%	Load known keys, ms	Recognition, s
AES	256	110	0	100	5	6,831
DES	64	110	0	100	5	6,902
TripleDES	128	50	60	46	5	7,729
RC2	128	47	63	43	5	6,911
					Total time, min	
Total (average)		317	123	72	40,56	

Публикации по проекта

1. Todorov D., Karova M., Machine Secret Key Recognition in a Homogeneous Environment, International Conference Automatics and Informatics’2021, Varna, Bulgaria, 30 Sept.-2 Oct. 2021, ISBN: 978-1-6654-2661-9;
2. Todorov D., Karova M. , Appropriate Conversion of Machine Learning Data, Annual Journal TU-Varna, 2021.

Благодарности

Финансирането е от бюджетната субсидия за наука на Технически университет-Варна за 2021г.