

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Южно-Уральский государственный университет (национальный исследовательский университет)»
Высшая школа электроники и компьютерных наук
Кафедра системного программирования

Разработка веб-приложения для бинарной классификации вредоносных команд по метрике MITRE с использованием алгоритмов машинного обучения

Научный руководитель:
ст. преподаватель кафедры СП
К.Ю. Никольская

Автор:
студент группы КЭ-403
М.Д. Григорьев

Челябинск, 2024 г.

ЦЕЛЬ И ЗАДАЧИ ИССЛЕДОВАНИЯ

Цель: разработать веб-приложение для бинарной классификации вредоносных команд по метрике MITRE с использованием алгоритмов машинного обучения

Задачи:

1. Провести обзор научной литературы
2. Подготовить обучающий набор данных
3. Реализовать выбранные методы машинного обучения
4. Разработать веб-приложение для классификации вредоносных команд по метрике MITRE
5. Провести тестирование разработанного веб-приложения

MITRE ATT&CK

MITRE | ATT&CK[®] Matrices Tactics Techniques Data Sources Mitigations Groups Software Campaigns Resources Blog Contribute Search Q

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	9 techniques	14 techniques	19 techniques	13 techniques	42 techniques	17 techniques	31 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (3)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (3)	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	Build Image on Host	Credentials from Password Stores (5)	Browser Information Discovery	Exploitation for Credentials Access	Exploitation of Remote Services	Exploitation of Remote Services	Data Encrypted for Impact	
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication						
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Deobfuscate/Decode Files or Information	Forge Web Credentials						
Phishing for Information (3)	Establish Accounts (3)	Obtain Capabilities (6)	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deploy Container	Input Capture (4)						
Search Closed Sources (2)	Stage Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Event Triggered Execution (16)	Direct Volume Access	Modify Authentication Process (3)						
Search Open Technical Databases (5)	Trusted Relationship	Valid Accounts (4)	Scheduled Task/Job (5)	Create or Modify System Process (4)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Fac Authentication Intercept						
Search Open Websites/Domains (3)	Shared Modules	Software Deployment Tools	Serverless Execution	Event Triggered Execution (16)	Exploitation for Privilege Escalation	Escape to Host	Multi-Fac Authentication Request Generation						
Search Victim-Owned Websites	System Services (2)	User Execution (3)	External Remote Services	External Remote Services	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Network Sniffing						
	Windows Management Instrumentation	Implant Internal Image	Hijack Execution Flow (12)	Process Injection (12)	Scheduled Task/Job (5)	Scheduled Task/Job (5)	OS Credential Dumping						
	Modify Authentication Process (8)	Office Application Startup (6)	Pre-OS Boot (1)	Pre-OS Boot (1)	Pre-OS Boot (1)	Pre-OS Boot (1)	Steal Application Access Tokens						
							Steal or Forge Authentication Certificates						
							Modify Cloud Compute						

MITRE | ATT&CK[®] Matrices Tactics Techniques Defenses CTI Resources Benefactors

Home > Tactics > Enterprise > Defense Evasion

TACTICS

- Enterprise ▾
 - Reconnaissance
 - Resource Development
 - Initial Access
 - Execution
 - Persistence
 - Privilege Escalation
 - Defense Evasion**
 - Credential Access
 - Discovery
 - Lateral Movement
 - Collection
 - Command and Control
 - Exfiltration
 - Impact
 - Mobile ▾
 - ICS ▾

Defense Evasion

The adversary is trying to avoid being detected.

Defense Evasion consists of techniques that adversaries use to avoid detection throughout their compromise. Techniques used for defense evasion include uninstalling/disabling security software or obfuscating/encrypting data and scripts. Adversaries also leverage and abuse trusted processes to hide and masquerade their malware. Other tactics' techniques are cross-listed here when those techniques include the added benefit of subverting defenses.

ID: TA0005
Created: 17 October 2018
Last Modified: 19 July 2019

[Version Permalink](#)

Techniques: 43

ID	Name	Description
T1548	Abuse Elevation Control Mechanism	Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.
.001	Setuid and Setgid	An adversary may abuse configurations where an application has the setuid or setgid bits set in order to get code running in a different (and possibly more privileged) user's context. On Linux or macOS, when the setuid or setgid bits are set for an application binary, the application will run with the privileges of the owning user or group respectively. Normally an application is run in the current user's context, regardless of which user or group owns the application. However, there are instances where programs need to be executed in an elevated context to function properly, but the user running them may not have the specific required privileges.
.002	Bypass User Account Control	Adversaries may bypass UAC mechanisms to elevate process privileges on system. Windows User Account Control (UAC) allows a program to elevate its privileges (tracked as integrity levels ranging from low to high) to perform a task under administrator-level permissions, possibly by prompting the user for confirmation. The impact to the user ranges from denying the operation under high enforcement to allowing the user to perform the action if they are in the local administrators group and click through the prompt or allowing them to enter an administrator password to complete the action.

ДИАГРАММА ВАРИАНТОВ ИСПОЛЬЗОВАНИЯ

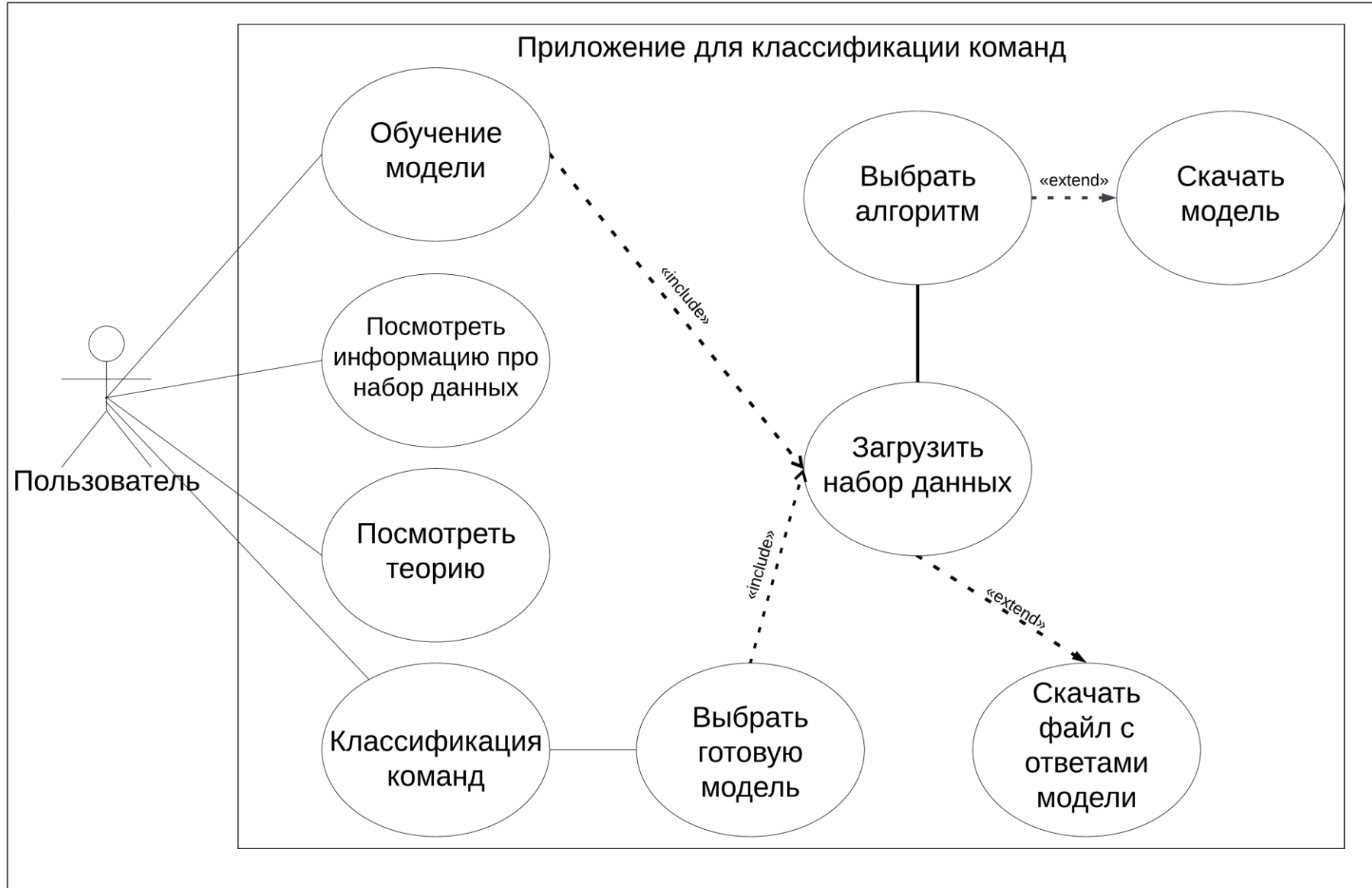
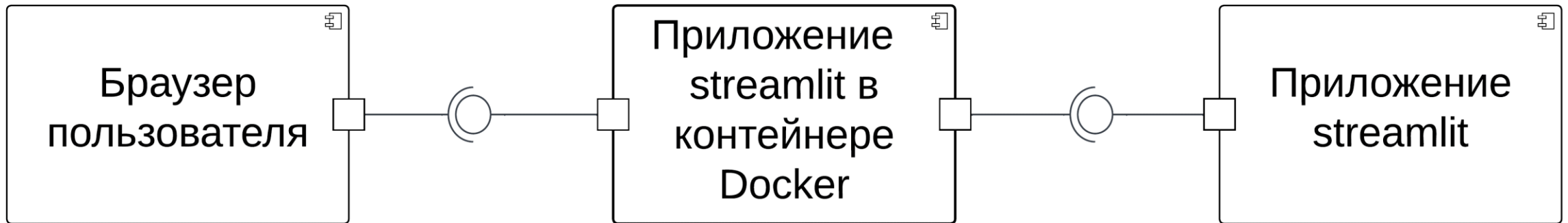


ДИАГРАММА КОМПОНЕНТОВ



СРЕДСТВА РАЗРАБОТКИ

- **Язык программирования:** Python 3.10.6
- **Редактор исходного кода:** VSCode 1.78.2
- **Среда разработки модели машинного обучения:** Jupyter Notebook
- **Библиотеки:** scikit-learn 1.2.2, pandas 1.5.0, NumPy 1.21.6, matplotlib 3.7.1, streamlit 1.35.0

НАБОР ДАННЫХ

- Количество классов команд: 2
- Общее количество записей: 1 742
- Количество видов команд: 14 (Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, Impact, Safe)

Вид команды	Команды MITRE
Execution	<code>\$assembly = [Ref].Assembly.GetType('{0}{1}i{2}' -f \$a,\$b,\$u)</code>
Command and Control	<code>\$field.SetValue(\$null,\$true)</code>
Discovery	<code>\$ping = New-Object System.Net.Networkinformation.Ping</code>
Privilege Escalation	<code>\$computer = "<hostname>"</code>
Credential Access	<code>\$cred = New-Object System.management.Automation.PSCredential(\$user, \$pass)</code>

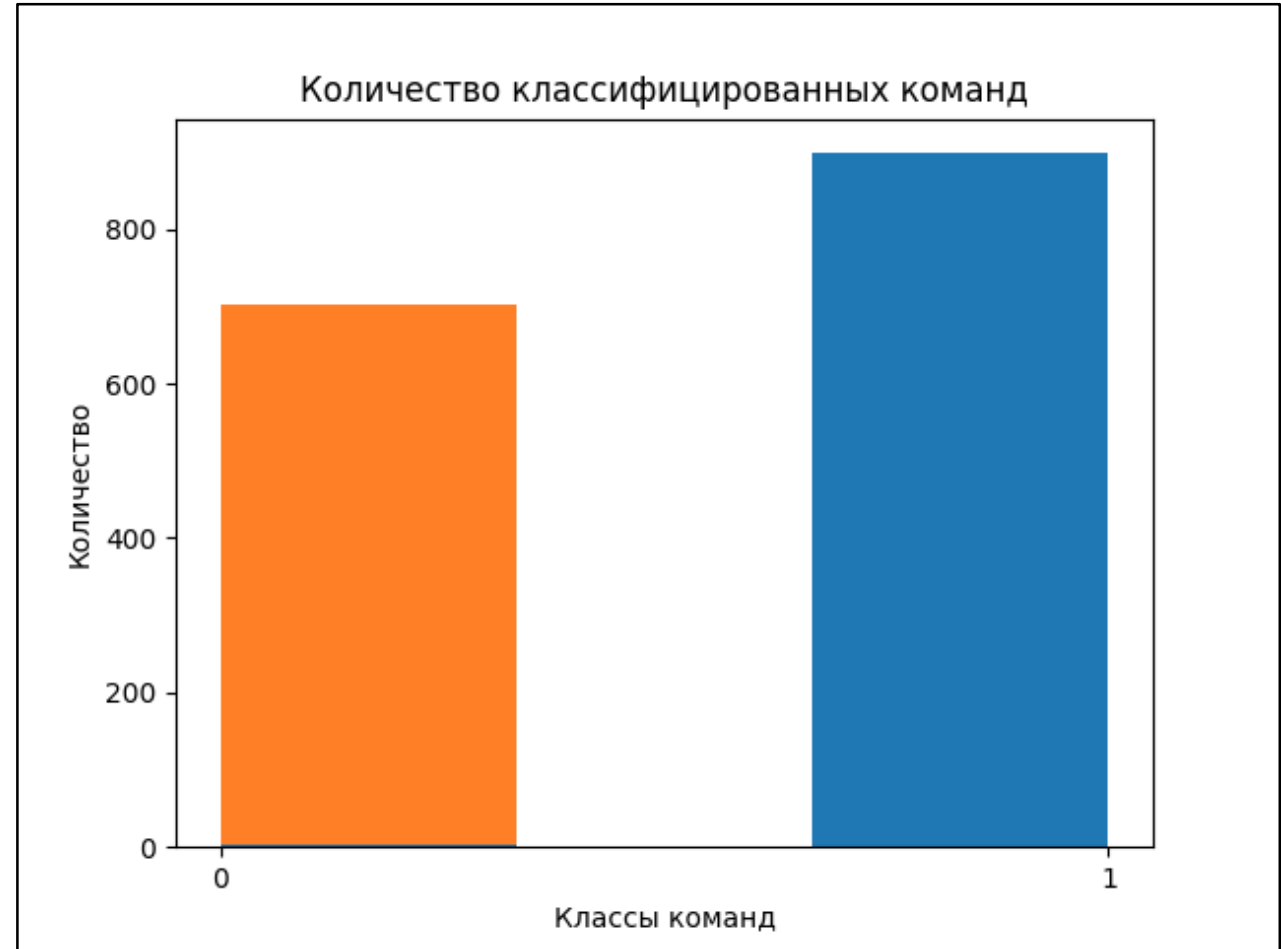
ПРЕДОБРАБОТКА

1. Разметка набора данных

2. Чистка данных

Итого:

- Количество записей: 1 600



АЛГОРИТМЫ МАШИННОГО ОБУЧЕНИЯ

1. Наивный Байес (Naïve Bayes)
2. Логистическая Регрессия (Logistic Regression)
3. Дерево Решений (Decision Tree)
4. Случайный Лес (Random Forest)
5. Бустинг (Boosting)
6. Метод опорных векторов (Support Vector Machines)
7. К-ближайших соседей (K-Nearest Neighbors)

ОБУЧЕНИЕ МОДЕЛЕЙ

- Для обучения было использовано 80% от всей выборки (1 280 записей из 1 600)
- Для тестирования было использовано 20% от всей выборки (320 записей из 1600)
- Обучение производилось с помощью локальных возможностей (CPU: AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx @ 1.40GHz 2.10 GHz)

ГЛАВНАЯ СТРАНИЦА

✕Deploy ⋮

Главная

Обучение

Классификация

Набор данных

Теория

Приложение для классификации команд

Это приложение для обучения моделей машинного обучения для классификации команд

Как использовать приложение:

- Чтобы обучить модель - перейдите в раздел [Обучение](#)
- Чтобы использовать обученные модели - перейдите в раздел [Классификация](#)
- Чтобы узнать про используемый для обучения датасет - перейдите в раздел [Датасет](#)
- Чтобы узнать про используемые алгоритмы - перейдите в раздел [Теория](#)

СТРАНИЦА ОБУЧЕНИЕ

×⋮

Главная

Обучение


Классификация


Набор данных

Теория

Обучение модели

Загрузите датасет

 Drag and drop file here
Limit 200MB per file • CSV

 POWERSHELL.csv 152.6KB ×

Загружен датасет: POWERSHELL.csv

Выберите алгоритм:

SVC ▾

Введите C:

1.0 - +

Введите kernel:

linear

Введите gamma:

СТРАНИЦА КЛАССИФИКАЦИЯ

×🌊 RUNNING... Stop ⋮

Главная

Обучение


Классификация


Набор данных

Теория

Классификация


Выберите модель


 Drag and drop file here
Limit 200MB per file • SAV Browse files

 SVC(kernel='linear').sav 102.6KB ×

Выбран файл: SVC(kernel='linear').sav

Загрузите датасет

 Drag and drop file here
Limit 200MB per file • CSV Browse files

 POWERSHELL.csv 152.6KB ×

Загружен датасет: POWERSHELL.csv

СТРАНИЦА ТЕОРИЯ

×Deploy ⋮

Главная

Обучение

Классификация

Набор данных

Теория

Наивный Байесовский Классификатор ^

Классификатор, основанный на теореме Томаса Байеса. Является главным методом для понимания вероятности некоторого события $P(A|B)$ при наличии некой новой информации, $P(B|A)$ и априорной субъективной оценки вероятности события $P(A)$

$$P(A|B) = \frac{P(B|A) * P(A)}{P(B)}$$

Наивные байесовы классификаторы объединяют в общий классификатор ряд желательных в практическом машинном самообучении качеств. К ним относятся:

1. интуитивно понятный подход;
2. возможность работы с малыми данными;
3. низкие затраты на тренировку и предсказание;
4. часто надежные результаты в разнообразных условиях.

Логистическая Регрессия ▼

Дерево Принятия Решений ▼

Метод Опорных Векторов ▼

АКТ О ВНЕДРЕНИИ


АКТ о внедрении научно-технической продукции

Данный акт удостоверяет, что в ООО «Р-Вижн» внедрен в опытную эксплуатацию приложение для бинарной классификации вредоносных команд по метрике MITRE с использованием алгоритмов машинного обучения, разработанный студентом группы КЭ-303 Григорьевым Максимом Дмитриевичем, научный руководитель – старший преподаватель кафедры системного программирования ФГАОУ ВО «ЮУрГУ (НИУ)» Никольская Ксения Юрьевна.

Приложение для бинарной классификации вредоносных команд по метрике MITRE с использованием алгоритмов машинного обучения используется в коммерческих целях.

Акт подписал

Генеральный директор

 Бондаренко А.В.

31.05.2023 г.



ОСНОВНЫЕ РЕЗУЛЬТАТЫ

1. Проведен обзор научной литературы
2. Подготовлен обучающий набор данных
3. Реализованы выбранные методы машинного обучения
4. Разработано веб-приложение для классификации вредоносных команд по метрике MITRE
5. Проведено тестирование разработанного веб-приложения

АНАЛИЗ ЛИТЕРАТУРЫ

Название	Авторы	Набор данных	Алгоритм	Точность
Data Mining Applied to Intrusion Detection: MITRE Experiences	Bloedorn, E. E., Talbot, L. M., & DeBarr, D. D. (n.d.)	Собран вручную	Random Forest	91%
Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix	Wenjun Xiong, Emeline Legrand, Oscar Åberg, Robert Lagerström	база знаний MITRE ATT&CK	Decision Tree	97%
A Machine Learning Approach to Dataset Imputation for Software Vulnerabilities	Shahin Rostami, Agnieszka Kleszcz, Daniel Dimanov, Vasilios Katos	ENISA	Logistic Regression	99,88%
A Novel Enhanced Naïve Bayes Posterior Probability (ENBPP) Using Machine Learning: Cyber Threat Analysis	Ayan Sentuna, Abeer Alsadoon, P. W. C. Prasad, Maha Saadeh, Omar Hisham Alsadoon	Собран вручную	Naïve Bayes	92-96%

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ СТРАНИЦЫ КЛАССИФИКАЦИЯ

Название теста	Шаги	Ожидаемый результат	Тест пройден?
Загрузка готовой модели машинного обучения.	<ol style="list-style-type: none">1. Нажать на кнопку «Загрузить файл».2. Выбрать файл.	Программа должна вывести на экран название файла.	Да
Загрузка набора данных	<ol style="list-style-type: none">1. Нажать на кнопку «загрузить файл».2. Выбрать файл в формате .csv.	Программа должна вывести название файла.	Да
Вывод результата классификации модели.	<ol style="list-style-type: none">1. После загрузки набора данных автоматически запустится классификация команд.	Результат классификации будет выведен в виде таблицы, где правильные ответы выделены зеленым а неправильные – красным.	Да
Скачать результат классификации.	<ol style="list-style-type: none">1. Нажать на кнопку «Скачать файл».	Файл с результатами классификации в формате .csv должен появиться в загрузках браузера.	Да

ФУНКЦИОНАЛЬНОЕ ТЕСТИРОВАНИЕ СТРАНИЦЫ ОБУЧЕНИЕ

Название теста	Шаги	Ожидаемый результат	Тест пройден?
Загрузка набора данных	<ol style="list-style-type: none">1. Нажать на кнопку «загрузить файл».2. Выбрать файл в формате .csv.	Программа должна вывести название файла.	Да
Выбор алгоритма и гиперпараметров модели	<ol style="list-style-type: none">1. Выбрать алгоритм из списка.2. Настроить значения гиперпараметров.	Значения гиперпараметров должны примениться к модели.	Да
Начать обучение модели	<ol style="list-style-type: none">1. Нажать на кнопку «начать обучение».	Программа должна вывести на экран слово «Готово!» и точность получившейся модели.	Да
Скачать получившуюся модели	<ol style="list-style-type: none">1. Нажать на кнопку «Скачать модель».	Файл скаченной модели должен появиться в загрузках браузера.	Да

A/B ТЕСТИРОВАНИЕ

Количество данных	Алгоритм	Score
300	GaussianNB	0,98
	LogisticRegression	0,97
	DecisionTreeClassifier	0,96
	RandomForestClassifier	0,96
	XGBClassifier	0,97
	SVC	0,98
	KNN	0,97
600	GaussianNB	0,96
	LogisticRegression	0,98
	DecisionTreeClassifier	0,98
	RandomForestClassifier	0,99
	XGBClassifier	0,97
	SVC	0,98
900	GaussianNB	0,98
	LogisticRegression	0,99
	DecisionTreeClassifier	0,98
	RandomForestClassifier	0,97
	XGBClassifier	0,98
	SVC	0,96
	KNN	0,97

Количество данных	Алгоритм	Score
1200	GaussianNB	0,96
	LogisticRegression	0,98
	DecisionTreeClassifier	0,98
	RandomForestClassifier	0,97
	XGBClassifier	0,98
	SVC	0,96
	KNN	0,99
1500	GaussianNB	0,98
	LogisticRegression	0,96
	DecisionTreeClassifier	0,97
	RandomForestClassifier	0,95
	XGBClassifier	0,99
	SVC	0,97
	KNN	0,97

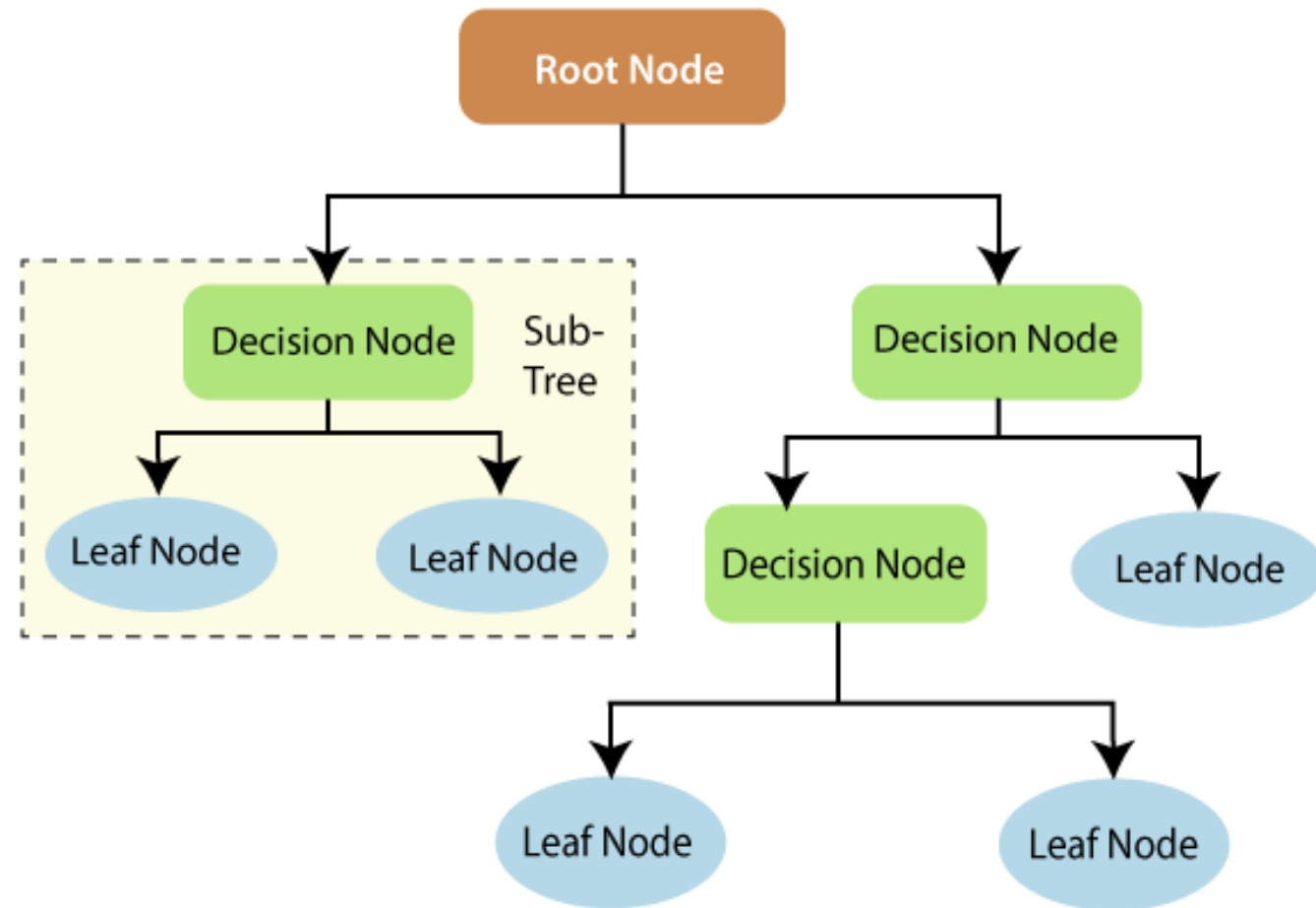
МЕТРИКИ НА ТЕСТОВЫХ ДАННЫХ

Модель	Accuracy	Recall	Precision	F1
Gaussian Naïve Bayes	0,9812500	0,9944751	0,9884393	0,9890109
Logistic Regression	0,9945234	0,9967534	0,9912876	0,9915966
Random Forest Classifier	0,9836862	0,9822995	0,9916362	0,9864222
Decision Tree Classifier	0,9687500	0,9833333	0,9719101	0,9708222
XGBoost	0,9631820	0,9787213	0,9681148	0,9723599
SVM	0,9884122	0,9886734	0,9881825	0,9812521
KNN	0,9887631	0,9812552	0,9823677	0,9887721

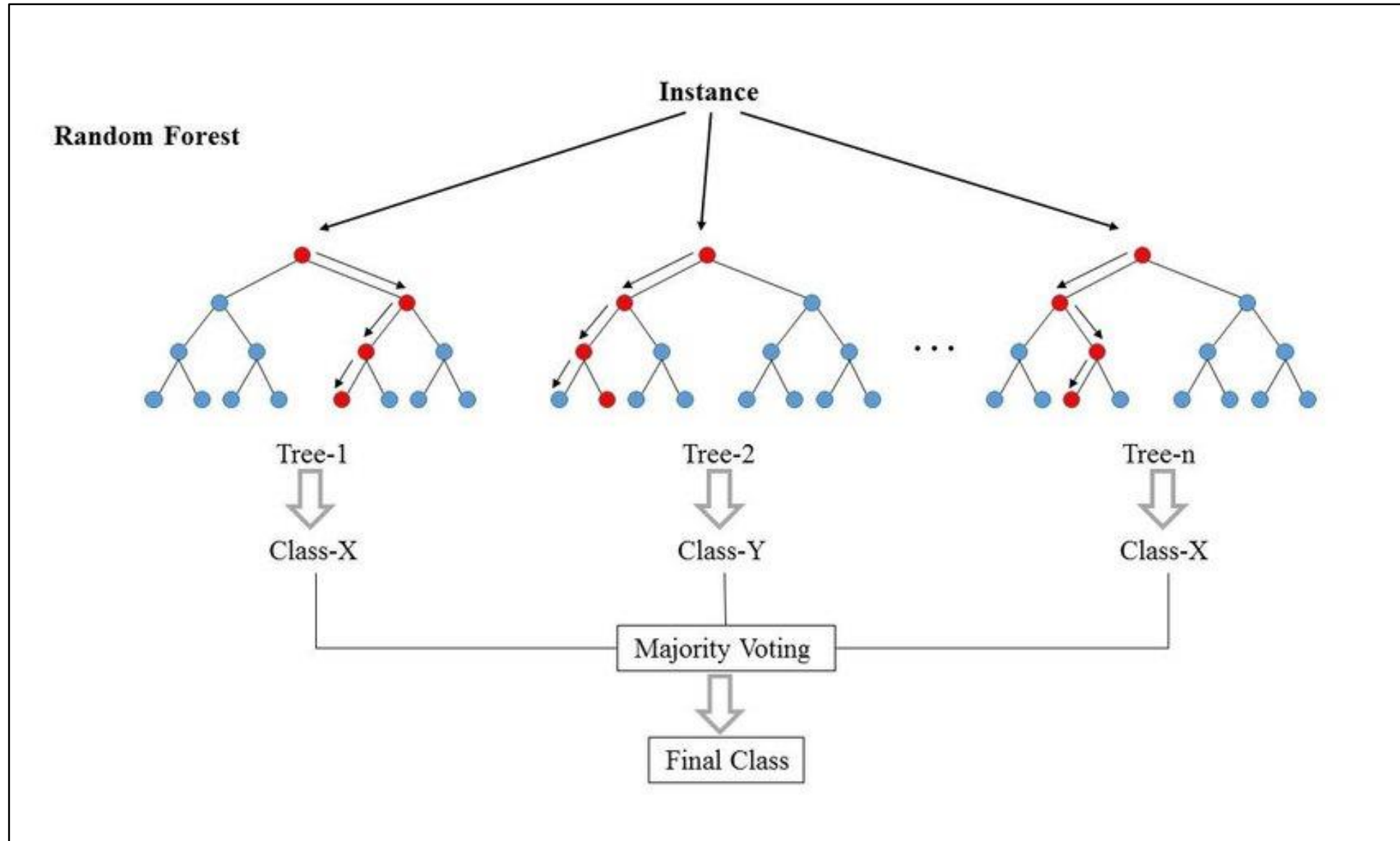
NAIVE BAYES

$$P(A | B) = \frac{P(B | A) \cdot P(A)}{P(B)}$$

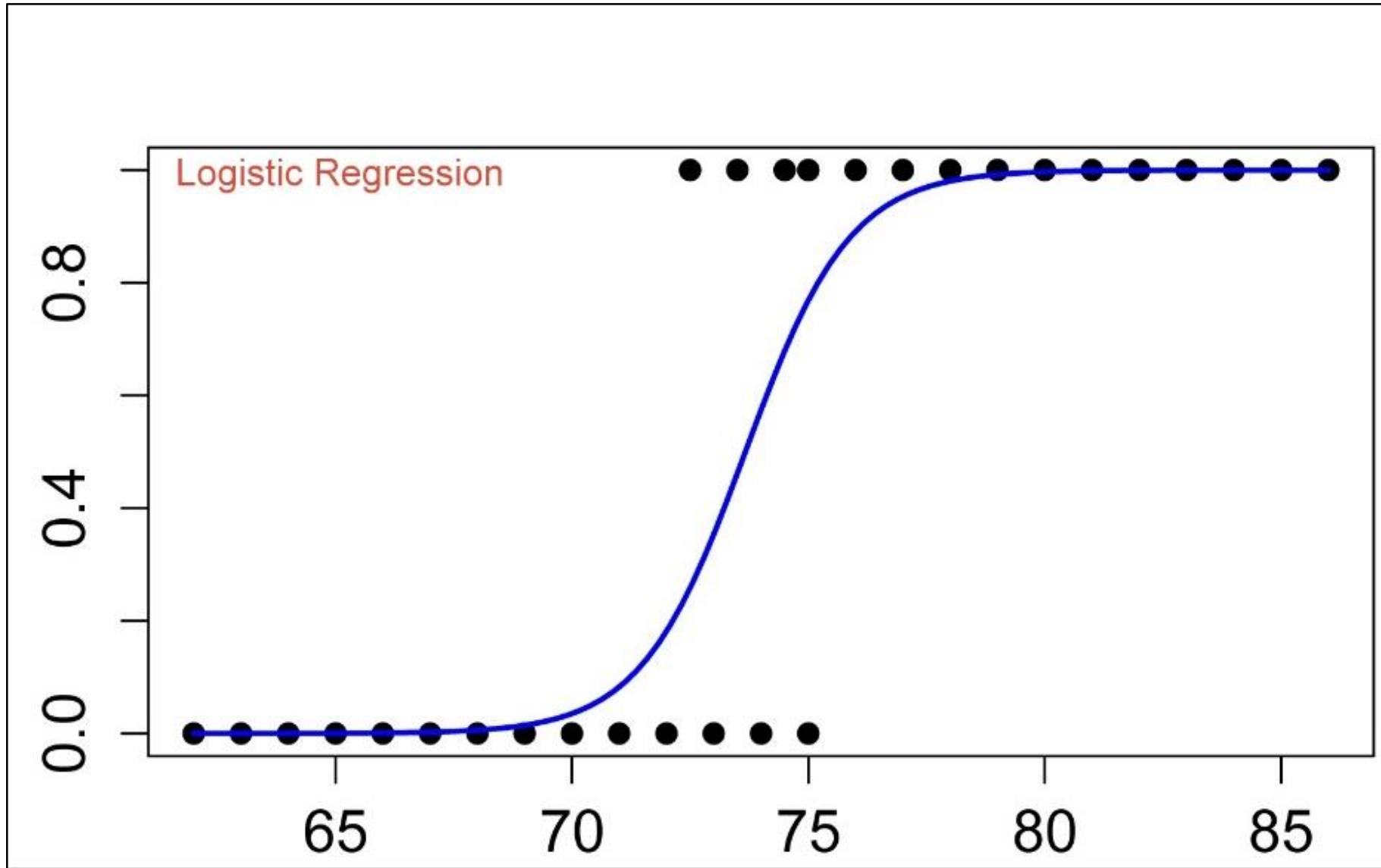
DECISION TREE



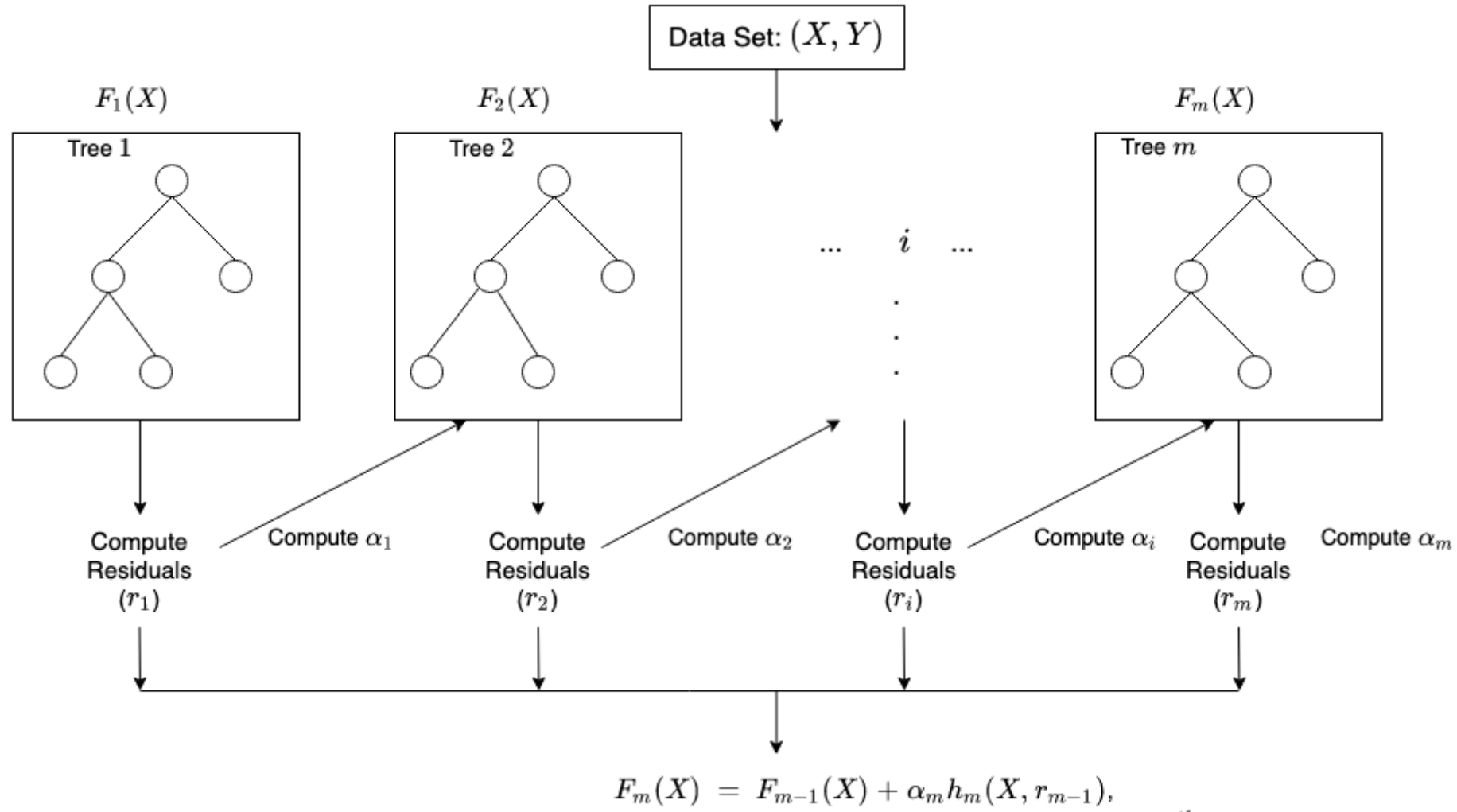
RANDOM FOREST



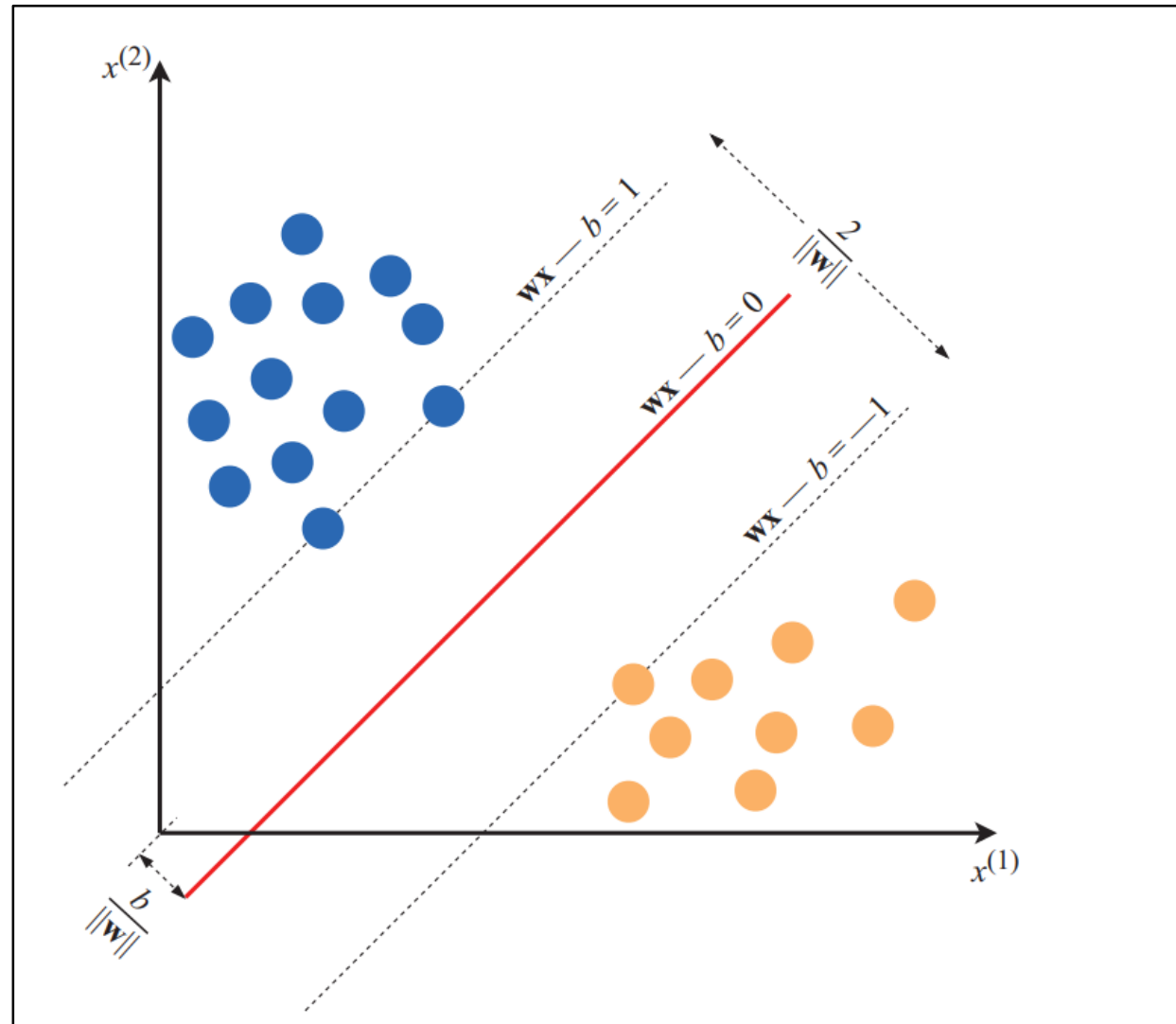
LOGISTIC REGRESSION



XGBOOST



Support Vector Machines



K-Nearest Neighbors

