**Malware Analysis Toolkit with Machine Learning Integration**

* **Data Collection and Preparation-** Gather a dataset containing malicious samples kaggle.
* **Feature Extraction-** byte sequences, opcode frequency, file metadata
* **Feature Selection-** subset of the features to improve the model's performance
* **Data Splitting**-80 Training and 20 testing sets
* **Feature Scaling**-
* **Model Selection and Training-** Find the most feasible one by developing all possible versions of ML.
* **Hyperparameter Tuning**
* **Model Evaluation**
* **Interpretation and Analysis**
* **Iterate and Refine**
* **Deployment**

**Target Audience**

* Security Software Developers
* Law Enforcement and Government Agencies
* Malware Analysts
* Penetration Testers
* Security Operations Center (SOC) Teams
* Forensic Investigators
* Reverse Engineers
* Threat Intelligence Analysts
* Ethical Hackers
* Incident Responders
* Security Researchers

1. Problem Identification

To a preliminary study on the relevant work

To Identify Research Gap

Review Existing Work

Review Existing Technology

Review Evaluation Methods

1. Literature Review(Abstract, Introduction, Conclusion) To study Existing Work

a. To identify Available Dataset

b. To identify preprocess technique

c. To identify the available technology to build, train and test the model.

d. To identify evaluation metrics available to test the model

e. ……..

Read 5 papers (Fully)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Citation | Brief Summary of the Work | Technology | Limitations | Contribution |
| Yadav, K., Sethi, A., et al. (2022).  <https://www.igiglobal.com/gateway/chapter/292228>  ‌ | The capacity to detect possible future malware by learning from existing malware patterns makes this method very popular | Machine Learning |  |  |
| Babaagba, K. O., & Adesanya, S. O. (2019). https://doi.org/10.1145/3318396.3318448 |  | Malware Analysis using Machine Learning. |  |  |
| Alhaidari, F., Shaib, N. A., Alsafi, et al. (2022)., 1–15. https://doi.org/10.1155/2022/1615528 |  | Using Machine Learning and Sandboxing Analysis Techniques. Computational Intelligence and Neuroscience |  |  |
| Samara, M ., El-Alfy, E., (2019) |  | Open-Source Android Malware  Detection Tools |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Technological Review

|  |  |  |  |
| --- | --- | --- | --- |
| Technology | Pros | Cons | Citation |
| SVM |  |  | ABC (2020) |
| KNN |  |  |  |
| Naïve Bayes |  |  |  |
| Random Forest |  |  |  |

Evaluation 🡪 Review

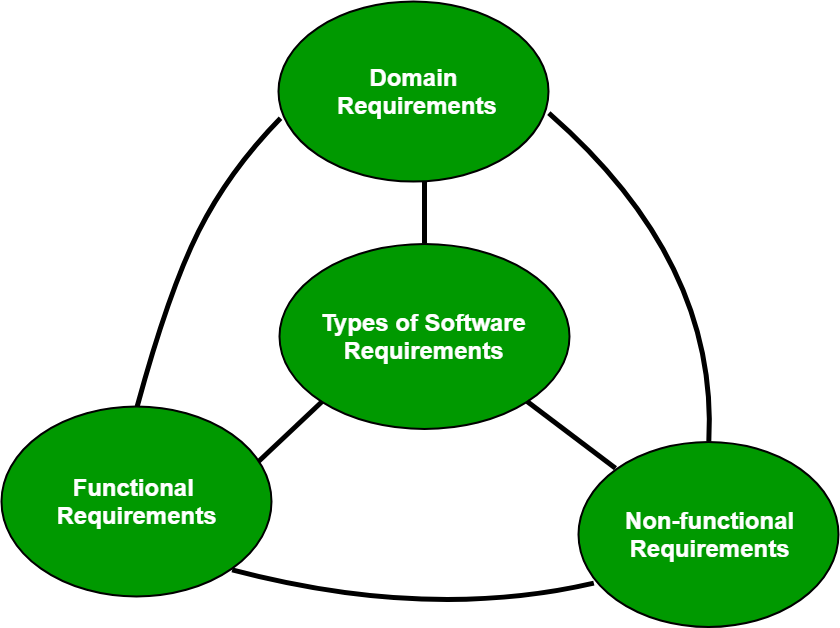
|  |  |  |  |
| --- | --- | --- | --- |
| Dataset |  |  |  |
|  |  |  |  |

1. Requirement Felicitation 🡪 SRS

a. To identify requirements elicitation methods best fits for this project.

b. To identify list function requirements.

c. To identify list of non-functional requirements.



1. Design 🡪 Design Specification

a. To design architecture diagram

b. To derive a system design using OODM

c. To design suitable UI

1. Implementation 🡪 Working Prototype

a. To identify the technology stack

b. To build the machine learning model.

c. To train and test the ML model.

1. Testing 🡪 test result

a. To conduct model testing to measure the most accurate model.

b. To conduct a prototype testing (unit testing, integration testing, system testing)

c. to carryout non-functional testing

1. Finalize the Documentation and Prototype

a. Complete the project report.

8. Methodology

a. Research Methodology- using sander’s onion model

|  |  |
| --- | --- |
| **Research Philosophy** | What and Why? |
| **Research Approach** | What and Why? |
| **Research Strategy** | What and Why |
| **Research Choice** | What and Why |
| **Time Horizon** | What and Why? |

b. Development Methodology

What is the development methodology(third person perspective) The development methodology the team will work on this project is prototyping because the requirements are not clear in the beginning and evolves over the time through literature review, brainstorming and experiments.

i. Design 🡪 OOADM // SSADM (DFD)

ii. Programming paradigm 🡪 OOP or SP or FP or …

iii. Evaluation Methodology🡪 testing MML🡪model testing 🡪 evaluation metrics // Unit, integration and system 🡪 for the prototype solution methodology 🡪 what are different ways in which you can solve the problem.

1. Existing Work

a. What algorithms they have used?

b. What algorithms that can be used.

c. Project Management Methodology

i. Scope

-In scope

a. Preprocessing

b. Feature Engineering

c. Model Building

d. Training and testing

e. Deployment

f. CLI

-Out scope

a. GUI

ii. Schedule

* Gantt Chart

WBS

> Problem Identification

\*Initial LR

\* Finalizing research gap

\* Finalizing Proposal

> Literature Review

\*LR on Exiting Work

\* LR on Technology available

> Requiremnt Elicitation

\* Deriving FR

\* Deriving NFR

> Design

\* Architecture Design

\* System Desigm

\* UI Design

> Implementation

\* Model Implementation

\* UI implementation

> Testing

\* Model Testing

\* System Testing

\* Performance Testing

> Documentation

\* Finalizing the documentation

iii. Risks and Mitigations

* Risks and mitigations 🡪 related to Social, Legal, Ethical, Professional Issues (ACS)

Scope

~~Budget (not there)~~

Time

(Schedule)

9. Resource Requirements

a. Hardware Resources

b. Software Resources

c. Human Resources

i. Who are the people in your team

- What they are good at

- What role they will play

d. Skill Requirements

e. Data Requirements

Obfuscation and packing.

1. Problem Identification

2. Literature Review(Abstract, Introduction, Conclusion)

Initial Literature Review Existing published work in IEEE, ACM 🡪 Semantic Scohlar

5 research papers (last 5 year) 🡪 Abstract 🡪 Introduction 🡪 Conclusion

From this research paper you have to read 🡪 Research Gap

3. Problem background

a. Problem

b. Significance of the problem, can even bring statistics (Should be cited)

c. Aim-one sentence (To design develop and evaluate a machine learning model to identify high risk target audiences(High Risk Students) in risk area(Academic Performance) in the field targeted(Tertiary Education))

d. Objectives(Has to SMART)

i. To identify the problem related to generating tags from the product manually is time consuming and labour-intensive task there to automate using deep learning,

ii. To conduct literature review on how currently deep learning used in generating tags from the product.

iii. To identify available options to generate tags from the product image.

To design, develop and evaluate a machine learning model to identify high risk target audiences(High Risk Students) in risk area

Background to the problem

1.1 Problem

1.2 Significance of the problem

1.3 Aims

To design develop…

Objectives

1. To identify the problem

2. To conduct literature review

1.4 Objectives are the things that we will be using in the Gant chart\

2. Proposed Methodology

2.1 Research Methodology

Research methodology for this project has been covered using Saunder’s research model. Cite –

Table in three coloumns

|  |  |  |
| --- | --- | --- |
| Research Philosophy | Positivism | Give the justification for selec |
| Research Approach |  |  |
|  | Experiment, Self evaluation, brain storm |  |
| Time Horizon |  |  |

Evaluation Methodology

Classification rOC, LOLC

hOW TO EVALUATE A CLASSIFICATION MODEL

CITE USING RESEARCH PAPER

CONFUSION MATRIX, F1 SCORE

Solution Methodology

What are the steps to build a ML model and how yoi are planning too do each of them

iii. Evaluation Methodology🡪 testing MML🡪model testing 🡪 evaluation metrics // Unit, integration and system 🡪 for the prototype solution methodology 🡪 what are different ways in which you can solve the problem.

1. Existing Work

a. What algorithms they have used?

b. What algorithms that can be used.

3.2.3 Evaluation/ testing methodology/ metrics

classification matrix – which must be included

3.2.4 Solution methodology – come up with the steps in developing the system

For each step what are the solution

What is Project Management Methodology to use

Schedule

Risk, Resources

Scope - initial set of functions and nonfunctional requirements

Resource Requirments

Deliverables and dates

Literature review -> LR document

Milestones

Template from excel for work breakdown

– first draft

Aims and the work breakdown structure goes in hand in

Course Learning Objectives

Role

Learning Outcomes

-----------------------------------------------

Objectives

Aims

Literature Review – In Progress insert a table

Include 5 works similar to your work

Research Paper

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Citation | Brief | Technology | Limitations | Contribution |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Competative products

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Products |  |  |  |  |
| Feature 01 – functions they have | X |  |  |  |
| Feature 02 |  |  |  |  |
|  |  |  |  |  |

Significance of the problem – Justification

Methodology

Research Methodology

In this project

Cite where saunders initially started and add the references

Development Methodology

Tell the methodology chosen and justify()

3.2.1 Design Methodology

3.2.2. Program Paradigm

iii. Evaluation Methodology🡪 testing MML🡪model testing 🡪 evaluation metrics // Unit, integration and system 🡪 for the prototype solution methodology 🡪 what are different ways in which you can solve the problem.

1. Existing Work

a. What algorithms they have used?

b. What algorithms that can be used.

Auc

3.2.3 Evaluation/ testing methodology/ metrics

classification matrix – which must be included

3.2.4 Solution methodology – come up with the steps in developing the system

Steps and the choices

For each step what are the solution

SCOPE – FUNCTIONAL REQUIREMENTS

1. Dataset – tell what are the datasets available

Tell that the dataset is publicly available in kegal

2. Pre- processing – data extraction, data ..

3. Model selection

4. Building the

- Spliting the data 80% 20% like so and explain

-

Out of scope – hyper parameter tuning

3.3 Project Management Methodology

- What is the methodology - Prince 2 and Agile Prince 2 -> find what is that etc

3.3.1 Schedule

3.3.1.1 Deliverables and dates – doing a particular feature, LR, experimenting and identifying the best model, preprossing - steps, training, testing

Using the moscow principle

O - nothing

# Should we ask if we should add the wireframe diagrams as an output

We’ll add it as a separate doc?

In scope

Functional requirements

Point form or table

Out scope

What we are not going to cover

Competitive Analysis Template

Schedule

Deliverables and Dates – one line of explanation

Include software functions and documentation.

Include it in a table.

3.3.2.2.2 Project Plan

3.3.2.3 Resource Management.

3.3.2.3.1 Hardware Resource.

3.3.2.3.2 Software Resource.

3.3.2.3.3 Skill Requirement.

- NEW SKILL REQUIREMNTS

3.3.2.3.4 Data Requirement.

3.3.2.4 Risk Managemnt

SOCIAL , ETHICAL, LEGAL RISKS

WHEN WE PUT IT INTO THE WORLD

LEGAL

PRIVACY RELATED RULES IN AUSSIE

HOW TO ENSURE THE PRIVACY

Access Level

Capabilities

Role

CLO’s – Course Learning Outcome

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| NAMES |  |  |  |  |  |
| ROLE |  |  |  |  |  |
| CAPABILITIIES |  |  |  |  |  |
| CLOs |  |  |  |  |  |
| Degree Program |  |  |  |  |  |

Hardware requirements

* Gpu, processing

Software Requirements

What are the programming language – why we have chosen it

Librarirs

Add the team contract.

WHERE’S MACHINE LEARNING?