# Developing a Robust Android System Towards Malicious URLs
# UQU-CS-2022-08

Afrah Alsaadi, Afnan Munshi, Jomanah Bajahlan, Nedaa Elgazzar, Lujain Batouq

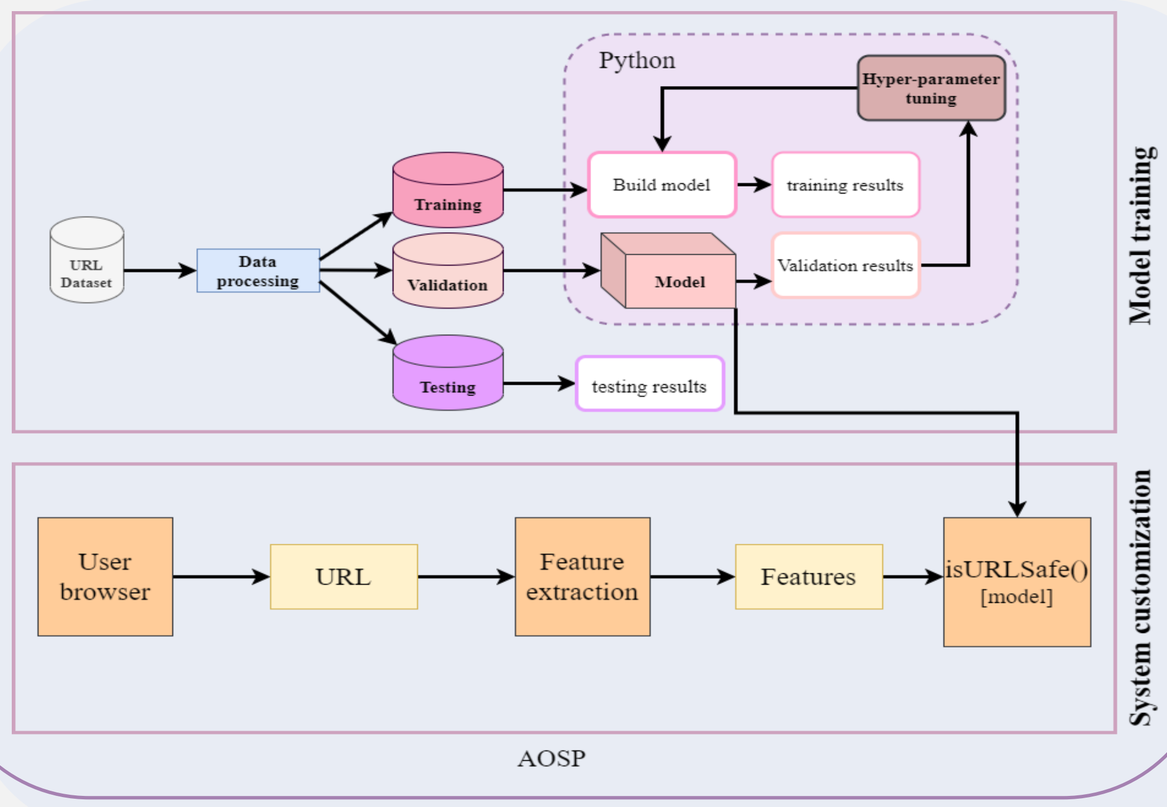
Superviser: Dr. Sarah Al-Shareef

Dept. of Computer Science, Umm Al-Qura University, KSA, 2023

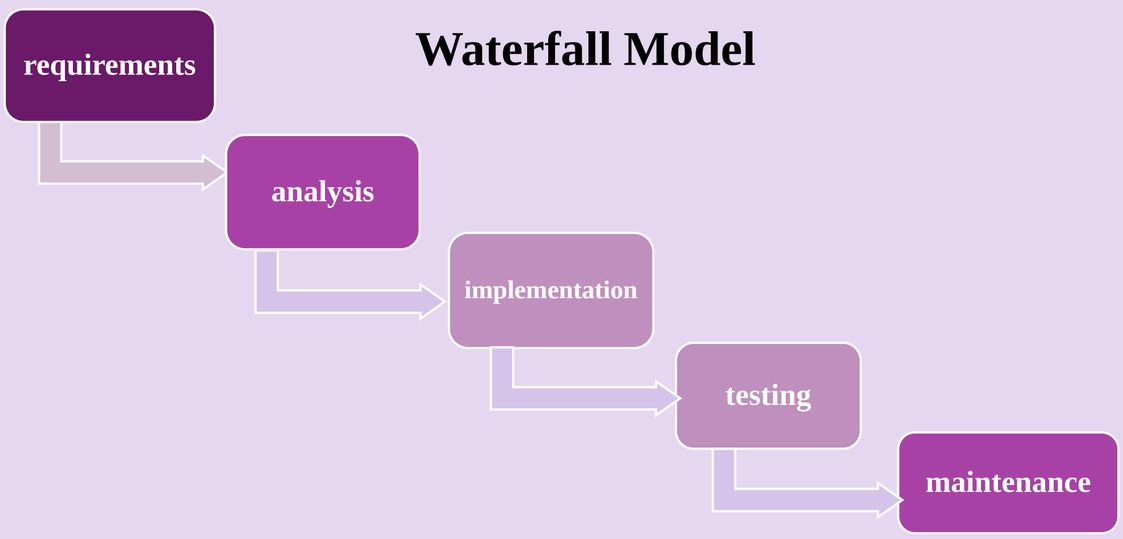
## Abstract:

Every application we use daily can get hacked in multiple ways. the common way to spread malware now is by sending malicious URLs. Hence, we propose a machine-learning-based solution to detect these URLs in the background without requiring additional steps from the user. First, we will train a machine learning (ML) model using classification algorithms to classify URLs into malicious or safe ones. we customized the Android OS to embed our malicious URL detector so all URLs in any application will be checked in the background once the user clicks on them from any installed application. The project employed an RF model with competitive performance, then the model was converted and deployed to Java. After that, a version of the Android Open-Source Project was downloaded, customized with the malicious URL detector, built, and tested on the Emulator.

## Structure




## Methodology




## Conclusion

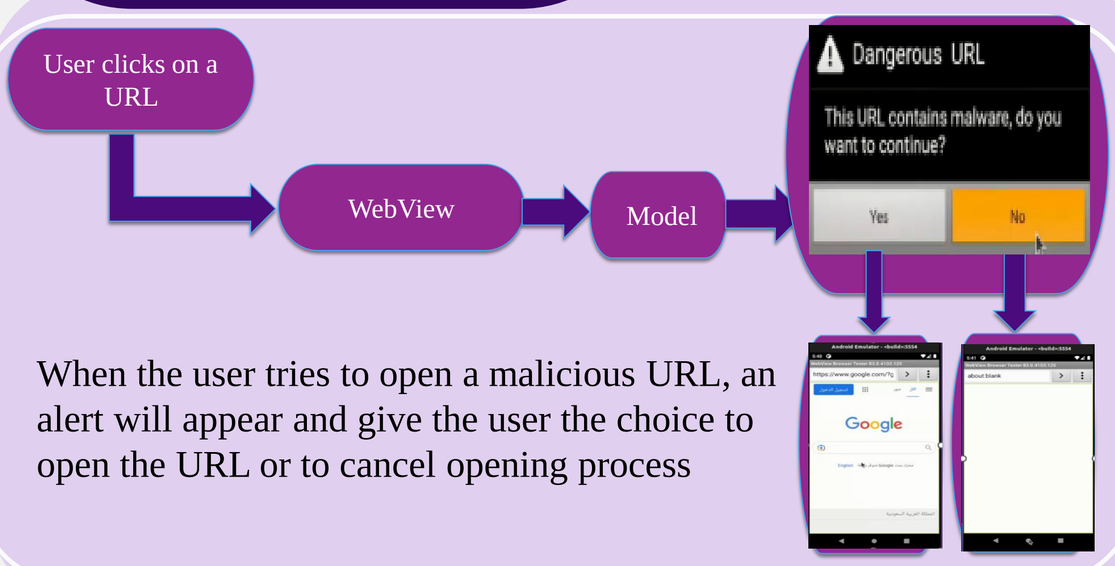
ML is used to build a model that can be trained to classify any URL as benign or malicious and modify an Android OS to embed a malicious URL detector model.

## Reference

## Aims and Objectives

Protect the users from malicious URLs by analyzing and classifying URLs. With the help of the ML model, which is trained to classify any URL as benign or malicious and it will not need frequent updating

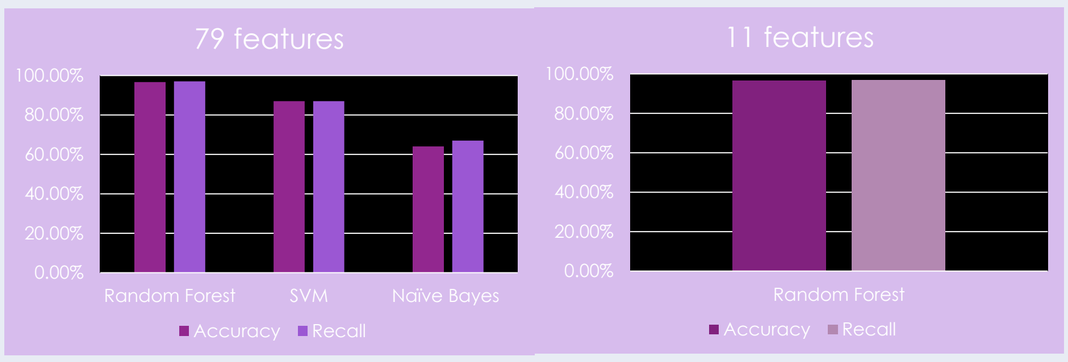
## Implementation




When the user tries to open a malicious URL, an alert will appear and give the user the choice to open the URL or to cancel opening process

## Results

| Malicious class | | | | Benign class |
|---|---|---|---|---|
| Spam | Phishing | Defacement | Malware | |
| 44k | | | | 35k |




The Random Forest classifier has the highest accuracy and recall rate among other classifiers, with 96.7% of accuracy and 97% of recall.

## Future work

- Customize a newer version of Android.
- Integrate our model into the customized Android.
- Give users information about malicious URL types.

**Contact:**
Group Email: robustos.2023@gmail.com
Supervisor Email: saashareef@uqu.edu.sa

Greetings of thanks to our supervisor Dr. Sarah Al-shareef her help, guidance, and supervision over us.