R·I·T
B. Thomas Golisano
College of Computing and
Information Sciences

Smartphone security evaluation in the era of Big Data

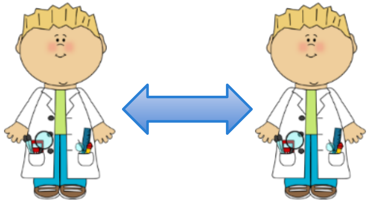
Igor Khokhlov | Leon Reznik
ixk8996@rit.edu | lr@cs.rit.edu

This material is partially based upon work supported by the National Science Foundation under Award # ACI-1547301

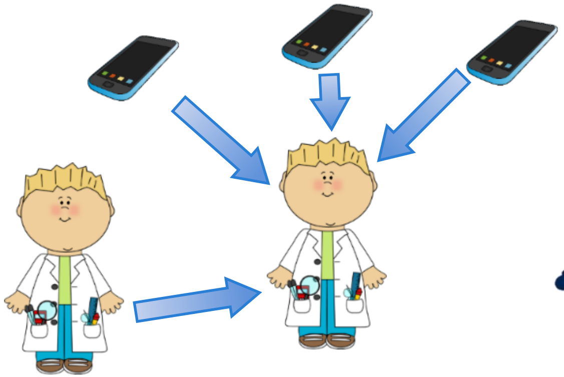
From old data collection model to new infrastructure

Old data collection model

Modern data collection model



From a scientist to a scientist



Citizen science

Internet of Things

Quality Data

What is data quality?

The Data Story Has Changed…

- **The Model of Generating/Consuming Data has Changed**

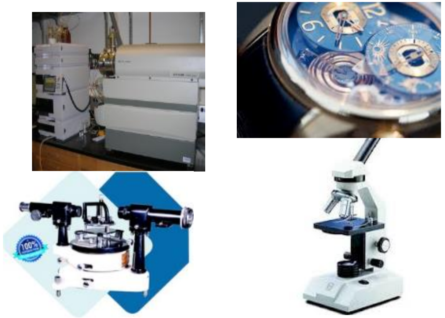
Old Model: Few companies are generating data, all others are consuming data

New Model: all of us are generating data, and all of us are consuming data

@U.Fasoli Big Data and Fast Data combined – is it possible? Swiss Data Forum, 2015
https://www.slideshare.net/SwissDataForum/big-data-and-fast-data-combined-is-it-possible-55642899

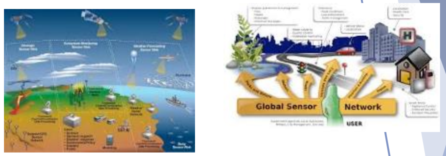
Big Data problems

Social media and networks
(all of us are generating data)



Scientific instruments
(collecting all sorts of data)

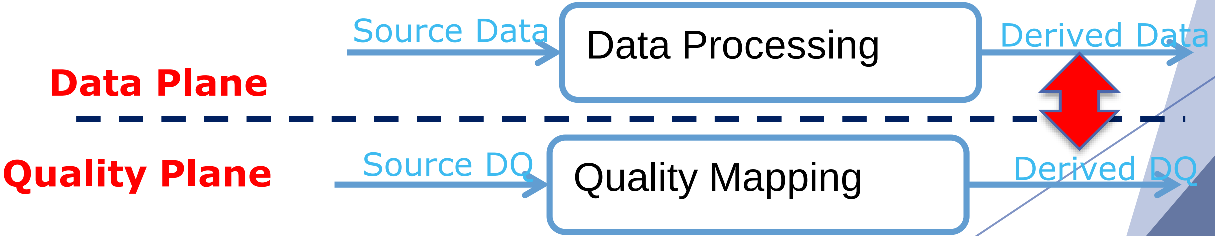
Mobile devices
(tracking all objects all the time)



Sensor technology and networks
(measuring all kinds of data)

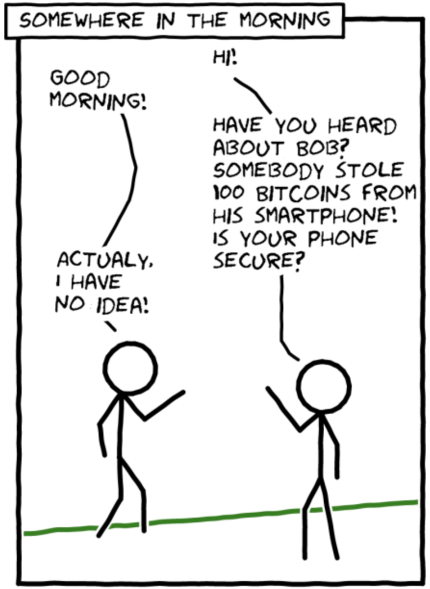
- The progress and innovation is no longer hindered by the ability to collect data
- But, by the ability to manage, analyze, summarize, visualize, and discover knowledge from the collected data in a timely manner and in a scalable fashion

Data Quality Management

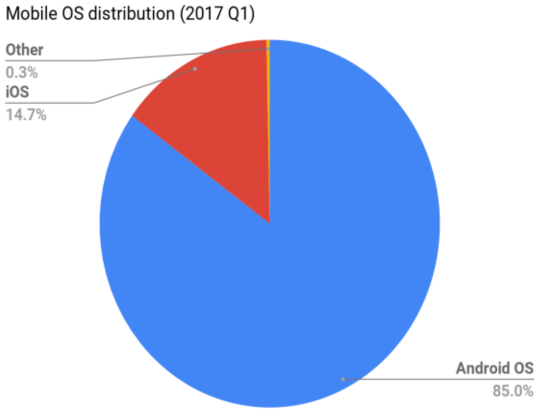


Personal touch

Why is that important?


SOMEWHERE IN THE MORNING
GOOD MORNING!
HI!
HAVE YOU HEARD ABOUT BOB? SOMEBODY STOLE 100 BITCOINS FROM HIS SMARTPHONE! IS YOUR PHONE SECURE?
ACTUALY, I HAVE NO IDEA!

- Smartphones store very private information
- Mobile OS security settings may be confusing for a regular smartphone user
- Android OS extremely popular



Smartphone sensors

- 19 various sensor have been discovered:
  - Accelerometer,
  - Barometer,
  - Gesture,
  - Humidity,
  - Face id,
  - Fingerprint: rear, side, under display, Front,
  - Temperature,
  - Gyroscope,
  - Ambient Light,
  - Heart rate,
  - Compass,
  - UV,
  - Iris Scanner,
  - Spo2,
  - Proximity,
  - Color Spectrum

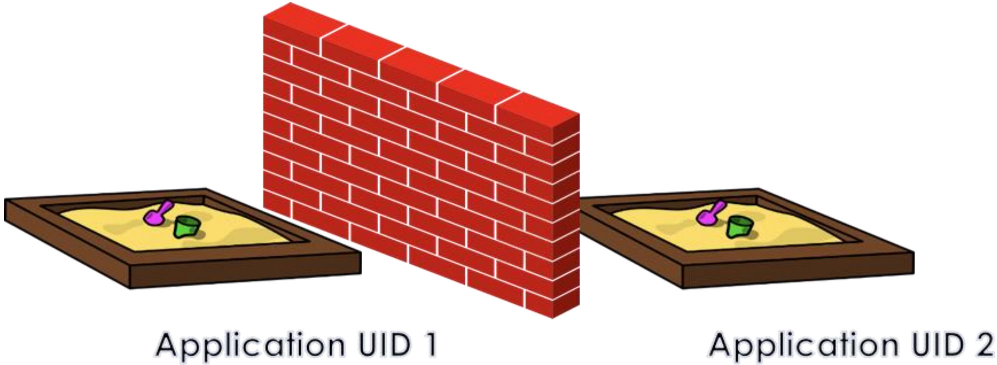
Sensor Type	# of Unique Types
Accelerometer	52
Barometer	5
Compass	18
Gyroscope	14
Proximity	20

Basics of Cyber-Security Defense

Before initializing defense against more complex and sophisticated attacks, it is important to find and fix simple breaches.

Android OS security features

Sandboxing



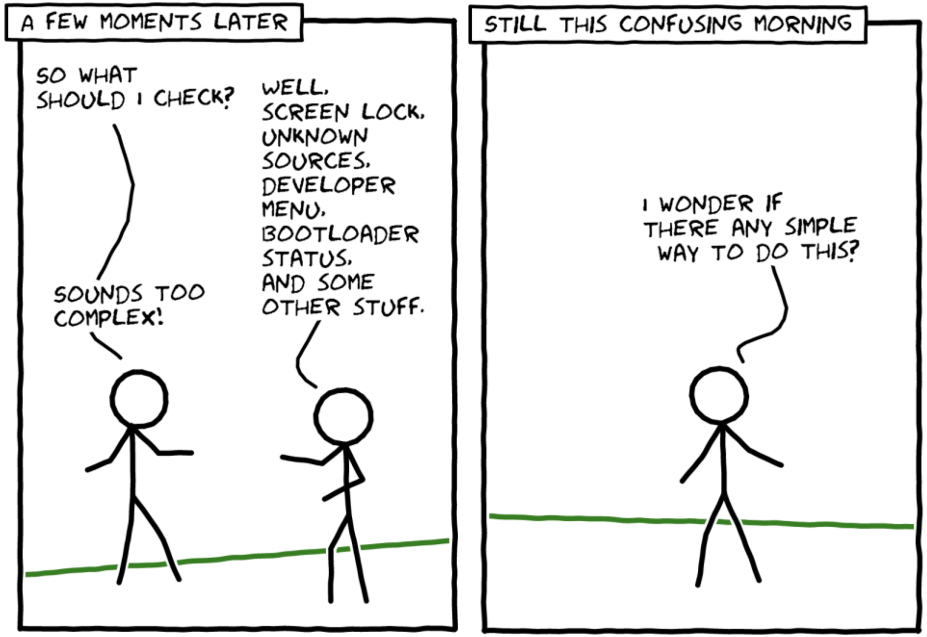
Permissions

In order to use device’s resources, an application should ask for a permission

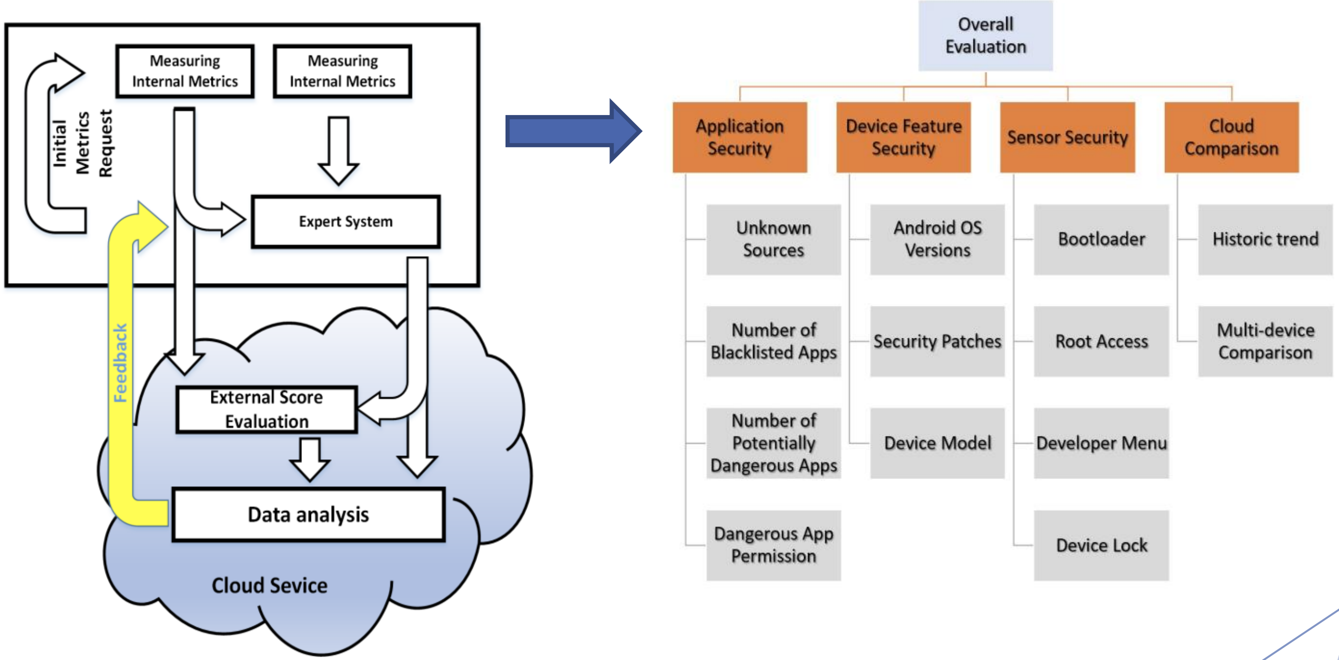
What should I check

- Screen lock
- Android OS version
- Unknown sources
- Potentially harmful applications
- Developer's menu
- Bootloader status
- “Root status”

- **Compare with others**


A FEW MOMENTS LATER
SO WHAT SHOULD I CHECK?
WELL. SCREEN LOCK, UNKNOWN SOURCES, DEVELOPER MENU, BOOTLOADER STATUS, AND SOME OTHER STUFF.
SOUNDS TOO COMPLEX!
STILL THIS CONFUSING MORNING
I WONDER IF THERE ANY SIMPLE WAY TO DO THIS?

Distributed Architecture

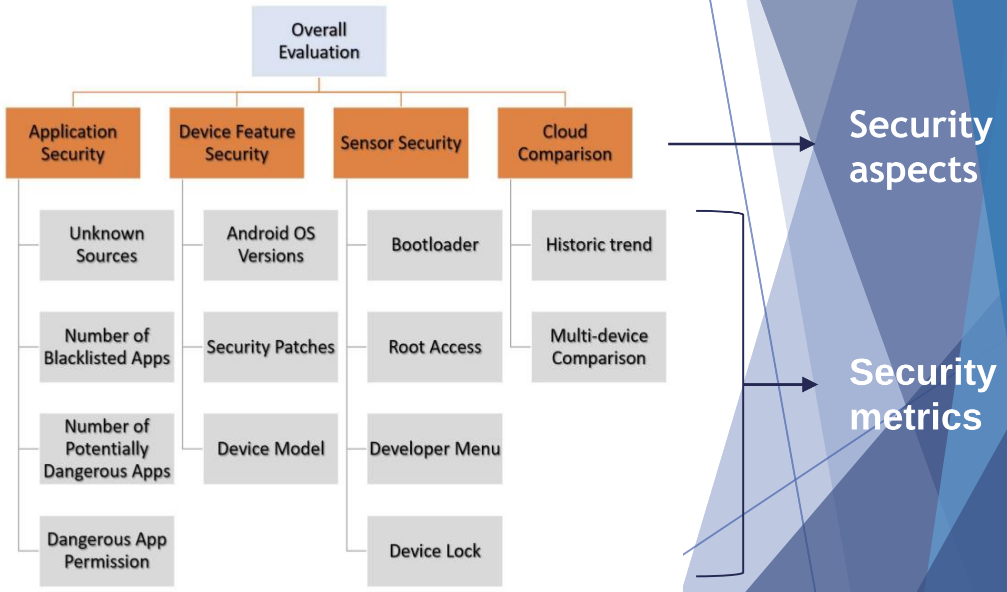

Initial Metrics Request
Measuring Internal Metrics
Measuring Internal Metrics
Expert System
Feedback
External Score Evaluation
Data analysis
Cloud Sevice

- Overall Evaluation
  - Application Security
    - Unknown Sources
    - Number of Blacklisted Apps
    - Number of Potentially Dangerous Apps
    - Dangerous App Permission
  - Device Feature Security
    - Android OS Versions
    - Security Patches
    - Device Model
  - Sensor Security
    - Bootloader
    - Root Access
    - Developer Menu
    - Device Lock
  - Cloud Comparison
    - Historic trend
    - Multi-device Comparison

Android Expert System Module

Benefit of a Expert System:

- Ability to handle ambiguous and/or incomplete data
- Easily expanded or reduced by manipulating its components



Overall Evaluation

Application Security

- Unknown Sources
- Number of Blacklisted Apps
- Number of Potentially Dangerous Apps
- Dangerous App Permission

Device Feature Security

- Android OS Versions
- Security Patches
- Device Model

Sensor Security

- Bootloader
- Root Access
- Developer Menu
- Device Lock

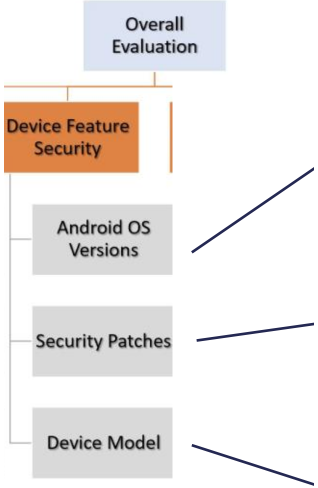
Cloud Comparison

- Historic trend
- Multi-device Comparison

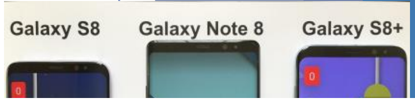
Security aspects

Security metrics

Expert System Module, Cont’D



Nougat
API 24



Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.3%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.3%
4.1.x	Jelly Bean	16	1.2%
4.2.x		17	1.8%
4.3		18	0.5%
4.4	KitKat	19	8.6%
5.0	Lollipop	21	3.8%
5.1		22	15.4%
6.0	Marshmallow	23	22.7%
7.0	Nougat	24	20.3%
7.1		25	10.5%
8.0	Oreo	26	11.4%
8.1		27	3.2%

Table 3: Android OS List

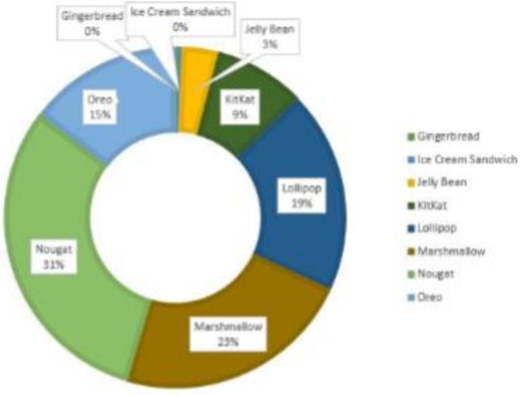
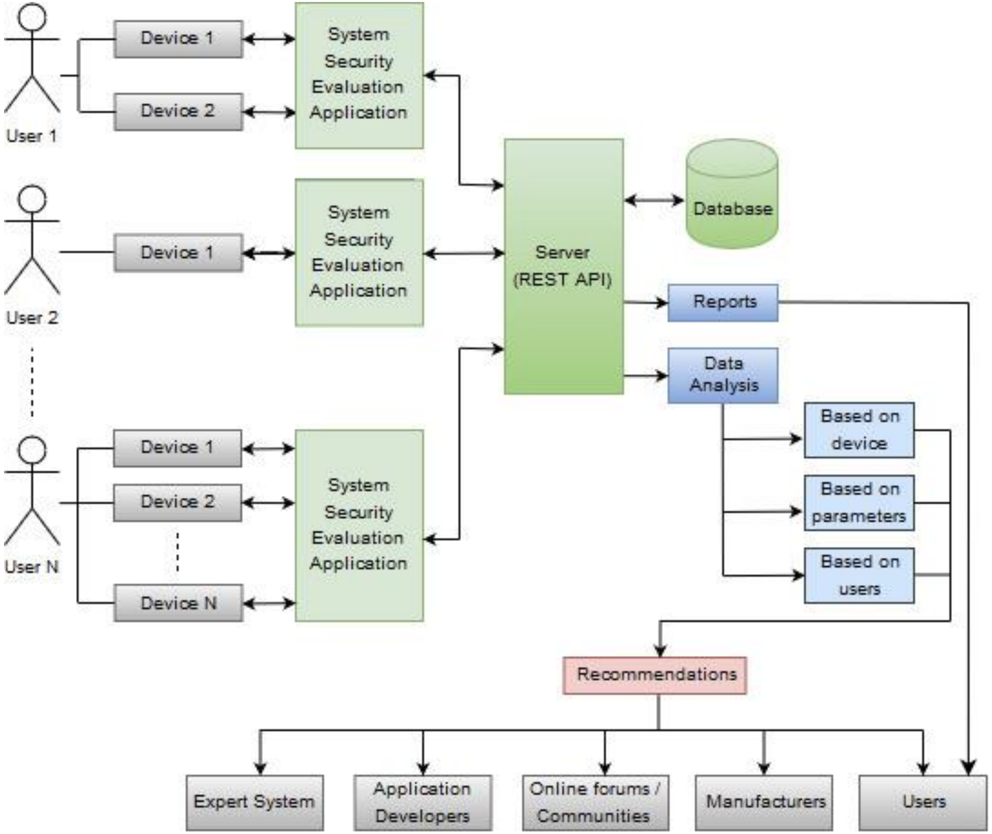
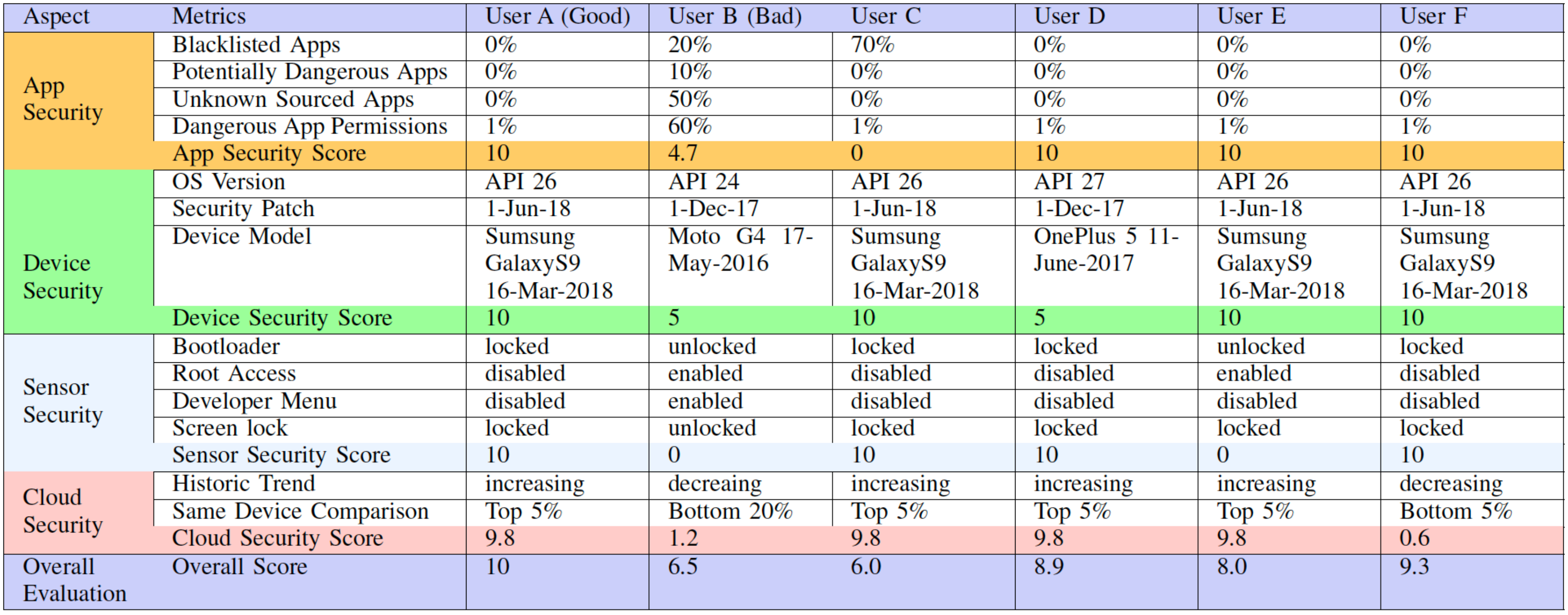


Figure 3: Android OS Distribution

The Cloud Component

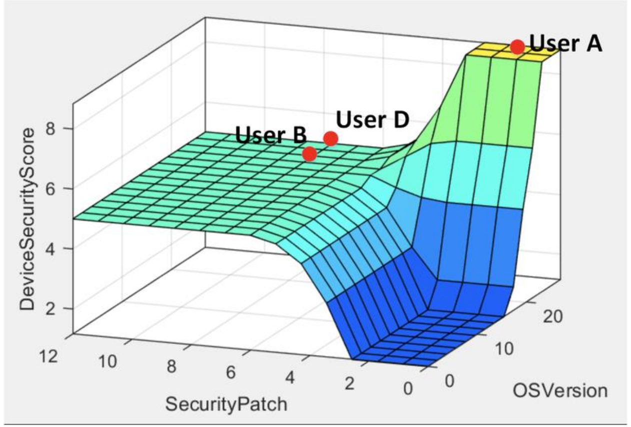


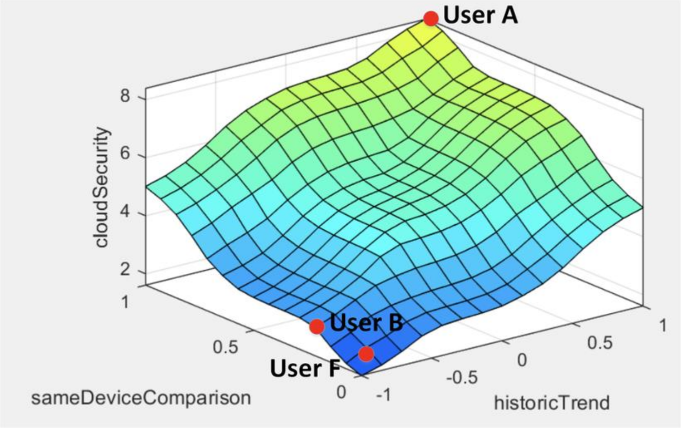
Use Cases

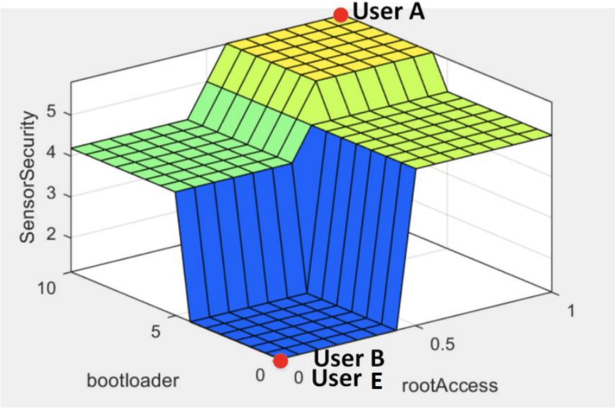


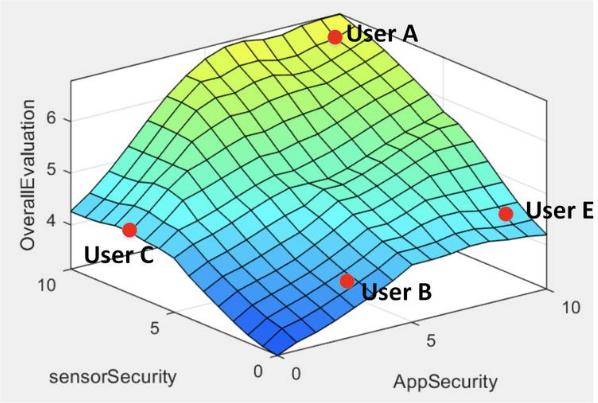
Aspect	Metrics	User A (Good)	User B (Bad)	User C	User D	User E	User F
App Security	Blacklisted Apps	0%	20%	70%	0%	0%	0%
	Potentially Dangerous Apps	0%	10%	0%	0%	0%	0%
	Unknown Sourced Apps	0%	50%	0%	0%	0%	0%
	Dangerous App Permissions	1%	60%	1%	1%	1%	1%
	App Security Score	10	4.7	0	10	10	10
Device Security	OS Version	API 26	API 24	API 26	API 27	API 26	API 26
	Security Patch	1-Jun-18	1-Dec-17	1-Jun-18	1-Dec-17	1-Jun-18	1-Jun-18
	Device Model	Sumsung GalaxyS9 16-Mar-2018	Moto G4 17-May-2016	Sumsung GalaxyS9 16-Mar-2018	OnePlus 5 11-June-2017	Sumsung GalaxyS9 16-Mar-2018	Sumsung GalaxyS9 16-Mar-2018
	Device Security Score	10	5	10	5	10	10
Sensor Security	Bootloader	locked	unlocked	locked	locked	unlocked	locked
	Root Access	disabled	enabled	disabled	disabled	enabled	disabled
	Developer Menu	disabled	enabled	disabled	disabled	disabled	disabled
	Screen lock	locked	unlocked	locked	locked	locked	locked
	Sensor Security Score	10	0	10	10	0	10
Cloud Security	Historic Trend	increasing	decreaing	increasing	increasing	increasing	decreasing
	Same Device Comparison	Top 5%	Bottom 20%	Top 5%	Top 5%	Top 5%	Bottom 5%
	Cloud Security Score	9.8	1.2	9.8	9.8	9.8	0.6
Overall Evaluation	Overall Score	10	6.5	6.0	8.9	8.0	9.3

Use Cases

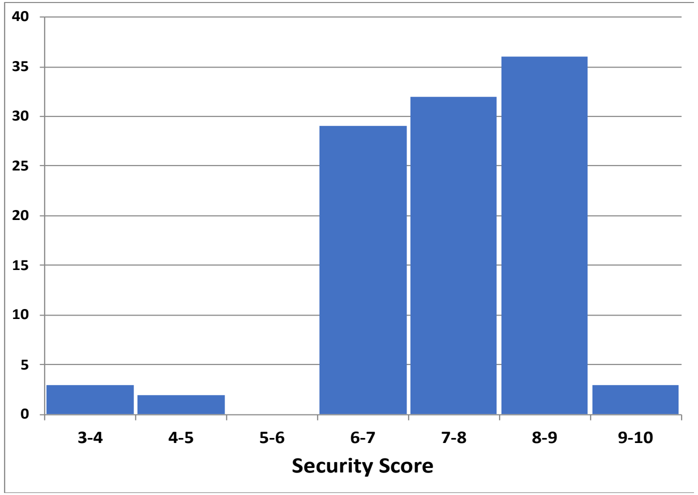

User A
User D
User B
DeviceSecurityScore
8
6
4
2
12
10
8
6
4
2
0
SecurityPatch
0
10
20
OSVersion

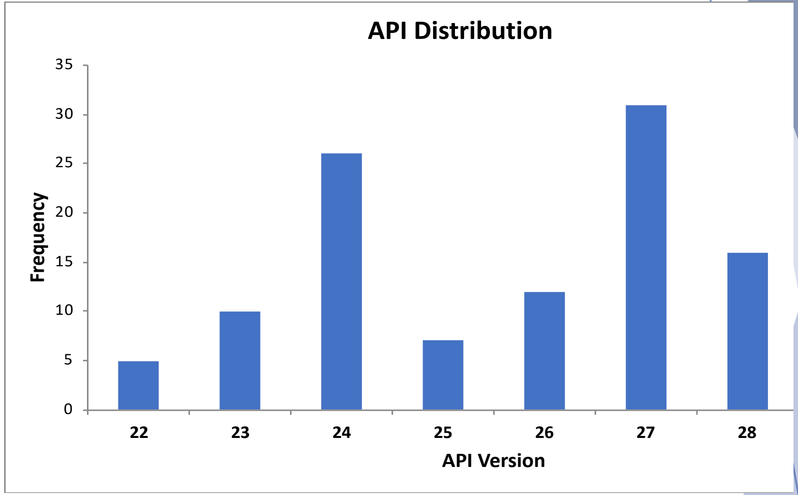

User A
cloudSecurity
8
6
4
2
1
User B
User F
0.5
0
sameDeviceComparison
-1
-0.5
0
0.5
1
historicTrend


User A
SensorSecurity
5
4
3
2
10
5
0
bootloader
User B
User E
0
0.5
1
rootAccess


User A
OverallEvaluation
6
5
4
User C
User E
User B
10
5
0
sensorSecurity
0
5
10
AppSecurity

Current state of smartphone security. Our statistics.





Maximum	9.8
Minimum	3.9
Standard Deviation	1.4
Average	7.5
Median	7.3

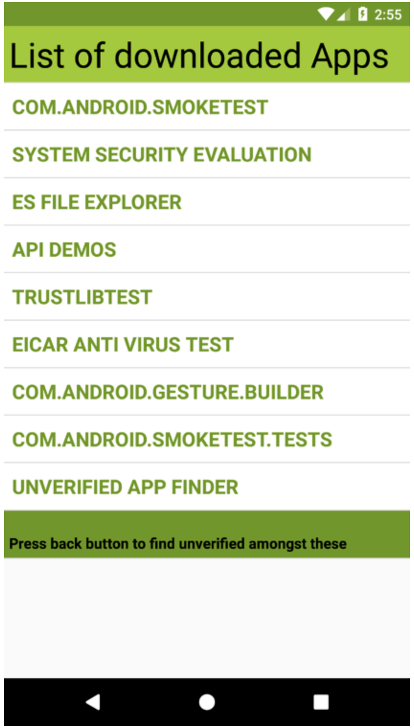
Apps on Google Play

Detector of unverified apps

VERIFIED

DETECTOR OF UNVERIFIED APPS

https://goo.gl/qR2A1i



2:55

List of downloaded Apps

COM.ANDROID.SMOKETEST

SYSTEM SECURITY EVALUATION

ES FILE EXPLORER

API DEMOS

TRUSTLIBTEST

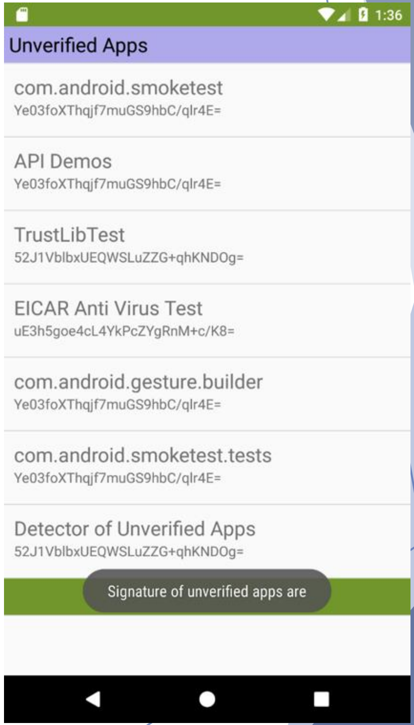
EICAR ANTI VIRUS TEST

COM.ANDROID.GESTURE.BUILDER

COM.ANDROID.SMOKETEST.TESTS

UNVERIFIED APP FINDER

Press back button to find unverified amongst these



1:36

Unverified Apps

com.android.smoketest
Ye03foXThqjf7muGS9hbC/qlr4E=

API Demos
Ye03foXThqjf7muGS9hbC/qlr4E=

TrustLibTest
52J1VblbxUEQWSLuZZG+qhKNDOg=

EICAR Anti Virus Test
uE3h5goe4cL4YkPcZYgRnM+c/K8=

com.android.gesture.builder
Ye03foXThqjf7muGS9hbC/qlr4E=

com.android.smoketest.tests
Ye03foXThqjf7muGS9hbC/qlr4E=

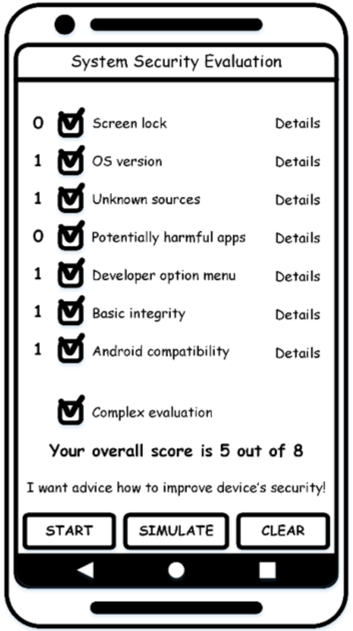
Detector of Unverified Apps
52J1VblbxUEQWSLuZZG+qhKNDOg=

Signature of unverified apps are

Apps on Google Play

Security Evaluation

https://goo.gl/EzVb9b



System Security Evaluation

0 ☑ Screen lock Details

1 ☑ OS version Details

1 ☑ Unknown sources Details

0 ☑ Potentially harmful apps Details

1 ☑ Developer option menu Details

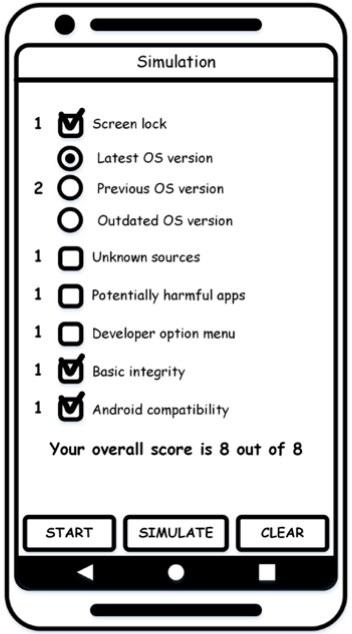
1 ☑ Basic integrity Details

1 ☑ Android compatibility Details

☑ Complex evaluation

Your overall score is 5 out of 8

I want advice how to improve device's security!



Simulation

1 ☑ Screen lock

● Latest OS version

2 ○ Previous OS version

○ Outdated OS version

1 □ Unknown sources

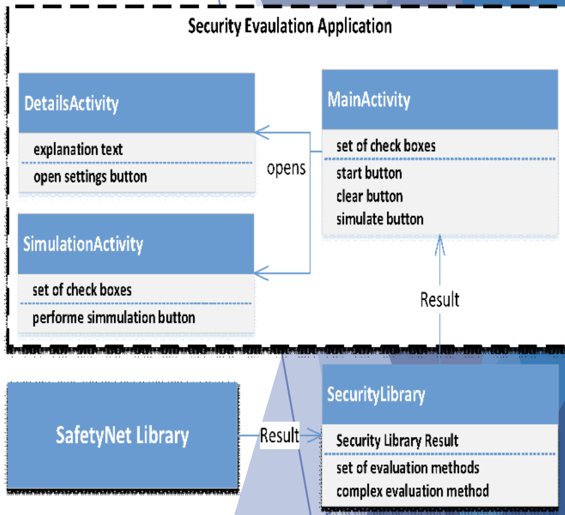
1 □ Potentially harmful apps

1 □ Developer option menu

1 ☑ Basic integrity

1 ☑ Android compatibility

Your overall score is 8 out of 8



Security Evaulation Application

DetailsActivity
- explanation text
- open settings button

MainActivity
- set of check boxes
- start button
- clear button
- simulate button

opens

SimulationActivity
- set of check boxes
- performe simmulation button

Result

SafetyNet Library

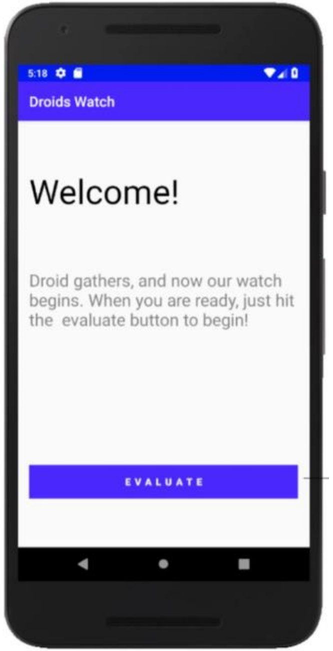
Result

SecurityLibrary
- Security Library Result
- set of evaluation methods
- complex evaluation method

Wait for the demo

Cloud Version : https://dataqualitylab.page.link/SECLD

Droids Watch



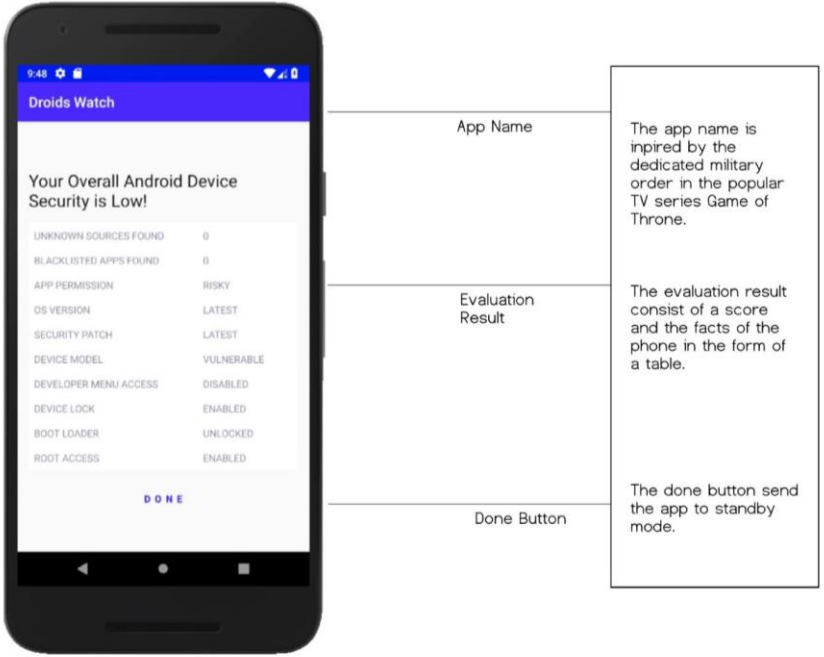
5:18

Droids Watch

Welcome!

Droid gathers, and now our watch begins. When you are ready, just hit the evaluate button to begin!

EVALUATE



9:48

Droids Watch

Your Overall Android Device Security is Low!

UNKNOWN SOURCES FOUND	0
BLACKLISTED APPS FOUND	0
APP PERMISSION	RISKY
OS VERSION	LATEST
SECURITY PATCH	LATEST
DEVICE MODEL	VULNERABLE
DEVELOPER MENU ACCESS	DISABLED
DEVICE LOCK	ENABLED
BOOT LOADER	UNLOCKED
ROOT ACCESS	ENABLED

DONE

The app name is inpired by the dedicated military order in the popular TV series Game of Throne.

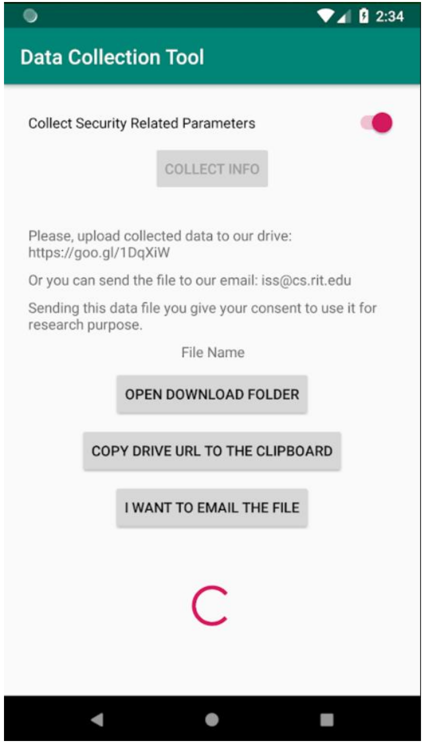
The evaluation result consist of a score and the facts of the phone in the form of a table.

The done button send the app to standby mode.

Wait for the demo

Enjoy the demo

Data Collection Tool



Collect Security Related Parameters

Please, upload collected data to our drive: https://goo.gl/1DqXiW

Or you can send the file to our email: iss@cs.rit.edu

Sending this data file you give your consent to use it for research purpose.

File Name

- Collects smartphone's data such as a device model, hardware description, onboard sensors, and various security metrics.
- No private information about the owner is recorded.
- It gives a user an option to prepare data for sending it to the specified email or remote folder.

https://play.google.com/store/apps/details?id=
com.dataqualitylab.collectinfo.collectinfo

(Shortened URL: https://goo.gl/JmM8Mm)

Data set

- Information from more than one hundred devices
- Four groups of information:
  - Basic device information
  - Sensor information
  - Application permissions information:
    - permissions requested
    - permissions granted
  - Security related information

Conclusion

- Tools currently available in Google Play mostly concentrate on virus detection, and the methods focus on application source code analysis.
- We developed a rule-based intelligent system that performed security evaluation, taking certain system features and parameters as inputs, and producing a security score as an output.
- We employed hierarchical architecture of the fuzzy logic expert system that allows easy framework adaptation to incorporate new security features in the future.
- To design such a system, the main Android OS features that are related to the security and participated in the overall security evaluation were investigated and analyzed
- The framework employs a cloud for storing security scores and their further analysis that includes a comparison with other user devices or with equivalent devices owned by other users.
- To evaluate the framework’s performance, an empirical study that included an examination of various use cases was conducted.