ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Search Rank Fruad and Malware Detection in Google Play using Dot Net

K. Radha Krishna
Department of Computer Science & Engineering
Jogaiah Institute of Technology and Sciences College of Engineering,
Palakol, West Godavari Dt., A.P-534 268, India.

Mr.A.Veerabhadra Rao
Department of Computer Science & Engineering
Jogaiah Institute of Technology and Sciences College of Engineering,
Palakol, West Godavari Dt., A.P-534 268, India.

ABSTRACT:

Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation. To identify malware, previous work has focused on app executable and permission analysis. In this paper, we introduce FairPlay, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. FairPlay correlates review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from Google Play app data (87 K apps, 2.9 M reviews, and 2.4M reviewers, collected over half a year), in order to identify suspicious apps. FairPlay achieves over 95 percent accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps. We show that 75 percent of the identified malware apps engage in search rank fraud.

FairPlay discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology. FairPlay also helped the discovery of more than 1,000 reviews, reported for 193 apps that reveal a new type of "coercive" review campaign: users are harassed into writing positive reviews, and install and review other apps

INTRODUCTION

1.1 Introduction to Project

The commercial success of Android app markets such as Google Play [1] and the incentive model they offer to Popular apps make them appealing targets for fraudulent and malicious behaviors. Some fraudulent developers deceptively boost the search rank and popularity of their Apps (e.g., through fake reviews and bogus installation Counts) [2].

while malicious developers use app markets as a Launch pad for their malware [3], [4], [5], [6]. The motivation For such behaviors is impact: app popularity surges translate Into financial benefits and expedited malware proliferation.

Cite this article as: K. Radha Krishna & Mr.A.Veerabhadra Rao, " Search Rank Fruad and Malware Detection in Google Play using Dot Net", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 6 Issue 8, 2019, Page 30-41.

Organization Profile

Software Solutions is an IT solution provider for a dynamic environment where business and technology strategies converge. Their approach focuses on new ways of business combining IT innovation and adoption while also leveraging an organization's current IT assets. Their work with large global corporations and new products or services and to implement prudent business and technology strategies in today's environment.

Xxxxxxx's Range Of Expertise Includes:

- Software Development Services
- Engineering Services
- Systems Integration
- Customer Relationship Management
- Product Development
- Electronic Commerce
- Consulting
- IT Outsourcing

We apply technology with innovation and responsibility to achieve two broad objectives:

- Effectively address the business issues our customers face today.
- Generate new opportunities that will help them stay ahead in the future.

This Approach Rests On:

- A strategy where we architect, integrate and manage technology services and solutions - we call it AIM for success.
- A robust offshore development methodology and reduced demand on customer resources.
- A focus on the use of reusable frameworks to provide cost and times benefits.

They combine the best people, processes and technology to achieve excellent results - consistency. We offer customers the advantages of:

Speed:

They understand the importance of timing, of getting there before the competition. A rich portfolio of reusable, modular frameworks helps jump-start projects. Tried and tested methodology ensures that we follow a predictable, low - risk path to achieve results. Our track record is testimony to complex projects delivered within and evens before schedule.

Expertise:

Our teams combine cutting edge technology skills with rich domain expertise. What's equally important - they share a strong customer orientation that means they actually start by listening to the customer. They're focused on coming up with solutions that serve customer requirements today and anticipate future needs.

A Full Service Portfolio:

They offer customers the advantage of being able to Architect, integrate and manage technology services. This means that they can rely on one, fully accountable source instead of trying to integrate disparate multi vendor solutions.

Services:

Xxx is providing its services to companies which are in the field of production, quality control etc with their rich expertise and experience and information technology they are in best position to provide software solutions to distinct business requirements.

1.2Purpose of the Project

In this project we will identify both the malware and the search rank fraud subjects in Google Play. This combination is not arbitrary: we posit that malicious developers resort to search rank fraud to boost the impact of their malware. Unlike existing solutions, we build this project on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets. We uncover these nefarious acts by picking out such trails. For instance, the high cost of setting up valid Google Play accounts forces fraudsters to reuse their accounts across review writing jobs, making them likely to review more apps in common than regular users. Resource constraints can compel fraudsters to post reviews within short time intervals. Legitimate users affected by malware may report unpleasant experiences in their reviews. Increases in the number of requested permissions from one version to the next, which we will call “permission ramps”, may indicate benign to malware (Jekyll-Hyde) transitions.

1.3 Existing System:

In the existing system the commercial success of Android app markets such as Google Play and the incentive model they offer to popular apps, make them appealing targets for fraudulent and malicious behaviors. Some fraudulent developers deceptively boost the search rank and popularity of their apps (e.g., through fake reviews and bogus installation counts), while malicious developers use app markets as a launch pad for their malware. The motivation for such behaviors is impact: app popularity surges translate into financial benefits and expedited malware proliferation. Fraudulent developers frequently exploit crowd sourcing sites (e.g., Freelancer, Fiverr, BestAppPromotion) to hire teams of willing workers to commit fraud collectively, emulating realistic, spontaneous activities from unrelated people (i.e., “crowdturfing”). We call this behavior “search rank fraud”.

Disadvantages of exiting system

- In addition, the efforts of Android markets to identify and remove malware are not always successful. For instance, Google Play uses the Bouncer system to remove malware. However, out of the 7,756 Google Play apps we analyzed using Virus Total, 12 percent (948) were flagged by at least one anti-virus tool and 2 percent (150) were identified as malware by at least 10 tools.

- Previous mobile malware detection work has focused on dynamic analysis of app executables as well as static analysis of code and permissions. However, recent Android malware analysis revealed that malware evolves quickly to bypass anti-virus tools.

1.2 Proposed System Algorithms

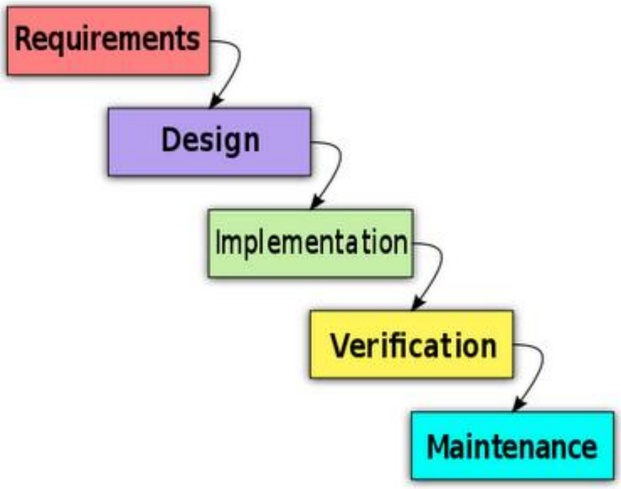
In this project we will identify both the malware and the search rank fraud subjects in Google Play. This combination is not arbitrary: we posit that malicious developers resort to search rank fraud to boost the impact of their malware. Unlike existing solutions, we build this project on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets. We uncover these nefarious acts by picking out such trails. For instance, the high cost of setting up valid Google Play accounts forces fraudsters to reuse their accounts across review writing jobs, making them likely to review more apps in common than regular users. Resource constraints can compel fraudsters to post reviews within short time intervals. Legitimate users affected by malware may report unpleasant experiences in their reviews. Increases in the number of requested permissions from one version to the next, which we will call "permission ramps", may indicate benign to malware (Jekyll-Hyde) transitions.

Advantage of Proposed System:

- We formulate the notion of co-review graphs to model reviewing relations between users. We develop PCF, an efficient algorithm to identify temporally constrained, co-review pseudo-cliques—formed by reviewers with substantially overlapping co-reviewing activities across short time windows.
- We use temporal dimensions of review post times to identify suspicious review spikes received by apps. We also identify apps with "unbalanced" review, rating and install counts, as well as apps with permission request ramps.

2. System Analysis

Software Development Life Cycle:-



There is various software development approaches defined and designed which are used/employed during development process of software, these approaches are also referred as "Software Development Process Models". Each process model follows a particular life cycle in order to ensure success in process of software development.

Requirements

Business requirements are gathered in this phase. This phase is the main focus of the project managers and stake holders. Meetings with managers, stake holders and users are held in order to determine the requirements. Who is going to use the system? How will they use the system? What data should be input into the system? What data should be output by the system? These are general questions that get answered during a requirements gathering phase. This produces a nice big list of functionality that the system should provide, which describes functions the system should perform, business logic that processes data, what data is stored and used by the system, and how the user interface should work. The overall result is the system as a whole and how it performs, not how it is actually going to do it.

Design

The software system design is produced from the results of the requirements phase. Architects have the ball in their court during this phase and this is the phase in which their focus lies. This is where the details on how the system will work is produced. Architecture, including hardware and software, communication, software design (UML is produced here) are all part of the deliverables of a design phase.

Implementation

Code is produced from the deliverables of the design phase during implementation, and this is the longest phase of the software development life cycle. For a developer, this is the main focus of the life cycle because this is where the code is produced. Implementation my overlap with both the design and testing phases. Many tools exists (CASE tools) to actually automate the production of code using information gathered and produced during the design phase.

Testing

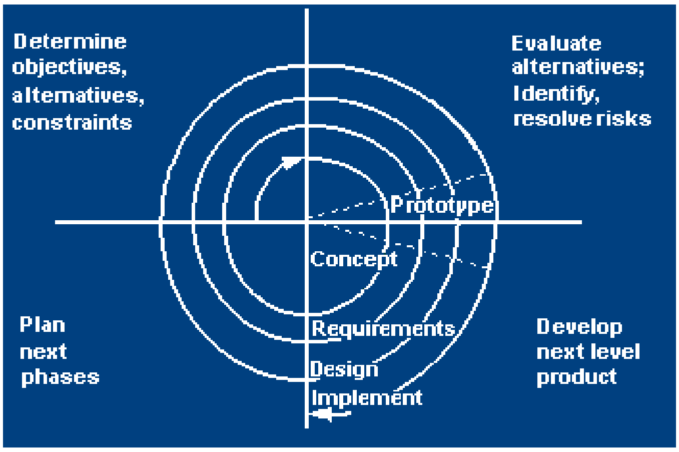
During testing, the implementation is tested against the requirements to make sure that the product is actually solving the needs addressed and gathered during the requirements phase. Unit tests and system/acceptance tests are done during this phase. Unit tests act on a specific component of the system, while system tests act on the system as a whole.

So in a nutshell, that is a very basic overview of the general software development life cycle model. Now let’s delve into some of the traditional and widely used variations.

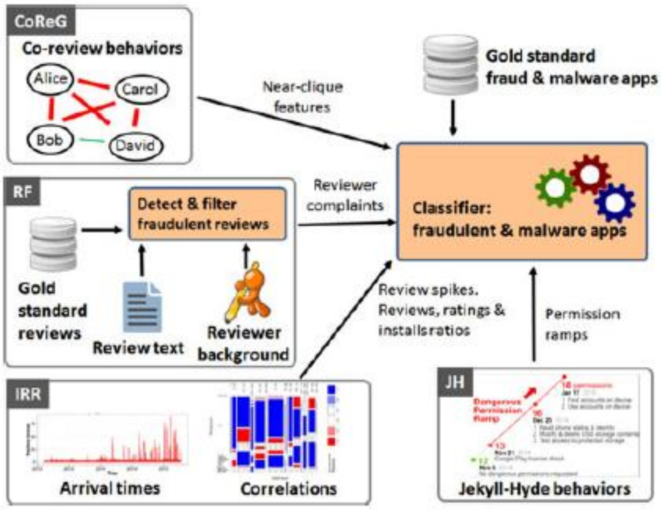
Sdlc Methdologies

This document play a vital role in the development of life cycle (SDLC) as it describes the complete requirement of the system. It means for use by developers and will be the basic during testing phase. Any changes made to the requirements in the future will have to go through formal change approval process.

SPIRAL MODEL was defined by Barry Boehm in his 1988 article, "A spiral Model of Software Development and Enhancement. This model was not the first model to discuss iterative development, but it was the first model to explain why the iteration models. As originally envisioned, the iterations were typically 6 months to 2 years long. Each phase starts with a design goal and ends with a client reviewing the progress thus far. Analysis and engineering efforts are applied at each phase of the project, with an eye toward the end goal of the project.The following diagram shows how a spiral model acts like:


Determine objectives, altematives, constraints
Evaluate alternatives; Identify, resolve risks
Prototype
Concept
Requirements
Design
Implement
Plan next phases
Develop next level product

System Architecture:



Selected Software:

Introduction to .Net Framework:

The **Microsoft .NET Framework** is a software technology that is available with several Microsoft Windows operating systems. It includes a large library of pre-coded solutions to common programming problems and a virtual machine that manages the execution of programs written specifically for the framework. The .NET Framework is a key Microsoft offering and is intended to be used by most new applications created for the Windows platform.

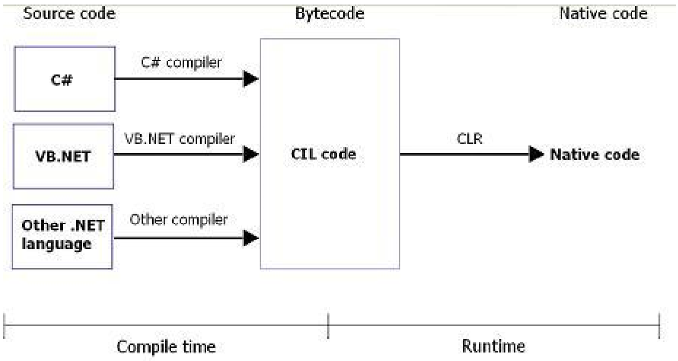
The pre-coded solutions that form the framework's Base Class Library cover a large range of programming needs in a number of areas, including user interface, data access, database connectivity, cryptography, web application development, numeric algorithms, and network communications. The class library is used by programmers, who combine it with their own code to produce applications.

Programs written for the .NET Framework execute in a software environment that manages the program's runtime requirements. Also part of the .NET Framework, this runtime environment is known as the Common Language Runtime (CLR).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

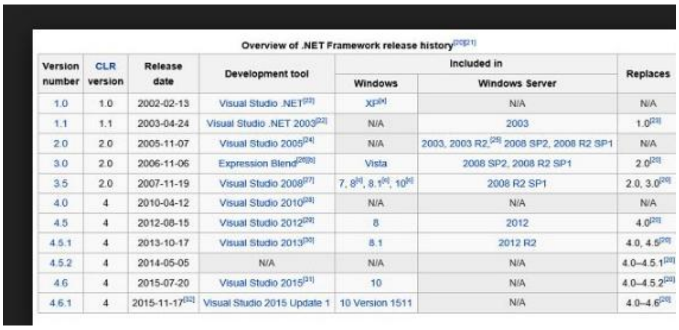
The CLR provides the appearance of an application virtual machine so that programmers need not consider the capabilities of the specific CPU that will execute the program. The CLR also provides other important services such as security, memory management, and exception handling. The class library and the CLR together compose the .NET Framework.

Architecture:



Visual overview of the Common Language Infrastructure (CLI)

The **.NET Framework** stack:



Overview of .NET Framework release history[20][21]

Version number	CLR version	Release date	Development tool	Included in		Replaces
				Windows	Windows Server	
1.0	1.0	2002-02-13	Visual Studio .NET[23]	XP[a]	N/A	N/A
1.1	1.1	2003-04-24	Visual Studio .NET 2003[22]	N/A	2003	1.0[23]
2.0	2.0	2005-11-07	Visual Studio 2005[24]	N/A	2003, 2003 R2,[25] 2008 SP2, 2008 R2 SP1	N/A
3.0	2.0	2006-11-06	Expression Blend[26][b]	Vista	2008 SP2, 2008 R2 SP1	2.0[20]
3.5	2.0	2007-11-19	Visual Studio 2008[27]	7, 8[d], 8.1[d], 10[d]	2008 R2 SP1	2.0, 3.0[20]
4.0	4	2010-04-12	Visual Studio 2010[28]	N/A	N/A	N/A
4.5	4	2012-08-15	Visual Studio 2012[29]	8	2012	4.0[20]
4.5.1	4	2013-10-17	Visual Studio 2013[30]	8.1	2012 R2	4.0, 4.5[20]
4.5.2	4	2014-05-05	N/A	N/A	N/A	4.0–4.5.1[20]
4.6	4	2015-07-20	Visual Studio 2015[31]	10	N/A	4.0–4.5.2[20]
4.6.1	4	2015-11-17[32]	Visual Studio 2015 Update 1	10 Version 1511	N/A	4.0–4.6[20]

Client Application Development:

Client applications are the closest to a traditional style of application in Windows-based programming. These are the types of applications that display windows or forms on the desktop, enabling a user to perform a task. Client applications include applications such as word processors and spreadsheets, as well as custom business applications such as data-entry tools, reporting tools, and so on. Client applications usually employ windows, menus, buttons, and other GUI elements, and they likely access local resources such as the file system and peripherals such as printers. Another kind of client application is the traditional ActiveX control (now replaced by the managed Windows Forms control) deployed over the Internet as a Web page. This application is much like other client applications: it is executed natively, has access to local resources, and includes graphical elements.

Server Application Development:

Server-side applications in the managed world are implemented through runtime hosts. Unmanaged applications host the common language runtime, which allows your custom managed code to control the behavior of the server.

This model provides you with all the features of the common language runtime and class library while gaining the performance and scalability of the host server.

Server-side managed code:

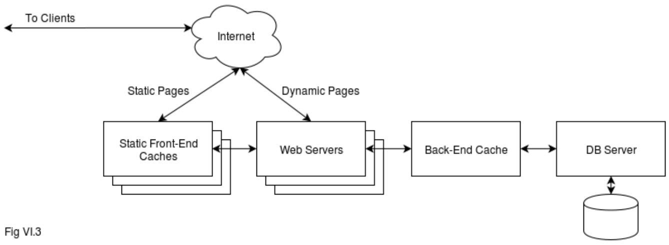


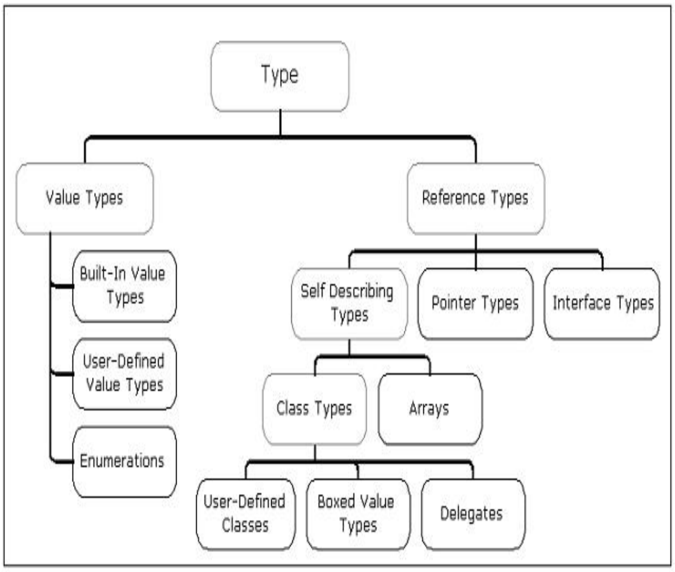
Fig VI.3

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Common Type System (CTS):

This data type problem is solved in .NET through the use of the **Common Type System** (**CTS**). The CTS defines the predefined data types that are available in IL, so that all languages that target the .NET framework will produce compiled code that is ultimately based on these types.

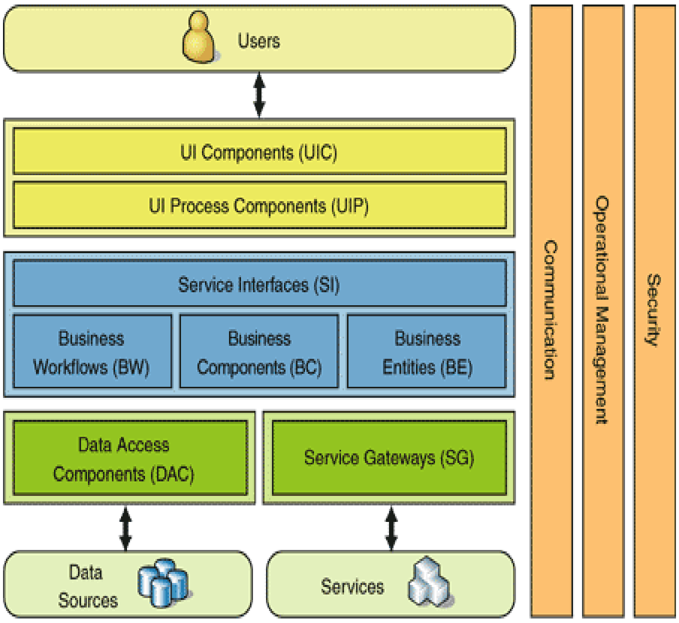
The CTS doesn't merely specify primitive data types, but a rich hierarchy of types, which includes well-defined points in the hierarchy at which code is permitted to define its own types. The hierarchical structure of the Common Type System reflects the single-inheritance object-oriented methodology of IL, and looks like this:



Common Language Specification (CLS)

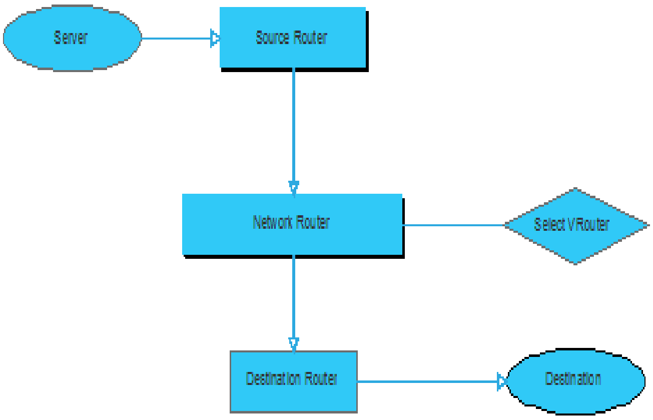
The Role of C# in .Net Enterprise Architecture:

C# requires the presence of the .NET runtime, and it will probably be a few years before most clients – particularly most home machines – have .NET installed. In the meantime, installing a C# application is likely to mean also installing the .NET redistributable components. Because of that, it is likely that the first place we will see many C# applications is in the enterprise environment. Indeed, C# arguably presents an outstanding opportunity for organizations that are interested in building robust, n-tiered client-server applications.

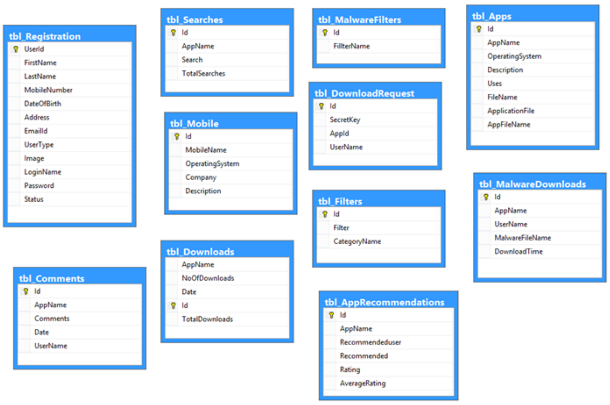


DFD Diagrams:

Context Level Diagram (O Level):



ER-DIAGRAM


tbl_Registration: UserId, FirstName, LastName, MobileNumber, DateOfBirth, Address, EmailId, UserType, Image, LoginName, Password, Status

tbl_Searches: Id, AppName, Search, TotalSearches

tbl_MalwareFilters: Id, FillterName

tbl_Apps: Id, AppName, OperatingSystem, Description, Uses, FileName, ApplicationFile, AppFileName

tbl_Mobile: Id, MobileName, OperatingSystem, Company, Description

tbl_DownloadRequest: Id, SecretKey, AppId, UserName

tbl_MalwareDownloads: Id, AppName, UserName, MalwareFileName, DownloadTime

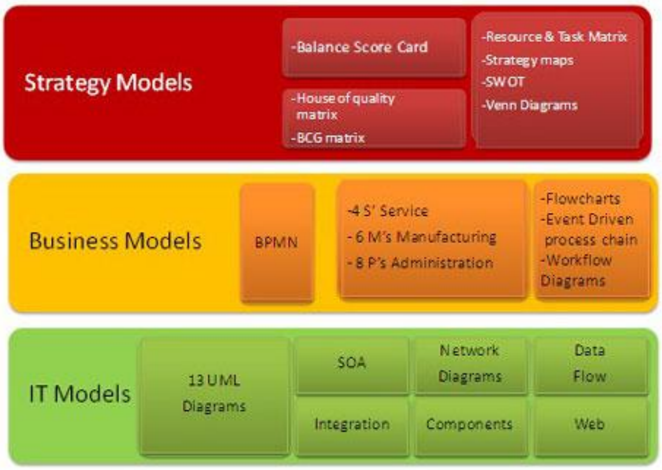
tbl_Filters: Id, Filter, CategoryName

tbl_Downloads: AppName, NoOfDownloads, Date, Id, TotalDownloads

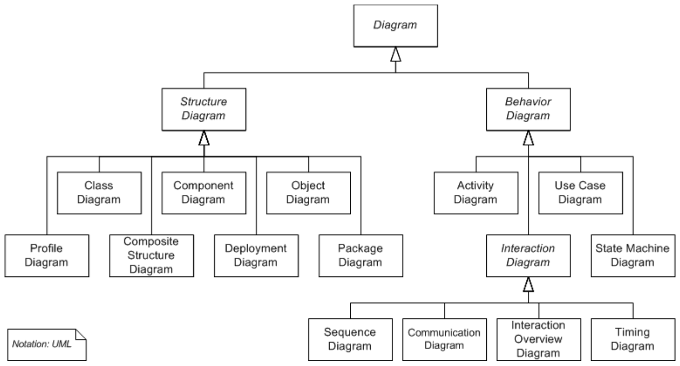
tbl_Comments: Id, AppName, Comments, Date, UserName

tbl_AppRecommendations: Id, AppName, Recommendeduser, Recommended, Rating, AverageRating

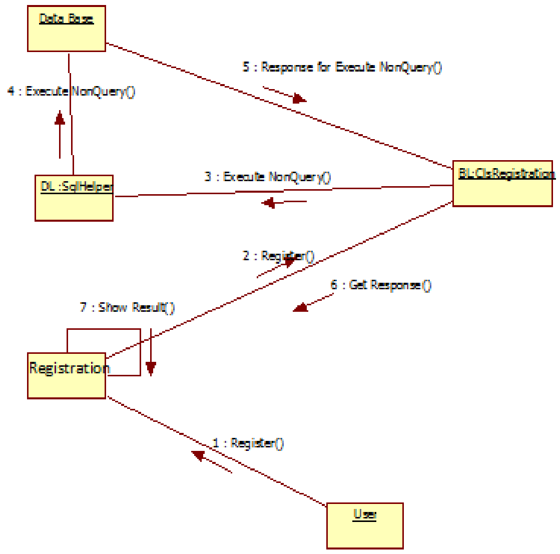
Uml Diagrams:



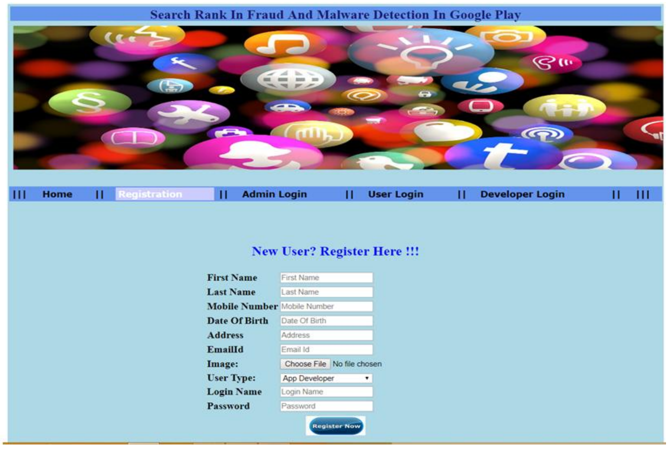
UML Diagrams Overview:



Collaboration diagram:



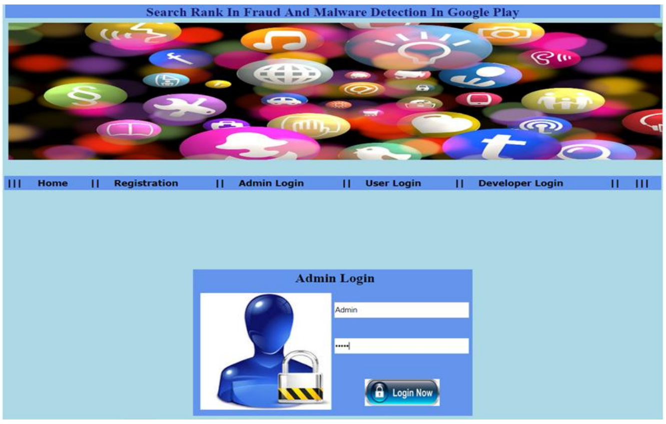
Output Screens:


Search Rank In Fraud And Malware Detection In Google Play

||| Home || Registration || Admin Login || User Login || Developer Login || |||

New User? Register Here !!!

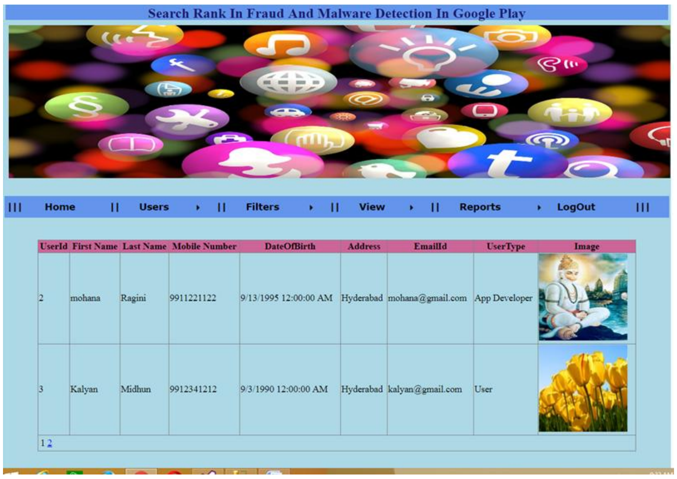
First Name	First Name
Last Name	Last Name
Mobile Number	Mobile Number
Date Of Birth	Date Of Birth
Address	Address
EmailId	Email Id
Image:	Choose File No file chosen
User Type:	App Developer
Login Name	Login Name
Password	Password


Search Rank In Fraud And Malware Detection In Google Play

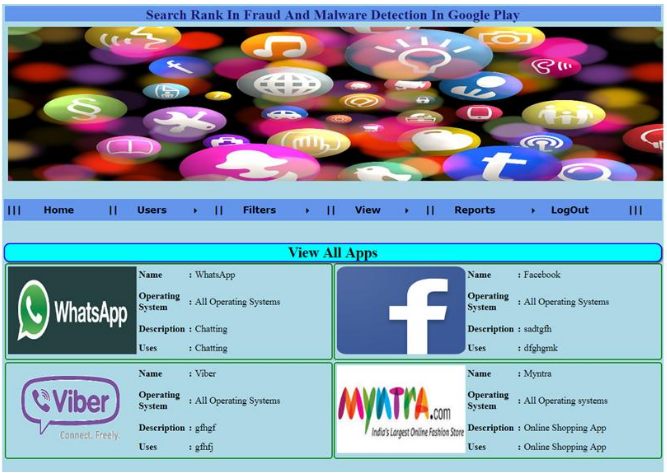
||| Home || Registration || Admin Login || User Login || Developer Login || |||

Admin Login

Admin
•••••



UserId	First Name	Last Name	Mobile Number	DateOfBirth	Address	EmailId	UserType	Image
2	mohana	Ragini	9911221122	9/13/1995 12:00:00 AM	Hyderabad	mohana@gmail.com	App Developer	
3	Kalyan	Midhun	9912341212	9/3/1990 12:00:00 AM	Hyderabad	kalyan@gmail.com	User	
1 2								



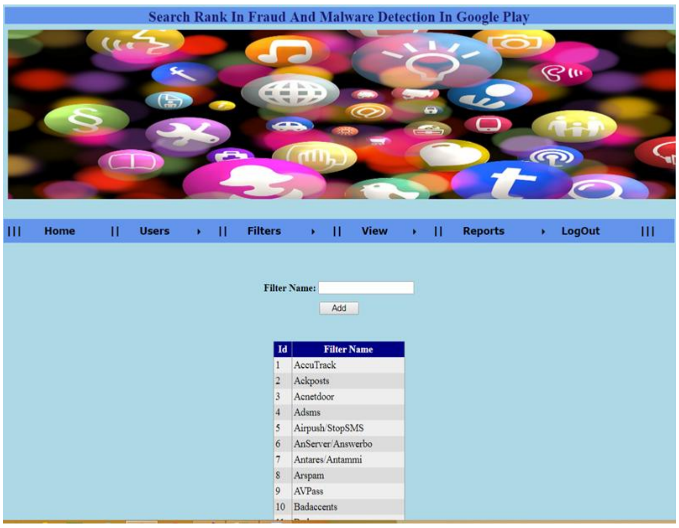
View All Apps

Name : WhatsApp
Operating System : All Operating Systems
Description : Chatting
Uses : Chatting

Name : Facebook
Operating System : All Operating Systems
Description : sadtgfh
Uses : dfghgmk

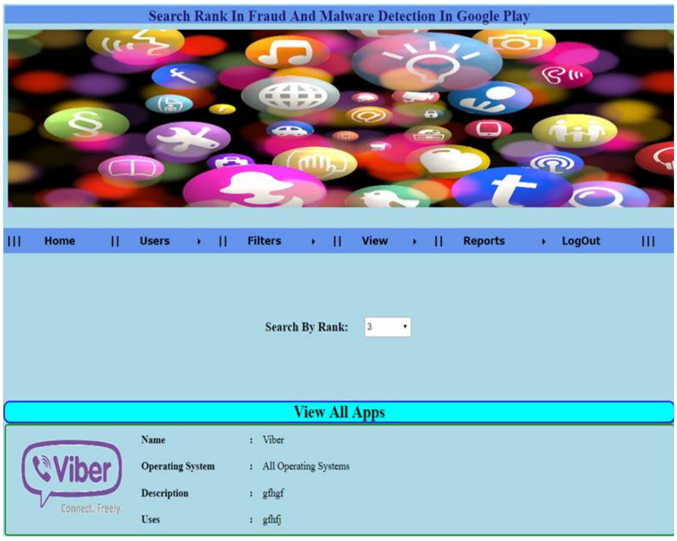
Name : Viber
Operating System : All Operating Systems
Description : gfhgf
Uses : gfhfj

Name : Myntra
Operating System : All Operating systems
Description : Online Shopping App
Uses : Online Shopping App



Filter Name:

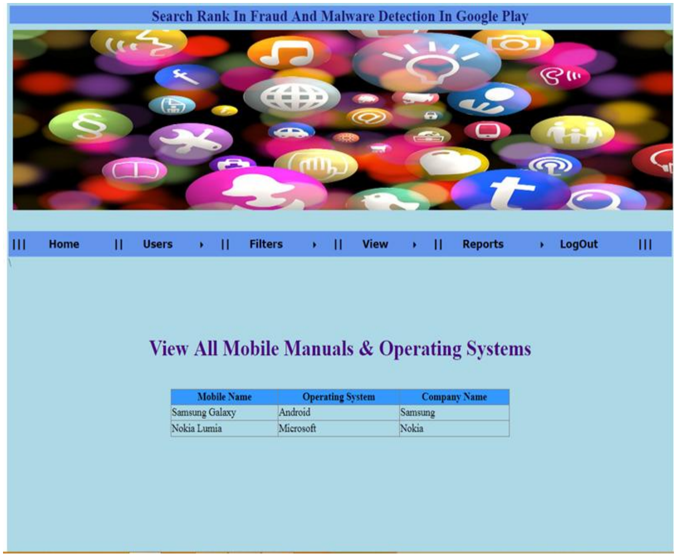
Id	Filter Name
1	AccuTrack
2	Ackposts
3	Acnetdoor
4	Adsms
5	Airpush/StopSMS
6	AnServer/Answerbo
7	Antares/Antammi
8	Arspam
9	AVPass
10	Badaccents



Search By Rank: 3

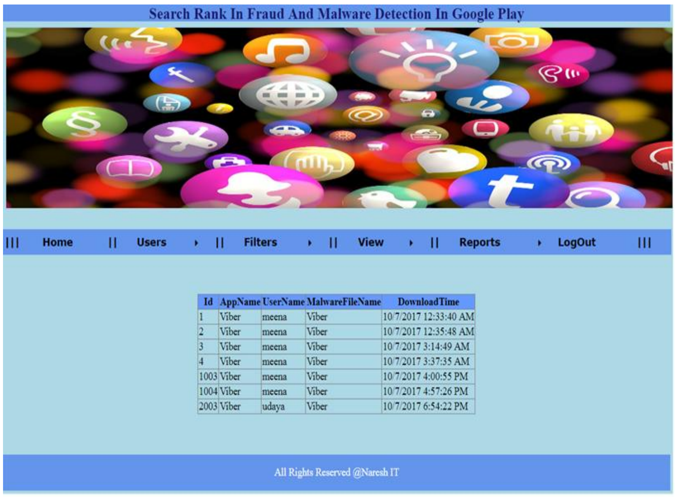
View All Apps

Name : Viber
Operating System : All Operating Systems
Description : gfhgf
Uses : gfhfj



View All Mobile Manuals & Operating Systems

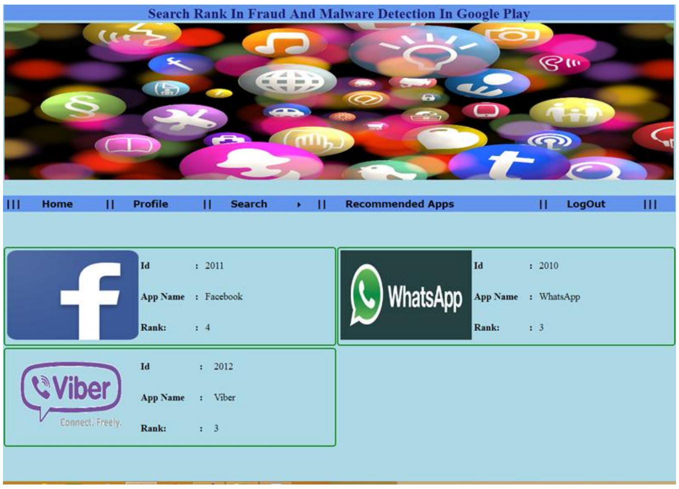
Mobile Name	Operating System	Company Name
Samsung Galaxy	Android	Samsung
Nokia Lumia	Microsoft	Nokia



Id	AppName	UserName	MalwareFileName	DownloadTime
1	Viber	meena	Viber	10/7/2017 12:33:40 AM
2	Viber	meena	Viber	10/7/2017 12:35:48 AM
3	Viber	meena	Viber	10/7/2017 3:14:49 AM
4	Viber	meena	Viber	10/7/2017 3:37:35 AM
1003	Viber	meena	Viber	10/7/2017 4:00:55 PM
1004	Viber	meena	Viber	10/7/2017 4:57:26 PM
2003	Viber	udaya	Viber	10/7/2017 6:54:22 PM

All Rights Reserved @Naresh IT

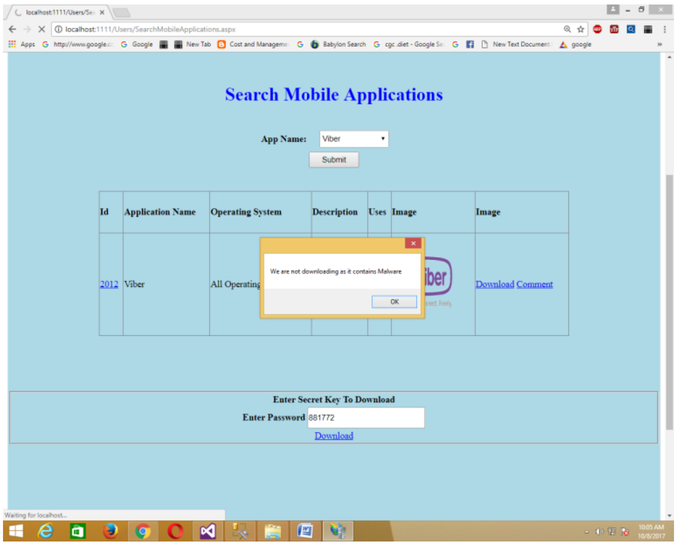
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal


Search Rank In Fraud And Malware Detection In Google Play
||| Home || Profile || Search || Recommended Apps || LogOut |||

Id	:	2011
App Name	:	Facebook
Rank:	:	4

Id	:	2010
App Name	:	WhatsApp
Rank:	:	3

Id	:	2012
App Name	:	Viber
Rank:	:	3



Search Mobile Applications

App Name: Viber

Submit

Id	Application Name	Operating System	Description	Uses	Image	Image
2012	Viber	All Operating				Download Comment

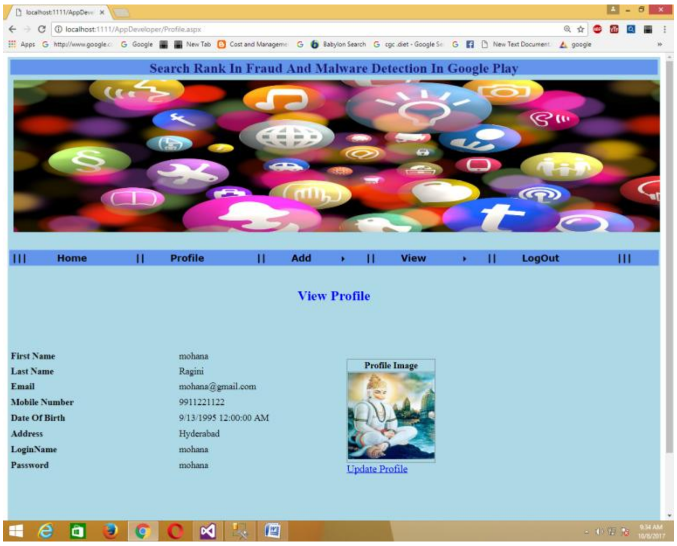
We are not downloading as it contains Malware

OK

Enter Secret Key To Download

Enter Password 881772

Download

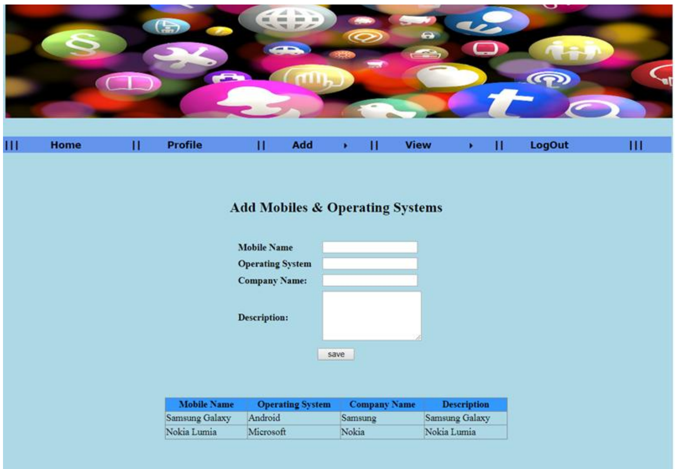

localhost:1111/AppDeveloper/Profile.aspx
Search Rank In Fraud And Malware Detection In Google Play
||| Home || Profile || Add || View || LogOut |||

View Profile

First Name	mohana
Last Name	Ragini
Email	mohana@gmail.com
Mobile Number	9911221122
Date Of Birth	9/13/1995 12:00:00 AM
Address	Hyderabad
LoginName	mohana
Password	mohana

Profile Image

Update Profile



Add Mobiles & Operating Systems

Mobile Name
Operating System
Company Name:
Description:

save

Mobile Name	Operating System	Company Name	Description
Samsung Galaxy	Android	Samsung	Samsung Galaxy
Nokia Lumia	Microsoft	Nokia	Nokia Lumia

Conclusion:

In this project we completed FairPlay, a system to detect both fraudulent and malware Google Play apps. Our experiments on a newly contributed longitudinal app dataset have shown that a high percentage of malware is involved in search rank fraud; both are accurately identified by FairPlay.

References:

[1] Google Play. [Online]. Available: https://play.google.com/

[2] E. Siegel, "Fake reviews in Google Play and Apple App Store,"Appentive, Seattle, WA, USA, 2014.

[3] Z. Miners. (2014, Feb. 19). "Report: Malware-infected Androidapps spike in the Google Play store," PC World. Available: http:// www.pcworld.com/article/2099421/reportmalwareinfectedandroid-apps-spike-in-the-google-play-store.html

[4] S. Mlot. (2014, Apr. 8). "Top Android App a Scam, Pulled From

GooglePlay,"PCMag.Available:http://www.pcmag.com/Article 2/0,2817,2456165,00.asp.

[5] D. Roberts. (2015, Jul. 8). "How to spot fake appsontheGooglePlaystore,"Fortune.Available:http://fortune.com/2015/07/08/google-play-fake-app/

[6] A. Greenberg (2012, May 23). "Researchers say they snuckmalware app past Google's 'Bouncer' Android market scanner,"Forbes Security, [Online]. Available:http://www.forbes.com/sites/andygreenberg/2012/05/23/researchers-say-they-snuckmalware-app-past-googles-bouncer-android-market-scanner/#52c8818d1041

[7].Freelancer.[Online].Available:http://www.freelancer.com

[8].BestAppPromotion. [Online]. Available: www.bestreviewapp.com/

[9].G. Wang, et al., "Serf and turf: Crowdturfing for fun and profit,"in Proc. ACM WWW, 2012. [Online]. Available: http://doi.acm.org/10.1145/2187836.2187928