1 International Conference on Information Technology, Computer and Telecommunication Engineering in Iran
اولین همایش بین المللی مهندسی فناوری اطلاعات کامپیوتر و مخابرات ایران
19 January 2020
۲۹ دی ماه ۱۳۹۸
www.ict.bcnf.ir

محاسبه ریسک های حریم خصوصی در جهت بهبود بکارگیری مجوزهای دسترسی در سیستم عامل اندروید

فخرالسادات نوری

دانشجوی کارشناسی ارشد موسسه آموزش عالی تعالی قم

دکتر عبدالرضا رسولی کناری

استادیار گروه کامپیوتر دانشگاه صنعتی قم

چکیده

امروزه بدلیل اینکه گوشی های هوشمند بخش جداناپذیری از زندگی هستند و بسیاری از اطلاعات شخصی افراد در گوشی هایشان است حفظ حریم خصوصی و دور ماندن این اطلاعات از دسترسی های ناخواسته مهم است.گرچه اقدامات امنیتی برای سیستم های تلفن همراه صورت گرفته است، اما این سیستم ها اغلب زمانیکه بر تصمیم گیری کاربران تکیه می کنند، شکست می خوردند. تحقیقات قبلی نشان می دهد که وابستگی به کاربران بی اثر است،زیرا کاربران قادر به درک مجوزهای مورد نیاز برنامه نیستند و چون برنامه های اندروید برای صحت عملکردشان نیاز به مجوز دسترسی و کنترل منابع مختلف دارند آگاهی نداشتن کاربران و اعطای مجوزهای نادانسته خطراتی دربر دارد.همچنین نبود روشی برای محاسبه ریسک بر اساس مجوزهای دسترسی، این خطرات را قوت می بخشد.

این مقاله روشی برای تحلیل مجوزهای اندروید بر اساس طبقه بندی به میزان ارتباطشان با فاش ساختن هویت کاربران می ارائه می دهد و برای هر برنامه ریسک احتمالی آن را بر اساس مجوزهای خطرناک انفرادی و ترکیبی محاسبه کرده و می تواند قیاسی برای امنیت برنامه ها باشد. همچنین با کمک منطق فازی به محاسبه ریسک برنامه های کاربردی اندروید می‌پردازد و نتایج قابل قبولی از ارزیابی آن ها نشان می‌دهد.

کلمات کلیدی: مجوزهای اندرویدی، منطق فازی، حریم خصوصی، امنیت، ریسک، مجوز، اندروید

۱- مقدمه

دستگاه های آندروید استفاده گسترده ای در زندگی شخصی و کسب و کار دارند. از کودکان تا سالمندان، تازه کاران تا کارشناسان، و در بسیاری از فرهنگ های مختلف در سراسر جهان، تنوع کاربر محور برای دستگاه های تلفن همراه وجود دارد.استفاده در همه جا از این دستگاه های تلفن همراه حالت جدیدی از حریم خصوصی و تهدیدات امنیتی بوجود اورده است.

آمارها بیانگر این مورد هستند که بیش از ۵۰ درصد از تمام گوشی های همراه در حال حاضر گوشی های هوشمند هستند، و این آمار برای سایردستگاه هایی مانند تبلت کامپیوترها که در حال اجرای سیستم عامل مشابه تلفن همراه هستند به حساب نمی آید[۱۳]. به گفته گوگل، بیش از ٤۰۰ میلیون دستگاه اندرویدی در سال های گذشته به تنهایی فعال شده اند. اکنون تعداد کاربران تجهیزات مبتنی بر اندروید در مقایسه با تجهیزات مبتنی بر ویندوز بیشتر است. در ماه مارس سال ۲۰۱۷ میلادی اندروید 37.39درصد از سهم بازار را به دست آورد که ۰,۰۲ درصد بیشتر از سهم ۳۷,۹۱ درصدی ویندوز است[۱۹].

با وجود این که اختلاف آمار مذکور بسیار اندک است، این وضعیت نشانه‌ای از پایان سلطه ویندوز بر بازار سیستم‌عامل‌ها و تغییر رفتار کاربران محسوب می‌شود. اما با گسترش روزافزون گوشی های هوشمند و تجهیزات موبایل در سطح جهان، استفاده از اینترنت در کامپیوترهای رومیزی رو به افول است و این می تواند شروعی برای آسیب رساندن به حریم خصوصی و سوء استفاده از اطلاعات ذخیره شده بر روی گوشی همراه اندروید باشد.

۲- مطالعات و کارهای مربوطه

تحقیقات پیشین انجام شده در این زمینه به سال های دوری برنمی گردد برای مثال در سال ۲۰۱۵ تالها و همکارانش، یک سیستم شناسایی بدافزار Android مبتنی بر مجوز به نام APK Auditor که از تجزیه و تحلیل استاتیک برای توصیف و طبقه بندی برنامه های آندروید به عنوان بی خطر یا مخرب استفاده می کند، پیشنهاد دادند[۱۶].

در همان سال چویی [۱]. و همکارانش گروه مجوزهای دسترسی را به ترتیب برای شناسایی کدهای مخرب بررسی کردند که مشکل نشت اطلاعات شخصی در محیط اندروید را با استفاده از روش کنترل دستیابی تصادفی در سیستم فایل معمولی آندروید از طریق نرم افزارهای مخرب جدید و یا کد های مخرب حل می کند. آن ها یک مدل کنترل دسترسی مبتنی بر استنتاج پیشنهاد کردند که می تواند برای دسترسی به امنیت پیشگیرانه استفاده شود و دقت بیشتری نسبت به دیگر تکنیک های تشخیص بدافزار دارد.

در سال ۲۰۱۶ نیز سوکولووا و همکارانش تحقیقی برمبنای تحلیل مجوزهای درخواستی هر طبقه انجام دادند[۱۴]. آن ها در این مطالعه یک روش برای توصیف رفتار طبیعی هر دسته از برنامه ها با برجسته کردن مجوزهای درخواستی مورد انتظار پیشنهاد دادند و مجوزهای مورد نیاز را به عنوان یک گراف مدل سازی کردند.

در سال ۲۰۱۸ شارما و همکارانش روشی به نام RNPDroid برای کاهش خطر با استفاده از تجزیه و تحلیل مجوز ها ارائه دادند[۵]. برای ارزیابی رویکرد پیشنهادی از مجموعه داده M0Droid که شامل ۴۰۰ نمونه برنامه کاربردی اندروید می باشد، استفاده شده است. M0Droid ابزاری برای شناسایی الگوی رفتاری برنامه ها و طبقه بندی آن ها است. تمام مجوزهای نمونه های به دست آمده از طریق مهندسی معکوس تجزیه و تحلیل شده و در مجموع ۱۶۵ مجوز می باشد.

همچنین در ۲۰۱۸ ژانگ روشی برای کمک به کاربران نهایی برای تصمیم گیری آگاهانه قبل از نصب ارائه داد [۶]. این تحقیق از تجزیه و تحلیل حساسیت و تشخیص اینکه آیا درخواست ها برای دسترسی به منابع و داده ها در عملکرد برنامه کاربردی مورد نیاز و ضروری است یا نه، استفاده می کند. برای این کار سیستم مبتنی بر ابر Privet، برای پوشش و ارزیابی ریسک حریم خصوصی خودکار طراحی شده است.

در ۲۰۱۹ سانگبونگ و همکارانش برنامه تحلیلی EZADroid به عنوان عامل تصمیم گیرنده برای محاسبه ریسک و میزان خطر ۵۰۰۰ برنامه اندرویدی را ارائه کردند که در این روش محاسبه ریسک با تمرکز بر استفاده از مجوزهای اندروید و تکنیک AHP انجام گرفته است [۱۰].

در نهایت، این مطالعه یک رتبه حفظ حریم خصوصی و یک آستانه هشدار خطر بر اساس بهترین معیارهای کارایی برای برنامه ها ارائه می دهد.

۳- بیان مسئله

امنیت اطلاعات و حفظ حریم خصوصی تمام انواع دستگاه های الکترونیکی مسائله ای برای کاربران است. اما کاربران تلفن های هوشمند در رابطه با حفظ حریم خصوصی تلفن خود بیشتر از کامپیوترشان نگران هستند. آنها به خصوص در مورد خطر برنامه های مخرب و عدم درک هدف مجوزها نگرانند. تجزیه و تحلیل بیش از ۱ میلیون برنامه در سیستم عامل آندروید گوگل نشان می دهد که هر برنامه بطور متوسط درخواست پنج مجوز را دارد[۱۲]. این بدان معنی است که دسترسی هر برنامه که اجازه اجرا بر روی دستگاه بصورت بالقوه را دارا است توانایی ضربه زدن به جنبه های خاصی از اطلاعات را دارد. با وجود این نیاز، مطالعات مختلف امنیتی و اقدامات حفظ حریم خصوصی قابلیت استفاده تقریبا ناکارای خود را نشان داده اند که اغلب با مقاومت کاربران مواجه می شوند. برخی کارها نیز در زمینه کمک به فهم کاربران از مجوزهای درخواستی نیز صورت گرفته است اگرچه استفاده از مکانیسم امنیتی در متون بیشتر از پلت فرم های موبایل مورد توجه است[۳].

بنابراین نبود روشی برای محاسبه ریسک بر اساس مجوزهای دسترسی خطرزا و اولویت های امنیتی کاربر ، خطرات برنامه های

مخرب را قوت می بخشد. همچنین علاوه بر مجوزهای انفرادی، مجوزهای ترکیبی که از مجموع چندین مجوز انفرادی خطرناک تشکیل شده اند می توانند به ریسک بالای حریم خصوصی نیز منجر شوند. در نهایت وجود روشی منطقی فازی برای محاسبه ریسک که قوانینش بر اساس انواع مجوزهای برنامه های کاربردی، نظر کاربر و گروه بندی مجوزهای خطرزا استوار باشد به تصمیم گیری بهتر کاربر کمک خواهد کرد.

پژوهش حاضر با تمرکز بر روی پلت فرم آندروید، به دلیل باز بودن و محبوبیت آن و دسترسی به منابع حساس است. این تحقیق ابتدا به بررسی کل مجوزهای ممکن در سیستم عامل اندروید پرداختیه و در مجموع ۲۷٤ مجوز که نزدیک به ۵۱ عدد از آن ها بر اساس دسترسی شان به منابع، خطرناک محسوب می شوند، یافت شد[۲٦]. از میان این ۵۱ مجوز ۳٦ عدد مربوط به مجوزهای حریم خصوصی بودند که در ٤ گروه مجوزهای انفرادی با ریسک بالا، متوسط، پایین و خیلی پایین طبقه بندی شدند. این طبقه بندی بر اساس میزان ارتباط این مجوزها با فاش سازی هویت کاربر دستگاه اندروید می باشد، که هر چه بیشتر در این زمینه تاثیرگذار باشد در گروه ریسک بالاتری قرار می گیرد. از ترکیب مجوزهای انفرادی و دسترسی بدون محدودیت به اینترنت، مجوزهای ترکیبی خطرناک حاصل می شوند که در ٤ گروه ریسک خیلی بالا، بالا، متوسط و پایین جای می گیرند. مجوزهای ۲۰ برنامه کاربردی که درصدر جدول برترین ها بودند[۲۰]. بررسی شده و بر اساس مجوزهای خطرزا میزان ریسک اولیه هر یک محاسبه گردیده است. در نهایت با کمک منطق فازی و لحاظ کردن مجوزهای درخواستی، اولویت های کاربر و درجه ریسک تقریبی برنامه ها بر طبق جدول های حاصله ریسک نهایی آنان محاسبه می گردد.

برای این کار دو سیستم خبره یکی برای مجوزهای انفرادی و دیگری برای مجوزهای ترکیبی طراحی شد و سیستم خبره سومی ریسک نهایی برنامه را مشخص می نماید. با کمک سیستم های خبره طراحی شده، محاسبه ریسک برای هر برنامه ی کاربردی بر اساس مجوزهای درخواستی اش امکان پذیر می باشد. همچنین علاوه بر طراحی سیستم خبره سوم به کمک شبیه ساز متلب، نمونه ای طراحی و شبیه سازی شده که محاسبه ریسک نهایی را با سرعت و سهولت بیشتری انجام می دهد.

٤- بررسی ریسک های حریم خصوصی بر اساس مجوزهای دسترسی

اگرچه حریم خصوصی موضوعی قابل درک و ساده است اما تعریف آن برای افراد مختلف، متفاوت است. بعضی ها تنها دسترسی به حاظه جانبی و گالری را نوعی تهاجم به حریم خصوصی می دانند و بعضی دیگر حتی در مورد اطلاعات تاریخچه مرورگر یا تقویم خود نیز حساسند. این موضوع باعث شد در کنار طبقه بندی مجوزهای درخواستی برنامه ها برحسب ارتباط آن ها با انتشار هویت صاحب دستگاه [8]. نظرات کاربر را نیز برای محاسبه ریسک لحاظ شود. مجوزهای خطرناک بر اساس معرفی مرجع androiddeveloper [27]. آمده است.

در این تحقیق از دو روش محاسبه ریسک بر اساس میانگین جدول ضرایب و دیگری استفاده از سیستم خبره فازی برای محاسبه ریسک استفاده شده است. جدول زیر طبقه بندی مجوزها را بر اساس میزان ارتباط با افشای هویت کاربر را نشان می دهد:

جدول ۱: طبقه بندی مجوزها بر اساس میزان ارتباط با افشای هویت کاربر[8].

ضریب اهمیت	مجوزها
٤	خواندن وضعیت تلفن و شناسه، خواندن پروفایل، سنسور بدن
۳	تصدیق حساب کاربری(ایجاد حساب کاربری)، یافتن حساب کاربری، استفاده از حساب ها
۲	پردازش تماس های خروجی (خواندن کارت تماس)، تماس مستقیم با شماره ها، خواندن گزارش تماس، نوشتن گزارش تماس، خواندن مخاطبان، اصلاح (نوشتن) مخاطبان، خواندن حافظه خارجی، نوشتن در حافظه خارجی، خواندن پیام، دریافت پیام sms، دریافت پیام mms، ارسال پیام، خواندن جریان اجتماعی، ضبط صدا، دوربین
۱	دسترسی به مکان تقریبی، دسترسی به مکان دقیق، دسترسی به وضعیت شبکه، دسترسی به وضعیت wi-fi، مدیریت بلوتوث، گرفتن وظایف، خواندن تقویم، نوشتن یا اصلاح تقویم، خواندن تاریخچه نشانه گذاری ها، خواندن تاریخچه، خواندن دیکشنری کاربر، خواندن فید، دریافت wap push، Voicemail، Sip

٤-۱- محاسبه ریسک بر اساس جدول ضرایب

این روش شامل بررسی لیست مجوزها و امتیازات درخواستی هر برنامه است که پس از بررسی لیست و ارزیابی آنان، مجوزهای درخواستی خطرزای برنامه کاربردی طبق گروه بندی مجوزها مشخص می شود. سپس بر اساس ضرایب اختصاص یافته به هر گروه از مجوزها ریسک اولیه به ازای هر برنامه کاربردی تعیین می گردد. در آخر ریسک نهایی در این روش با کمک میانگین گیری از ریسک های حاصله بر اساس مجوزهای انفرادی و ترکیبی بدست می آید. فرمول محاسبه ریسک در این روش در زیر آمده است:

ریسک= مجموع ضرایب حاصله از بررسی مجوزهای خطرناک برنامه کاربردی / ۲

در این تحقیق مجوزهای انفرادی و مجوزهای ترکیبی که امکان آسیب رساندن به حریم خصوصی یا عملکرد عادی دستگاه را داشتند به چهار گروه تقسیم شده و به هر گروه ضریب اهمیت (درجه ریسک) تخصیص داده شده است.

رویکرد این تحقیق در طبقه بندی مجوزها بر اساس پتانسیل و توانایی آن ها برای دسترسی، جمع آوری و خارج کردن داده ها از دستگاه موبایل است. و در ارتباط با برخورد منتشرکننده یا توسعه دهنده برنامه کاربردی بعد از جمع آوری داده ها سه مورد وجود دارد و اینست که چگونه با داده ها در مرحله ذخیره، پردازش و انتقال در جهت حفظ حریم خصوصی برخورد خواهند کرد.

شبه کد زیر روش یاد شده در این مقاله را نشان می دهد:

```
1  privacyImpact = ۰
2  for all requestedPermissions{
3        if requestedPermission is in harmfulPermissionsI۱
4              privacyImpact += ٤
5        if requestedPermission is in harmfulPermissionsI۲
6              privacyImpact += ۳
7        if requestedPermission is in harmfulPermissionsI۳
8              privacyImpact += ۲
```

```
9       if requestedPermission is in harmfulPermissionsI٤
10        privacyImpact += ١
11   if application demands internet permission {
12      if requestedPermission is in harmfulPermissionsC١
13        privacyImpact += ٥
14      if requestedPermission is in harmfulPermissionsC٢
15        privacyImpact += ٤
16      if requestedPermission is in harmfulPermissionsC٣
17        privacyImpact += ٣
18      if requestedPermission is in harmfulPermissionsC٤
19        privacyImpact += ٢  } }
20  risk = privacyImpact / ٢
```

٤-٢- محاسبه ریسک بر اساس سیستم منطق فازی

این روش با طراحی دو سیستم خبره میزان ریسک بر اساس مجوزهای انفرادی و ترکیبی را می سنجد. در هر سیستم ورودی ها عبارتند از درجه ریسک برنامه بر مبنای ضرایب جداول دسته بندی مجوزها، نظر کاربر و ٤ گروه طبقه بندی مجوزها.

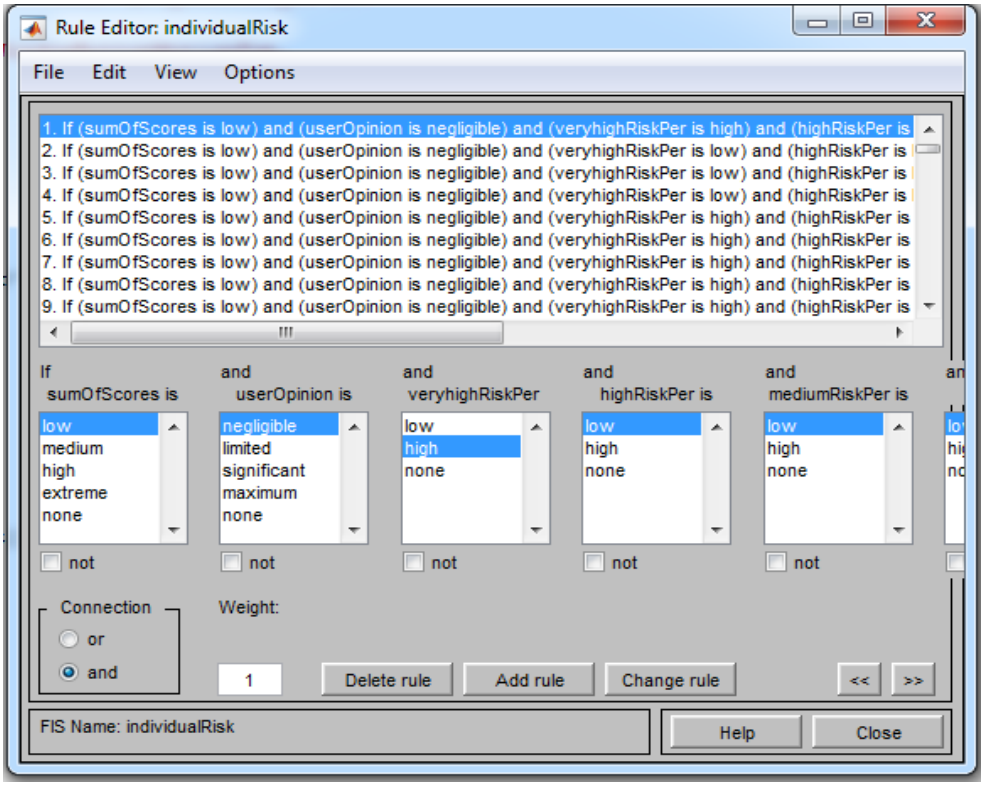
دو سیستم خبره یکی برای مجوزهای انفرادی و دیگری برای محاسبه ریسک مجوزهای ترکیبی امکان محاسبه ریسک نهایی برنامه کاربردی را فراهم می کند.

سیستم خبره فازی برای حل مسئله مطرح شده با بهره‌گیری از روش استنتاج ممدانی که متغییرهای ورودی و خروجی این روش فازی هستند و فازی زدایی خروجی به روش مرکز ثقل ارائه شده است. همچنین توابع عضویت ورودی و خروجی مثلثی می باشند که از سه پارامتر کران بالا، کران پایین و محتمل ترین مقدار تشکیل شده اند.

تعیین قوانین با استفاده از درجه ریسک محاسبه شده اولیه، نظر کاربر برنامه اندرویدی و اینکه هر برنامه اندرویدی به چه میزان از هریک از چهار گروه طبقه بندی شده مجوزها استفاده می کند، انجام گرفته است و ریسک انفرادی و ترکیبی برای هر سیستم بطور جداگانه بر طبق این قوانین تعیین می گردد

از ترکیب این سه شاخص قوانینی برای محاسبه ریسک انفرادی و ترکیبی برای هر سیستم بطور جداگانه تعیین می گردد.

برای مثال اگر مجموع ضرایب یک برنامه اندرویدی و میزان دسترسی به مجوزهای پرخطر، پایین باشد و از نظر کاربر دسترسی برنامه به مجوزهای موردنیازش بی اهمیت باشد ریسک برنامه پایین در نظر گرفته میشود ولی اگر همین برنامه با مجموع ضرایب و دسترسی کم ، مجوزهایی را درخواست کند که از نظر کاربر به اطلاعات حساسی دست می یابد، ریسک برنامه بالا در نظر گرفته میشود. شکل زیر نمایی از قوانین دو سیستم خبره انفرادی و ترکیبی است:



شکل ۱- قوانین سیستم خبره طراحی شده برای محاسبه ریسک بر اساس مجوزهای انفرادی و ترکیبی

می توان گفت نظر کاربر اولویت بالایی در طراحی این سیستم خبره داشته است و تنها در جایی که مجموع ضرایب ریسک بسیار بالا باشد نظر کاربر در اولویت پایین تر قرار می گیرد.

جمع آوری نظرات کاربران در مورد اولویت و میزان اهمیت هر یک از چهار گروه مجوز خطرناک معرفی شده با استفاده از پرسش نامه ای که شدت تاثیر سناریوی تهدید را نشان می دهد سنجیده می گردد.

قوانین سیستم فازی برای مجوزهای انفرادی و ترکیبی مشابه یکدیگرند و تنها نام گروه مجوزها با یکدیگر تفاوت دارند.

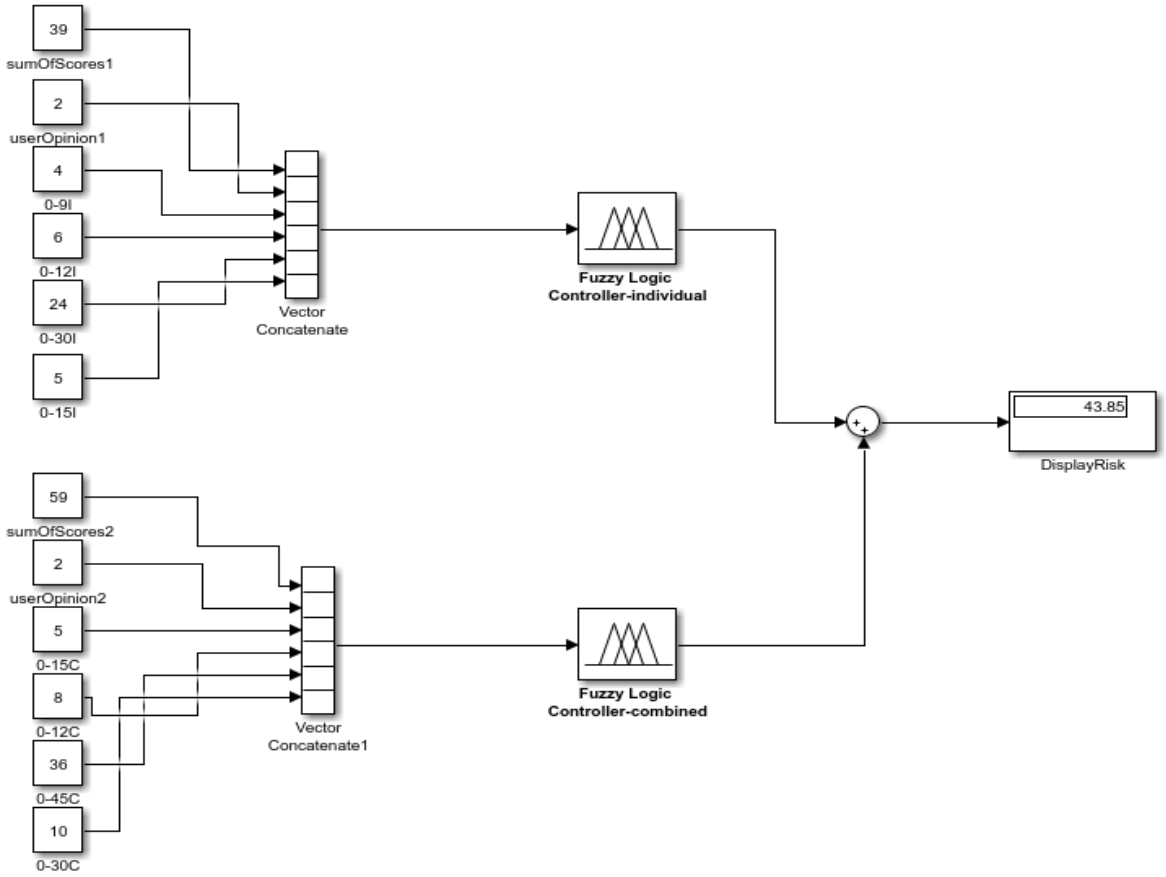
علاوه بر طراحی سیستم خبره برای محاسبه ریسک نهایی که از مجموع ریسک های انفرادی و ترکیبی بدست می آید با کمک شبیه ساز متلب به طراحی نمونه ای برای محاسبه ریسک پرداخته شده است. این شبیه ساز با استفاده از منطق فازی دو سیستم خبره طراحی شده برای ریسک انفرادی و ترکیبی و گرفتن ورودی قادر به محاسبه و نمایش ریسک نهایی می باشد.

این نمونه شبیه سازی شده از دوازده ثابت ورودی (constant) به همراه دو fuzzy logic controller متصل به دو سیستم خبره فازی طراحی شده برای محاسبه ریسک انفرادی و ترکیبی و دو vector concatenate و یک جمع کننده و صفحه نمایشی برای نمایش میزان ریسک نهایی تشکیل شده است.

استفاده از شبیه ساز به درک و مشاهده بهتر کل سیستم بصورت یکپارچه کمک کرده و با کمک آن می توان محاسبه ریسک نهایی را بسرعت انجام داد. شکل ۲ نمایی از شبیه ساز طراحی شده را نشان می دهد.

۵- اجرا و ارزیابی

در این تحقیق ۲۰ عدد از برترین برنامه های یک مارکت موبایل ایرانی را که بر اساس تعداد دانلود و میزان محبوبیت برنامه در تابستان ۹۶ در صدر جدول برنامه ها بودند برای بررسی و ارزیابی مجوزها بعنوان مجموعه داده انتخاب گردیدند[20].



شکل ۲- سیستم فازی شبیه سازی شده برای محاسبه ریسک

۵-۱- محاسبه ریسک برنامه های منتخب

پس از استخراج کلیه مجوزهای این ۲۰ برنامه و طبقه بندی مجوزهای خطرزای آنان بر طبق گروه بندی مجوزها ، مجموع ضرایب آن ها بر اساس ضریب های تخصیص داده شده به هر گروه مجوز، محاسبه شد و اطلاعات مربوط به آنان در جدول ۲ آمده است:

جدول ۲- اطلاعات مربوط به ۲۰ برنامه منتخب

نام برنامه های کاربردی	تعداد کل مجوزها	تعداد مجوزهای خطرناک	مجموع ضرایب مجوزهای انفرادی خطرناک	مجموع ضرایب مجوزهای ترکیبی خطرناک	تعداد دانلودها	تعداد ستاره های برنامه(محبوبیت از ۰ تا ۵)
Telegram	۳٤	۲۰	۳۹	۵۹	۱٦,۰۰۰,۰۰۰	٤
Instagram	۲۱	۱۲	۲٦	۳۸	۱۷,۰۰۰,۰۰۰	٤
Mobogram	۳۲	۱٦	۳۱	٤۷	۱,۰۰۰,۰۰۰	٤
Share it	۳۰	۱۳	۲۷	٤۰	۲۱,۰۰۰,۰۰۰	۵
Divar	۱۹	۹	۱۷	۲٦	۱۲,۰۰۰,۰۰۰	٤
ایرانسل من	۸	٤	۹	۱۳	۵,۰۰۰,۰۰۰	٤
Snapp	۱٦	۹	۱۹	۲۸	٤,۰۰۰,۰۰۰	۵
تقویم باد صبا	۱٤	۹	۱٤	۲۳	۸,۰۰۰,۰۰۰	۵
Zapya	۲۷	۱۳	۲۷	٤۰	۷,۰۰۰,۰۰۰	۵
Mx player	۱۲	۵	۷	۱۲	۸,۰۰۰,۰۰۰	۵
آپ	۱۵	۹	۱۹	۲۸	۳,۰۰۰,۰۰۰	٤
تلگرام فارسی	۲۸	۱۵	۳۰	٤۵	۲,۰۰۰,۰۰۰	٤
آپارات	۱۲	۵	۱۰	۱۵	٤,۰۰۰,۰۰۰	٤
همراه من	۸	٤	۹	۱۳	۲,۰۰۰,۰۰۰	۳
شیپور	۱۲	۸	۱۵	۲۳	۳,۰۰۰,۰۰۰	٤
تلوبیون	۱۱	۵	۷	۸	۳,۰۰۰,۰۰۰	۵
جعبه ابزار	۲۲	۱۲	۲۳	۳۵	٦,۰۰۰,۰۰۰	۵
B612	۱٤	۹	۱۷	۲٦	۳,۰۰۰,۰۰۰	٤
Plus messenger	۳۳	۱۹	۳۷	۵٦	۲,۰۰۰,۰۰۰	٤
موبوگرام دوم	۳۲	۱٦	۳۱	٤۷	۱,۰۰۰,۰۰۰	٤

در جدول بالا اطلاعاتی از قبیل تعداد مجوزها، مجموع ضرایب، تعداد دانلود و میزان محبوبیت برنامه ها آمده است. در این میان telegram با ۳٤ مجوز و ۲۰ مجوز خطرناک بعنوان خطرزاترین برنامه و ایرانسل من و همراه من به اتفاق با ۸ مجوز و ٤ مجوز خطرناک کم خطرترین برنامه می باشند. همچنین share it با ۲۱میلیون دانلود و ۵ ستاره محبوب ترین برنامه است در حالیکه موبوگرام دوم با ۱ میلیون دانلود دارای کمترین میزان دانلود می باشد. حال با استفاده از فرمول محاسبه ریسک آمده در قسمت "محاسبه ریسک بر اساس جدول ضرایب" و سیستم خبره فازی ریسک برنامه ها محاسبه می گردد:

جدول ۳- محاسبه ریسک ۲۰ برنامه منتخب با استفاده از دو روش میانگین ضرایب و سیستم خبره فازی

نام برنامه	میزان ریسک محاسبه شده بر اساس میانگین ضرایب	برچسب ریسک	میزان ریسک محاسبه شده بر اساس سیستم خبره	برچسب ریسک
Telegram	49	بالا	٤٣,٨٥	بالا
Instagram	32	محدود	٤١	محدود
Mobogram	39	محدود	٤٢	بالا
Shareit	33.5	محدود	٣٧,٣٢	محدود
Divar	21.5	محدود	٢٦,٩٣	محدود
ایرانسل من	11	بی اهمیت	١١,٦	بی اهمیت
Snapp	23.5	محدود	٢٧,٢٦	محدود
تقویم باد صبا	18.5	بی اهمیت	١٢,٤٣	بی اهمیت
Zapya	33.5	محدود	٣٩,٧	محدود
Mx player	9.5	بی اهمیت	١٠,٥٥	بی اهمیت
آپ	23.5	محدود	١١,٦	بی اهمیت
تلگرام فارسی	37.5	محدود	٤٢	بالا
آپارات	12.5	بی اهمیت	١١,٦	بی اهمیت
همراه من	11	بی اهمیت	١١,٦	بی اهمیت
شیپور	19	بی اهمیت	١١,٦	بی اهمیت
تلوبیون	7.5	بی اهمیت	١٠,٥٥	بی اهمیت
جعبه ابزار	29	محدود	١٧,٧	بی اهمیت
B612	21.5	محدود	١١,٦	بی اهمیت
Plus messenger	46.5	بالا	٤٢,٠٦	بالا
موبوگرام دوم	39	محدود	٤٢	بالا

بر اساس ارقام بدست آمده با کمک جدول ضرایب بالاترین ریسک محاسبه شده با مقدار ٤٩ مربوط به Telegram و پایین ترین ریسک با مقدار ۹,۵ متعلق به برنامه Mx player می باشد. از آنجایی که Telegram در حین نصب، مجوزهای بسیاری از گروه مجوزهای خطرناک انفرادی و ترکیبی درخواست می کند ریسک نصب بالایی دارد. بر مبنای برچسب گزاری میزان ریسک ها در روش میانگین مجموع ضرایب، ۲ برنامه دارای ریسک بالا، ۱۱ برنامه با ریسک محدود و ۷ برنامه ریسک محاسبه شده برایشان بی اهمیت بود. در بین برنامه های بررسی شده بر اساس جدول ضرایب هیچ برنامه ای دارای ریسک خیلی بالا نبود.

در ریسک محاسبه شده با استفاده از سیستم های خبره فازی همچنان Telegram با مقدار عددی ریسک ٤٣,٨٥ بالاترین میزان

ریسک را به خود اختصاص داده است و Mx player با ریسک ۱۰,۵۵ پایین ترین ریسک موجود را دارا می باشد. در این روش ۵ برنامه دارای ریسک بالا، ۵ برنامه دارای ریسک محدود و ۱۰ برنامه ریسک بی اهمیتی داشتند.

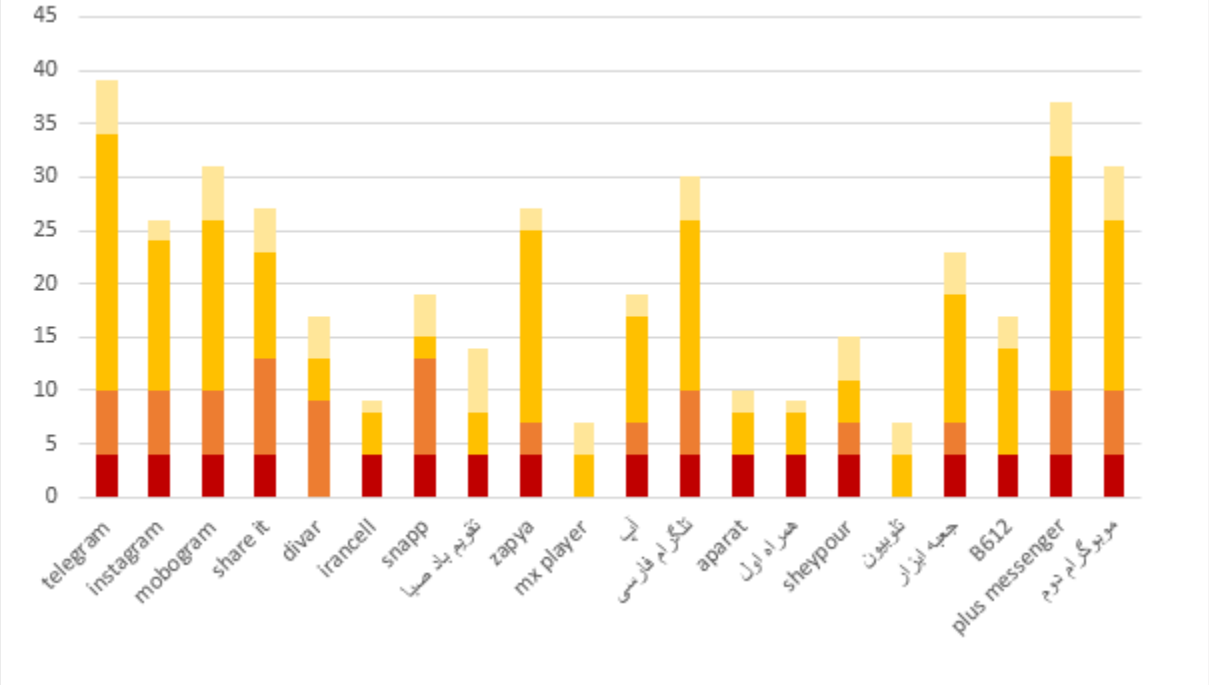
جدول ٤ پر تکرارترین مجوز ها را در بین ۲۰ برنامه نشان می دهد. در میان برنامه های منتخب همگی آنان درخواست دسترسی به وضعیت شبکه و دسترسی بدون محدودیت به اینترنت را داشتند.۱۷ برنامه درخواست دسترسی به خواندن وضعیت تلفن و خواندن و نوشتن اطلاعات حافظه خارجی را می کردند در این میان ۱۳ برنامه مجوز یافتن حساب ها را می خواستند. جدول زیر از بین ۲۰ برنامه مجوزهای خطرناک دارای بیشترین فراوانی را نشان می دهد.تمامی این برنامه ها تقاضای دسترسی بدون محدودیت به اینترنت را نیز داشتند.

جدول ٤- مجوز خطرزای دارای بیشترین استفاده

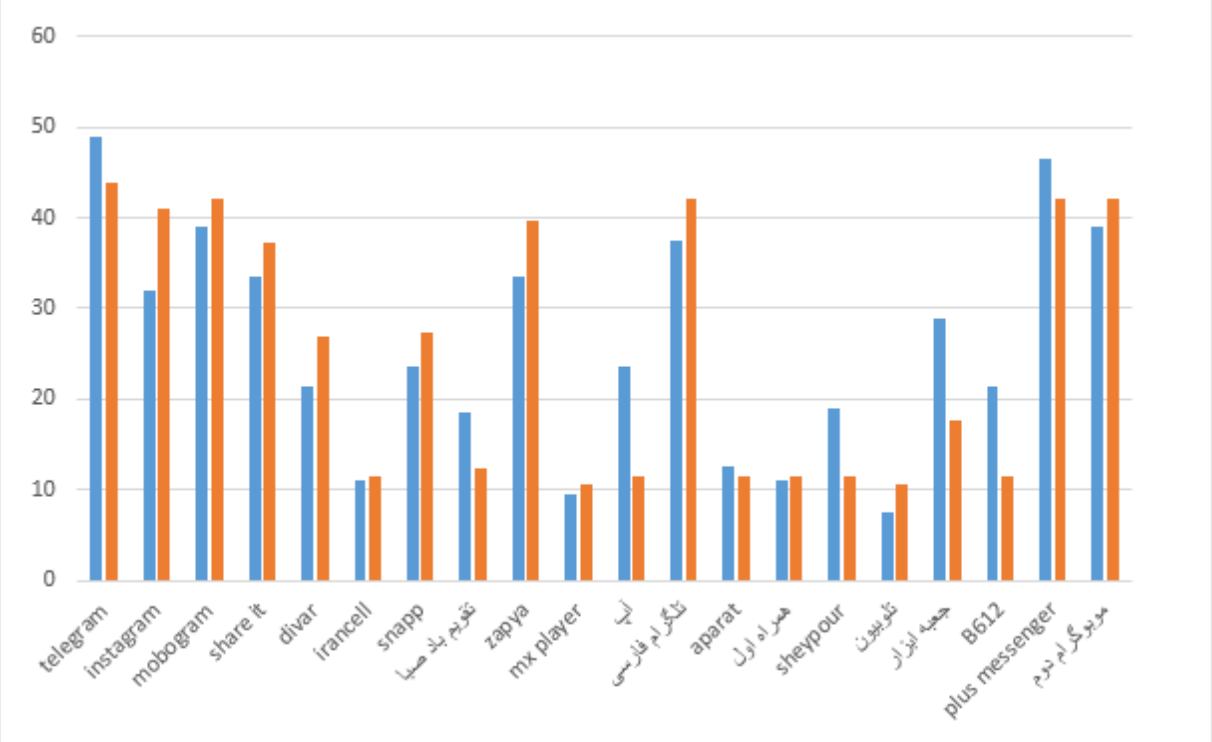
نام مجوز	میزان فراوانی
خواندن وضعیت تلفن و شناسه	٪۸۵
یافتن حساب ها در دستگاه	٪٦۵
تغییر یا حذف محتویات کارت حافظه	٪۸۵
خواندن کارت حافظه	٪۸۵
مشاهده اتصالات شبکه	٪۱۰۰

نمودار شکل ۳ میزان استفاده ۲۰ برنامه منتخب را به تفکیک ٤ گروه بندی مجوزهای خطرزا نشان می دهد. رنگ قرمز نمایانگر اولین گروه مجوزها که اطلاعات حساس را در برداشتند، است. رنگ نارنجی مجوزهای گروه دوم که اطلاعات شخصی مهم را شامل می شدند، می باشد. رنگ زرد گروه سوم مجوزها که دسترسی به اطلاعات شخصی کمتر حساس را درخواست می دادند، میباشد و رنگ کرم نشانگر گروه چهارم مجوزها که به اطلاعات مکانی،وضعیت اینترنت،تاریخچه و دیگر موارد دسترسی داشتند، است.

نمودار شکل ٤ میزان مطابقت ریسک محاسبه شده بر مبنای میانگین ضرایب مجوزها و سیستم خبره فازی را به شکل میله ای نشان می دهد. رنگ آبی میزان ریسک بدست آمده با کمک روش منطق فازی و رنگ نارنجی نشانگر ریسک محاسبه شده با کمک روش مجموع ضرایب خطرناک می باشد. ریسک محاسبه شده برای اغلب برنامه ها به هم نزدیک و با یکدیگر تطابق دارند.



شکل ۳- نمودار تفکیک میزان استفاده هر برنامه از مجوزهای خطرزا



شکل ٤- نمودار مقایسه ریسک بر مبنای سیستم های خبره و ریسک بر مبنای میانگین ضرایب مجوزهای خطرزا

٦- بررسی نتایج

همانطور که در جدول شماره ۳ آمد ریسک ۲۰ برنامه برتر انتخاب شده، محاسبه گردید. برای اثبات صحت نتایج گزارش شده برنامه های انتخابی برای مثال دو برنامه Telegram و Plus messenger که با استفاده از هر دو روش میانگین مجموع ضرایب مجوزها و سیستم های خبره فازی بدلیل مجوزهای درخواستی خطرزای بسیار، دارای ریسک نصب بالایی بودند بررسی می شود. این دو برنامه پیام رسان و Plus messenger نسخه غیر رسمی Telegram می باشد که از ابتدای ظهورشان طبق گزارشات بعلت نداشتن رمزنگاری پیش فرض و استفاده از پروتکل تغییر یافته MTProto که در مورد آن شفاف سازی وجود ندارد و همچنین ذخیره پیام های کاربران بر روی سرورهای شرکت سازنده ، متخصصین امنیت به خطرزا بودن این برنامه و حذف آن از دستگاه های همراه تاکید می کردند[23]. در این مقاله با بررسی مجوزهای درخواستی این دو برنامه که امنیت آن ها از گذشته زیر سوال بوده است ابعاد جدیدی از مشکلات امنیتی آن ها نشان داده شد.

همچنین برای تعیین صحت روش معرفی شده محاسبه ریسک برای برنامه های کاربردی از طریق میانگین مجموع ضرایب مجوزهای خطرزا و سیستم خبره فازی طراحی شده با استفاده از گزارش آمده در سایت خبری کلارک مبنی بر معرفی ٤٤ برنامه مخرب راه یافته به گوگل پلی، ۸ برنامه از میان آنان انتخاب شد[۲۱].اطلاعات مربوط به برنامه های مخرب گزارش شده و ریسک محاسبه شده آنان با استفاده از دو روش میانگین مجموع ضرایب و سیستم خبره طراحی شده در جدول ۵ آمده است. ریسک تمام برنامه های مخرب گزارش شده با کمک روش مجموع ضرایب، جزو بالاترین گروه ریسک ها با برچسب "خیلی بالا" قرار گرفت و با توجه به روش یاد شده در این تحقیق، این برنامه ها با توجه به مجوزهای درخواستی شان از ریسک بالایی برخوردارند.

درنتیجه نشان داده شد که دو روش یاد شده در این پژوهش در نشان دادن برنامه هایی که دارای مجوزهای تهاجمی و خطرزا هستند، تواناست و تمامی برنامه هایی که مخرب گزارش شده اند در سیستم طراحی شده ما نیز خطرزا تشخیص داده شدند.

۷- نتیجه گیری و کارهای پیشنهادی آینده

روش های بسیاری برای محاسبه ریسک نصب برنامه های کاربردی بر روی دستگاه های موبایل تاکنون پیشنهاد شده است که دشواری این مسیر را نشان می دهد. برای مثال پاندیتا از تکنیک پردازش زبان طبیعی و شناسایی توضیحات مجوزها استفاده کرد، اما این روش تنها تعداد فراخوانی مجوزها را در هر برنامه بررسی می کرد و ریسک برنامه را محاسبه نمی کرد[9].

متد دیگری توسط اس گیت برای تخصیص درجه ریسک به هر برنامه پیشنهاد شد که تنها یک روش گرافیکی بدون در نظر گرفتن روش محاسبه ریسک بود[12] .

تالها نیز سیستم تشخیص مخرب های اندروید بر اساس مجوزی را برای تجزیه و تحلیل استاتیک و توصیف و طبقه بندی برنامه های اندروید مطرح کرد ولی به علت عدم ارزیابی جامع و داشتن وابستگی های خارجی، کارآمد نبود[16] .

اما می توان گفت در این تحقیق با کمک دو روش میانگین مجموع ضرایب و طراحی سیستم خبره فازی امکان محاسبه ریسک تمامی برنامه های کاربردی بدون پیچیدگی مدل سازی امکان پذیر است.

اگرچه نمی توان گفت اگر برنامه ای درجه ریسک بالا و توانایی خواندن، نوشتن، ایجاد یا حذف اطلاعات را دارد ضرورتا و یقینا خطرناک است اما می تواند برای کاربر مضر باشد. میزان ریسک محاسبه شده در این تحقیق نشان دهنده حداکثر میزان پتانسیل ریسک برای هر برنامه کاربردی است.در واقع اینکه آیا مجوزهای یک برنامه بیش از حد تهاجمی است یا نه ممکن است به اولویت های حفظ حریم خصوصی کاربر بستگی دارد.

انتظار می‌رود که با اضافه کردن متریک ریسک به خلاصه اطلاعات اولیه برنامه های کاربردی در هنگام نصب و اگاه کردن کاربران در مورد نگهداری از حریم خصوصی و اطلاعات شخصی ذخیره شده خود بر روی دستگاه موبایل باعث تغییرات مثبت در اکوسیستم برنامه ها شود. هنگامی که کاربران برنامه های کم ریسک

تر را ترجیح می دهند، توسعه دهندگان نیز بیشتر به اصل حداقل امتیاز و درخواست مجوزهای مورد نیاز خود تشویق می شوند.

همچنین ممکن است که مقدمه ای از درجه ریسک باعث شود کاربران بیشتر به برای برنامه های کم خطر بپردازند .بدین ترتیب، این باعث ایجاد انگیزه ای در توسعه دهندگان برای ایجاد برنامه های کم ریسک تر که حاوی مجوزهای تهاجمی و به طور کلی مجوز بیش از نیاز نباشند می شود.

بعنوان تحقیقات آتی می توان از ترکیب بیش از دو مجوز برای ساخت مجوزهای ترکیبی استفاده کرد. همچنین پژوهش کنونی تنها برای سیستم عامل اندروید مطرح شده است ولی امکان ارتقاء و استفاده از آن برای سیستم عامل های دیگر گوشی همراه همچون windows phone و ios فراهم است.

جدول ۵- محاسبه ریسک برنامه های مخرب گزارش شده با استفاده از دو روش میانگین ضرایب و سیستم خبره فازی

نام برنامه	میزان ریسک محاسبه شده بر اساس میانگین ضرایب	برچسب ریسک	میزان ریسک محاسبه شده بر اساس سیستم خبره	برچسب ریسک
Whale camera	۸٤	خیلی بالا	۷۳,۵۵	خیلی بالا
Hot camera	۸۰	خیلی بالا	۷۳,۵۵	خیلی بالا
coco camera	۸٤	خیلی بالا	۷۳,۵۵	خیلی بالا
tiny cleaner	۸۲,۵	خیلی بالا	۷۳,۵۵	خیلی بالا
swan camera	۸٤	خیلی بالا	۷۳,۵۵	خیلی بالا
clever camera	۸٤	خیلی بالا	۷۳,۵۵	خیلی بالا
Topspeed Test2	۷۹	خیلی بالا	۷۳,۵۵	خیلی بالا
ice camera	۸٤	خیلی بالا	۷۳,۵۵	خیلی بالا

منابع و ماخذ

1. Choi. Junho and Sung. Woon and Choi. Chang and Kim. Pankoo, Personal information leakage detection method using the inference-based access control model on the Android platform, Elsevier, 2015.

2. E. Krutz. Daniel and Mirakhorli. Mehdi and A. Malachowsky. Samuel and Ruiz. Andres and Peterson. Jacob and filipski. andrew and smith. jared, A Dataset of Open-Source Android Applications, 12th Working Conference on Mining Software Repositories, 2015.

3. Enck. William and Ongtang. Machigar and McDaniel. Patrick, On lightweight mobile phone application certification, Acm.2009.

4. Gokhan. Bal and Rannenberg. Kai and I. Hong. Jason, Styx: privacy risk communication for the android smartphone platform based on apps data-access behavior patterns, Elsevier, 2015.

5. Sharma .Kavita and Gupta .B. B., Mitigation and risk factor analysis of android applications, Elsevier, 2018.

6. Zhang.Li Lyna, Mike Liang.Chieh-Jan, Lucis Li.Zhao, Liuy .Yunxin, Zhao.Feng, Chen.En-Hong, Characterizing Privacy Risks of Mobile Apps with Sensitivity Analysis, IEEE, 2018.

7. Moonsamy. Veelasha and Rong. Jia and Liu. Shaowu, Mining permission patterns for contrasting clean and malicious android applications, Elsevier, 2013.

8. Mylonas. Alexios and Theoharidou. Marianthi and Gritzalis. Dimitris, Assessing privacy risks in android: a user-centric approach, Springer international publishing Switzerland, 2014.

9. Pandita. Rahul and Xiao. Xusheng and Yang. Wei and Enck. William and Xie. Tao, WHYPER: towards automating risk assessment of mobile applications, Elsevier, 2012.

10. Yoo.Sangbong, Ryeol Ryu.Hong, Yeon. Hanbyul, Kwon.Taekyoung, Jang.Yun, Visual analytics and visualization for android security risk, Elsevier, 2019.

11. S. Gates. Christopher and Li. Ninghui, Generating summary risk scores for mobile applications, Ieee transactions on dependable and secure computing, 2014.

12. S. Gates. Christopher and Li. Ninghui, Effective risk communication for android apps, Ieee transactions on dependable and secure computing, 2014.

13. Shahriar. Hossain and Islam. Mahbubul, Android Malware Detection Using Permission Analysis, IEEE, 2017.

14. Sokolova. Karina and Lemercier. Marc and Perez. Charles, Android permission usage: a first step towards detecting abusive applications, The seventh international conferences on pervasive patterns and applications, 2015.

15. Sokolova. Karina and Perez. Charles and Lemercier. Marc, Android application classification and anomaly detection with graph-based permission patterns, Elsevier, 2016.

16. Talha. Kabakus Abdullah and Alper. Dogru Ibrahim and Aydin. Cetin, APK auditor: permission-based android malware detection System, Elsevier, 2015.

17. Theoharidou. Marianthi and Mylonas. Alexios and Gritzalis. Dimitris, A Risk

Assessment Method for Smartphones, Ieee, 2013.

18. Zhauniarovich. Yury and Russello. Giovanni, MOSES: supporting and enforcing security profiles on smartphones, Ieee transactions on dependable and secure computing, 2014.

19. Citrix. BYOD and Information Security. Fort Lauderdale, FL, USA: Citrix Systems, Inc. Available from http://citrix.com, 2014.

20. Cafebazar.ir

21. clark.com/technology/google-play-malware-app-hummingbad, 2016.

22. Dehghanpoor.Chris, http://www.blog.lookout.com/brain-test-re-emerges, 2016.

23. https://gizmodo.com/why-you-should-stop-using-telegram-right-now-1782557415,2016.

24. OWASP:Top10MobileRisks, http://www.owasp.org/index.php/WASP_Mobile_Security_Project, 2015.

25. Security Tips Android Developers, http://www.developer.android.com/training/articles/securitytips.html, 2014.

26. SecurityAndroidDevelopers, https://developer.android.com/reference/android/Manifest .permission.html, 2014.

27. Security.AndroidDevelopers, https://source.android.com/devices/tech/security, 2014.

28. StatCounter.com/ Web Analytics Made Easy, 2016.