****

**دانشگاه شهید بهشتی**

**دانشکده مهندسی و علوم کامپیوتر**

**اطلاعیه دفاع**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **نام استاد راهنما: جناب اقای دکتر**  **حسن حقیقی** | | | **نام دانشجو: محمد محسن حسام الحکما عکس** | |
| **مقطع:کارشناسی ارشد** | **گرایش:نرم افزار** | | | **رشته: مهندسی کامپیوتر** |
| **تاریخ:۲۹/۶/۱۴۰۰** | | | **نوع دفاع:**   * **دفاع پروپوزال □** * **دفاع پایان نامه ✓** * **دفاع رساله دکترا □** | |
| **ساعت: ۸:۰۰** | | |
| <http://194.225.24.96/defa-computer-4> **مکان:** | | |
| **عنوان: ارائه رویکردی کارآمد به منظور شناسایی بدافزار در سیستم‌عامل اندروید** | | | | |
| **داوران داخلی: جناب اقای دکتر مجتبی وحیدی اصل** | | **داوران خارجی: جناب اقای دکتر مرتضی امینی** | | |
| **چکیده:**  **با توجه فراگیر شدن استفاده از تلفنهای هوشمند در سالیان اخیر، لزوم توجه به امنیت تلفنهای هوشمند بیش از پیش افزایش یافته است. در این میان سیستم عامل اندروید پر استفاده ترین سسیتم عامل مورد استفاده در تلفنه ای هوشمند است. امروزه اندروید بیش از ۷۵ درصد سهم بازار تلفن های هوشمند را در اختیار دارد. این حوزه به قدری برای توسعه دهندگان بدافزارها جذاب شده که روزانه تعداد بسیار زیادی خانواده بدافزار جدید معرفی شده و سیستمهای بیشماری را الوده می سازند.**  **تا کنون تحقیقات بسیار زیادی در رابطه با شناسایی بدافزارهای سیستم عامل اندروید انجام گرفته است. سامانه های شناسایی بدافزار کنونی از روش های ایستا، روش های پویا و روش های ترکیبی به منظور شناسایی بدافزار استفاده میکنند. روش های ایستا بدون اجرا کردن کد برنامه اقدام به شناسایی می کنند و روش های پویا برای استخراج ویژگی نیاز به اجرای برنامه در محیط ایزوله دارند. روش های ترکیبی از ترکیب روش های پویا و ایستا به منظور شناسایی بدافزار استفاده می کنند. در این پایان نامه سعی شد تا روشی کارآمد به منظور شناسایی بدافزارهای سیستم عامل اندروید ارائه گردد که هم از دقت بالایی برخوردار باشد و هم سرعت قابل قبولی داشته باشد.**  **در روش پیشنهادی به منظور شناسایی کارامد بدافزارهای اندرویدی، از مجموعه داده OmniDroid با ۲۲۰۰۰ برنامه اندرویدی متشکل از ۱۱۰۰۰ برنامه سالم و ۱۱۰۰۰ برنامه مخرب استفاده شد. ابتدا طیف وسیعی از ویژگی های ایستا که برای استخراج به اجرای برنامه نیاز ندارند استخراج گردید. این ویژگیها شامل فراخوانی های تابعی، دسترسی ها، سرویس ها، دریافت کننده ها، فعالیت ها، نام بسته ها، کدهای دودویی و جریانهای داده ای هستند. پس از استخراج ویژگیها با استفاده از روشهای ساخت یافته اقدام به کاهش ویژگی ها و جداسازی ویژگی های کارامد صورت گرفت. سپس به منظور افزایش قابلیت اطمینان مدل شناسایی بدافزار، داده های خیالی ساخته شد. در ادامه زیرمجموعه ویژگی های استخراج شده به مدل یادگیری ماشین از نوع شبکه های عصبی مصنوعی از نوع LSTM ،CNN و Fully Connected وارد شدند و مدل یادگیری ماشین ساخته شد. در نهایت روش پیشنهادی به دقت 95.18 درصدی دست یافت که حدود ۵ درصد بیشتر از مقاله پایه است.** | | | | |